LE SECRET MÉDICAL ET LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Thèse

en vue de l'obtention du grade de

Docteur en droit

Présentée et soutenue publiquement le 11 décembre 2019 par

Valérie OLECH

Sous la direction de

Monsieur Bruno PY

Professeur de droit privé et sciences criminelles à l'Université de Lorraine

Devant le jury de soutenance ainsi composé :

Madame Alexandra BENSAMOUN (Rapporteur)
Professeur à l'Université de Rennes 1

Madame Bénédicte BEVIERE-BOYER (Suffrageant)
Maître de conférences-HDR à l'Université Paris 8

Monsieur Thibault DOUVILLE (Suffrageant)
Professeur à l'Université de Caen

Monsieur Patrick MISTRETTA (Rapporteur)
Professeur à l'Université Jean Moulin-Lyon 3

Monsieur Olivier RENAUDIE (Suffrageant)
Professeur à l'Université de Paris 1 Panthéon-Sorbonne

LE SECRET MÉDICAL ET LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Thèse

en vue de l'obtention du grade de

Docteur en droit

Présentée et soutenue publiquement le 11 décembre 2019 par

Valérie OLECH

Sous la direction de

Monsieur Bruno PY

Professeur de droit privé et sciences criminelles à l'Université de Lorraine

Devant le jury de soutenance ainsi composé :

Madame Alexandra BENSAMOUN (Rapporteur)
Professeur à l'Université de Rennes 1

Madame Bénédicte BEVIERE-BOYER (Suffrageant)
Maître de conférences-HDR à l'Université Paris 8

Monsieur Thibault DOUVILLE (Suffrageant)
Professeur à l'Université de Caen

Monsieur Patrick MISTRETTA (Rapporteur)
Professeur à l'Université Jean Moulin-Lyon 3

Monsieur Olivier RENAUDIE (Suffrageant)
Professeur à l'Université de Paris 1 Panthéon-Sorbonne

REMERCIEMENTS

Mes remerciements vont d'abord au Professeur Bruno Py. S'il m'a offert la chance de réaliser cette thèse, il a également été d'une rare disponibilité. Il aura fait de ces années de thèse des années formatrices, en me laissant progresser sans jamais me laisser perdre pied. Ces quelques lignes sont insuffisantes à lui exprimer ma gratitude, pour sa direction mais aussi, et c'est essentiel, pour sa vision de la vie, des rapports humains, de ce qu'est une équipe. Pour sa patience, aussi. C'est au Professeur et à la personne que j'exprime, par ces mots, ma déférence.

Mes plus vifs remerciements vont ensuite aux Professeurs Alexandra Bensamoun (Université de Rennes 1), Thibault Douville (Université de Caen), Patrick Mistretta (Université Jean Moulin-Lyon 3), Olivier Renaudie (Université Paris 1 Panthéon-Sorbonne) et à Madame Bénédicte Bévière-Boyer (Université Paris 8) pour avoir accepté de siéger dans le jury de cette thèse.

Je me suis souvent interrogée sur la façon de formuler mes remerciements aux personnes qui me soutiennent depuis toujours, à celles dont la rencontre a éclairé mon chemin, à ceux qui m'ont aidé, à mes amis, ma famille, tous ceux qui forment le tissu de ma vie. Il m'est impossible de procéder par énumération. Je ne peux pas plus effectuer une forme de hiérarchisation. J'ai, avec chacun d'eux, un lien unique, que j'espère vrai et qui n'a pas besoin de mots tant qu'il y a des actes. Ma gratitude n'est pas discible, ils ont tous une part dans ce travail comme ils prennent part à ma vie.

A mes parents,

A Thomas,

SOMMAIRE

Une table des matières figure à la fin de l'ouvrage

LISTE DES ABREVIATIONS

act. : actualité(s)
Adde : ajouter
AFNOR : Agence française de normalisation
AJ contrat : *L'Actualité juridique de droit des contrats*
AJ famille : *L'Actualité juridique de droit de la famille*
AJ pénal : *L'Actualité juridique de droit pénal*
AJCA : *L'Actualité juridique de droit des contrats d'affaires*
AJCT : *L'Actualité juridique de droit des collectivités territoriales*
AJDA : *L'Actualité juridique de droit administratif*
al. : alinéa
ALD *: Actualité législative Dalloz*
ANSM : Agence nationale de sécurité du médicament
ANSSI : Agence nationale de sécurité des systèmes d'information
Arch. ph. droit : *Archives de philosophie du droit*
ARS : Agence régionale de santé
art. : article
ASIP santé : Agence française de la santé numérique

Bull. : bulletin
Bull. civ. : Bulletin des arrêts de la Chambre civile
Bull. crim. : Bulletin des arrêts de la Chambre criminelle

C. civ. : Code civil
CP : Code pénal
c/ : contre
CAA : Cour administrative d'appel
CADA : Commission d'accès aux documents administratifs
Cah. dr. entr. : Cahier de droit de l'entreprise
Cah. jurispr. : Cahier de jurisprudence
CASF : Code de l'action sociale et des familles
CCC : *Contrats Concurrence Consommation* (Revue)
CDNOM : Chambre disciplinaire nationale de l'Ordre des médecins
CE : Conseil d'Etat
CourEDH : Cour européenne des droits de l'Homme
CEI : Commission électronique internationale
CEN : Comité européen de normalisation
CENELEC : Comité européen de normalisation en électronique et en électrotechnique
CEPEJ : Commission européenne pour l'efficacité de la justice
chron. : chronique
CI-SIS : Cadre d'interopérabilité des systèmes d'information de santé
Civ. 1ère : Première chambre civile de la Cour de cassation
Civ. 2ème : Deuxième chambre civile de la Cour de cassation
Civ. : Chambre civile de la Cour de cassation
CJCE : Cour de justice des Communautés européennes
CJUE : Cour de justice de l'Union européenne
CNIL : Commission nationale de l'informatique et des libertés
CNRS : Centre national de la recherche scientifique
COFRAC : Comité française d'accréditation
coll. : collection

Com. comm. électr. : Communication Commerce Electronique
Com. : Chambre commerciale de la Cour de cassation
comm. : commentaire(s)
concl. : conclusions
Cons. const. : Conseil constitutionnel
Consid. : considérant
Contra : en sens contraire
CPP : Code de procédure pénale
Crim. : Chambre criminelle de la Cour de cassation
CRPA : Code des relations entre le public et l'administration
CSP : Code de la santé publique
CSS : Code de la Sécurité Sociale
D. : *Recueil Dalloz*
dact. : dactylographié(e)
D. actu. : *Dalloz Actualités*
déc. : décembre
DH : *Dalloz Hebdomadaire*
DMP : Dossier médical partagé
doctr. : doctrine
DP : *Dalloz Périodique*
DP : dossier pharmaceutique
Dr. adm. : *Droit administratif* (Revue)
Dr. et patr. : *Droit et patrimoine* (Revue)
Dr. fam. : *Droit de la famille* (Revue)
Dr. fisc. : *Droit fiscal* (Revue)
Dr. pén. : *Droit pénal* (Revue)
Dr. soc. : *Droit social* (Revue)

éd. : édition
eIDASS : Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur
Enc. des collec. loc. : *Encyclopédie des collectivités locales Dalloz*
esp. : espèce
Et. et doc. : Etudes et documents du Conseil d'Etat
ETSI : European Telecommunications Standards Institute

fasc. : fascicule
févr. : février
FUSL : Facultés Universitaires Saint-Louis Bruxelles

Gaz. Pal. : *La Gazette du Palais*
GHT : Groupement hospitalier de territoire

HAS : Haute Autorité de santé
HDF : Heures de France

IA : intelligence artificielle
ibid. : *ibidem*
id. : *idem*
infra : ci-dessous
IR : *Recueil Dalloz Informations rapides*
IRJS : Institut de Recherche Juridique de La Sorbonne
ISO : Organisation internationale de normalisation

JA : *Juris Associations*
janv. : janvier
Jcl. : *Encyclopédie Juris-classeur*
Jcl. adm. : *Encyclopédie Juris-classeur de droit administratif*
Jcl. concurrence : *Encyclopédie Juris-classeur de droit de la concurrence*
Jcl. comm. : *Encyclopédie Juris-classeur de droit de la communication*
Jcl. Pénal Code *: Encyclopédie Juris-classeur de droit pénal*
JCP : *Juris-classeur périodique (La Semaine Juridique)*
JCP A : *Juris-Classeur périodique (la Semaine Juridique), édition administrations et collectivités territoriales*
JCP E : *Juris-Classeur périodique (la Semaine Juridique), édition entreprise*
JCP G : *Juris-Classeur périodique (la Semaine Juridique), édition générale*
JDSAM : *Journal de droit de la santé et de l'assurance maladie*
juill. : juillet

LGDJ : Librairie générale de droit et de jurisprudence
LEH : Les Etudes hospitalières
LIL : Loi informatique et libertés
LPA : *Les Petites Affiches*

n° : numéro
NIR : Numéro d'inscription au Répertoire des personnes physiques
NIS : Network and Information Security (Directive)
nov. : novembre

obs. : observations
oct. : octobre
op. cit. : *opere citato* (dans l'ouvrage précité)

p. : page(s)
pan. : panorama
PGSSI-S : Politique générale de sécurité des systèmes d'information de santé
PMSI : Programme de médicalisation des systèmes d'information
préf. : préface de
PI : *Propriétés intellectuelles* (Revue)
PSSI : Politique de sécurité des systèmes d'information
PUAM : Presses universitaires d'Aix-Marseille
PUF : Presses universitaires de France
PUL : Presses universitaires de Lyon
PUN : Presses universitaires de Nancy

rapp. : rapport
RDC : *Revue des contrats*
RDLF : *Revue des droits et libertés fondamentaux*
RDP : *Revue de droit public*
RDP : *Revue de droit public et de la science politique en France et à l'étranger*
RDS : *Revue droit & santé*
RDSS : *Revue de droit sanitaire et social*
Rec. : Recueil Lebon
rééd. : réédition
Rép. civ. : Répertoire de droit civil Dalloz
Rép. cont. admin. : Répertoire du contentieux administratif Dalloz

Rép. dr. eur : Répertoire de droit européen Dalloz
Rép. pén. : Répertoire de droit pénal et de procédure pénale Dalloz
Req. : Chambre des requêtes de la Cour de cassation
Rev. adm. : *La revue administrative*
Rev. int. dr. écon. : *Revue internationale de droit économique*
Rev. pén. : *Revue de droit pénitentiaire et de droit pénal*
Rev. sociétés : *Revue des sociétés*
RFAP : *Revue française d'administration publique*
RFDA : *Revue française de droit administratif*
RGDA : *Revue générale du droit des assurances*
RGDM : *Revue générale de droit médical*
RGPD : Règlement général sur la protection des données
RIDC : *Revue internationale de droit comparé*
RJEP : *Revue juridique de l'entreprise publique*
RJF : *Revue de jurisprudence fiscale*
RLDI : *Revue Lamy droit de l'immatériel*
RRJ : *Revue de la Recherche juridique*
RSC : *Revue de science criminelle et de droit pénal comparé*
RTD civ. : *Revue trimestrielle de droit civil*
RTD com. : *Revue trimestrielle de droit commercial*
RTD eur. : *Revue trimestrielle de droit européen*

S. : *Recueil Sirey*
sect. : section
Soc. : Chambre sociale de la Cour de cassation
somm. : sommaire
sous art. : sous l'article
spéc. : spécialement
ss. la dir. : sous la direction de
SSJS : sous-section jugeant seule
SSR : Sous-sections réunies
STAD : Système de traitement automatisé de données
supra : ci-dessus
svt. : et suivant(e)s

t. : tome
T. corr. : tribunal correctionnel
TA : tribunal administratif
th. : thèse
TIC : technologies de l'information et de la communication
trad. : traduction
Trib. : tribunal

USLB : Université Saint-Louis Bruxelles

v. : voir
V° : *verbo*
vol. : volume(s)

INTRODUCTION

« *Vivre efficactement, c'est vivre avec une information adéquate* »[1]

§ 1 - Le premier objet : Le secret médical

1. La polysémie du mot « secret ». Dès lors qu'il s'agit de porter un regard sur le secret en droit, la doctrine fait régulièrement mention de son étymologie[2]. Éloquente, elle pemettrait à tous d'en saisir le sens. Dans cette mesure, le « *pari communicationnel* »[3] à la base de toute définition ferait son office[4]. S'il est vrai que l'étymologie permet de comprendre que ce qui est secret est ce qui est tenu à part, ce qui ne doit pas être révélé[5], il n'est pourtant pas certain que sa compréhension soit univoque. C'est que le terme est polysémique. Dans le langage commun, le *secret* connaît deux formes, une forme adjectivale et une forme substantive. Chacune de ces formes comprend des définitions multiples au regard du contexte dans lesquelles elles sont employées[6]. Le terme aurait une traduction dans le vocabulaire juridique, le secret étant une

---

[1] N. WIENER, *Cybernetique et société*, coll. 10/18, Edition des Deux-Rives, 1971, p. 19

[2] Pour quelques exemples : B. FEUILLET- LE MINTIER, « Les fondements du secret médical », *Revue juridique de* l'Ouest 2000, *in Les médecins libéraux face au secret médical*, n° spéc., Pp. 1-9, *spéc.* p. 4 ; P. MALAURIE, « Le secret et le droit. Une petite anthologie littéraire », *in Mélanges Christian Mouly*, Litec, 1998, p. 106 ; M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, th. dact., ss. la dir. d'A. PROTHAIS, soutenue en 2004, Université de Lille 2, p. 6, n° II ; J. LAGRÉE, « Éthique et partage du secret professionnel », *RDSS* 2015, p. 465 ; C. GHICA-LERMARCHAND, « La responsabilité pénale de la violation du secret professionnel », *RDSS* 2015 p. 419.

[3] E. PIC, *Caractérisation de l'anglais des droits de l'homme en tant que langage de spécialiste : un essai de méthodologie terminologique*, th. dact., ss. la dir. de J. HUMBLEY, soutenue en 2007, Paris 7 ; « *Il est présupposé que les mots du definiens sont conventionnellement compris, connu, ou peuvent aisement l'être, parce qu'implicitement ou bien il renvoit au sens ordinaire des mots (celui du dictionnaire), ou bien il se rapportent au sens technique conféré dans un domaine, ou un champ lexical spécialisé que le lecteur est supposé pouvoir identifier* » (V. CHAMPEIL-DESPLATS, *Méthodologies du droit et des sciences du droit*, coll. Méthodes du droit, Dalloz, 2016, *spéc.* n° 485).

[4] M.-A. FRISON-ROCHE, *Secrets professionnels*, coll. Essai, Autrement, 1999, p. 17.

[5] De l'ancien français *segrei* ou plus tardivement *secroi*, ces deux formes sont elles-même issues du latin *secretum* signifiant « lieu écarté », « pensée ou fait qui ne doit pas être révélé ». L'adjectif *secretus* signifiant « séparé, à part », « solitaire, isolé, reculé ». *V°* « Secret » *in Dictionnaire historique et étymologique de la langue française Robert*, A. REY (dir.), T.2, 3ème éd., 2000.

[6] TLFi, <http://www.atilf.fr/tlfi>, ATILF - CNRS & Université de Lorraine, *V°* « Secret ».

« *chose cachée* » et « *par extension* », la « *protection qui couvre cette chose* » ; cette protection pouvant consister « *soit pour celui qui connaît la chose, dans l'interdiction de la révéler à d'autres* […] *soit pour celui qui ne la connaît pas, dans l'interdiction d'entrer dans le secret* »[7]. Cette distinction est une construction que la doctrine propose traditionnnellement pour distinguer *les secrets* en droit. Madame Lepage, à l'occasion d'une étude des secrets en matière pénale, en déploie les « *figures* »[8]. Tant sur le plan procédural que sur le plan substantiel, l'auteur remarque que le droit pénal prohibe – limite, s'agissant de la procédure pénale – les immixtions[9] et les révélations[10]. C'est un « *double verrouillage* »[11] qui caractériserait par exemple le secret des correspondances[12] ou le secret défense[13]. D'aucuns ajouteraient sans doute à cette liste la prohibition des immixtions dans le secret de la vie privée et la répression de la révélation de celui-ci[14]. En matière administrative, le Conseiller d'Etat Louis Fougère affirmait qu'il existait « *un double barrage légal : le mutisme de ses agents et le secret de ses papiers* »[15] . De cette distinction classique s'impose le constat de la multitude : la doctrine distingue *des* secrets en droit. Peut-être peut-on y voir la persistance des différences sémantiques : « *est-ce le secret qui protège ou est-ce le secret qu'on protège ? Il y a sans doute des deux* »[16]. Le secret est autant une technique qu'un objet, autant la chose que le résultat d'un

---

[7] *V°* « Secret », *in* G. CORNU (ss. la dir.), *Vocabulaire juridique*, 9ème éd., coll. Quadridge, PUF, 2011.
[8] A. LEPAGE, « Le secret, figure polymorphe du droit pénal », *in Mélanges en l'honneur du Professeur Michel Germain*, LexisNexis-LGDJ, 2015, p. 481.
[9] Que l'on pense par exemple aux saisies et perquisitions dont les règles procédurales se durcissent en fonction du secret qui est en jeu : le secret de la vie privée étant alors moins resistant que le secret de la défense nationale, le secret des sources des journalistes ou certains secrets professionnels (*Ibid.*). L'on peut également évoquer la prohibition de l'immixtion dans les lieux interessant la défense nationale (art. 413-7 du Code pénal) et dans les lieux privés (art. 226-4 du Code pénal).
[10] C'est le cas de l'infraction sanctionnant la violation du secret professionnel. L'incrimination inscrite à l'article 226-13 du Code pénal prohibe la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire.
[11] *Ibid.* n° 9.
[12] *Ibid.*, n° 8-9. L'article 226-15 du Code pénal et et l'article 432-9, al. 1er du Code pénal prohibe l'immixtion tandis que l'article 413-9, al. 1er du même Code puni la révélation du contenu des correspondances (art. 226-15 al. 2 et 432-9 al. 2 concernant la divulgation des correspondances émises par voie électroniques).
[13] *Ibid.* L'article 413-11, 1° du Code pénal réprime le fait pour une personne non qualifiée d'accéder ou de prendre connaissance d'un document, d'un objet, d'un procédé classé secret défense, le 3° du même article reprime le fait de révéler le secret ; et encore puni le fait pour la personne qui est dépositaire d'un élément classés secret défense de le révéler à une personne non qualifiée pour le recevoir (CP art. 413-10).
[14] CP Art. 226-1 à 226-3-1.
[15] L. FOUGERE, « Les secrets de l'administration », *Bull.* II AP, 1967, p. 21 ; l'expression est reprise par : F. MODERNE « Conception et élaboration de la loi du 17 juillet 1978 » *in Transparence et secret*, 16 et 17 octobre 2003 publié à la Documentation française, p. 19 et s. ; O. BUI-XIAN, « Les secrets de l'administration », *RDP* 2012, p. 1119.
[16] G. LOISEAU, *Rapport de synthèse, Actes du colloque annuel de la Semaine Juridique*, *Le secret à l'ère de la transparence*, *JCP G* 2012, suppl. au n° 47, p. 44 et s.

comportement qui permet d'affirmer qu'une chose est secrète. « *Depuis des temps anciens, le secret est un mode de protection, par exemple pour réserver aux initiés la connaissance de certains savoirs. Aujourd'hui encore, c'est une technique utilisée pour protéger des inventions qu'on ne veut pas rendre publiques en les brevetant. Mais le secret est aussi ce que le droit protège* »[17]. Cette construction est également celle qui préside à la définition doctrinale du « secret médical », il serait à la fois « objet » du droit et « mode de protection ».

2. La définition communément admise. Il n'existe aucune définition prétorienne ou légale[18] du « secret médical ». Selon la doctrine majoritaire, le « secret médical » serait un « droit du malade » et une « obligation du médecin » :

> « *Le secret médical, ce devoir fondamental du médecin, est une notion bien connue des juristes […]. Il constitue également un droit au fondement de la relation médicale, « institué dans l'intérêt des patients » selon l'article 4 du code de déontologie et consacré comme droit de l'usager du système de santé, selon la loi du 4 mars 2002. Le droit au respect du secret médical devient ainsi un élément de la protection juridique de la vie privée, la législation française rejoignant la jurisprudence de la Cour européenne des droits de l'homme, laquelle rattache le respect du secret médical à la protection de l'article 8 de la Convention. Or, cette affiliation met le secret à la merci de la volonté du malade : tout comme la personne est libre de dévoiler des aspects de sa vie privée, elle est libre de disposer du secret médical. Le patient est le « maître du secret », selon la formule classique, et le médecin ne peut le lui opposer pour, par exemple, refuser de lui communiquer certaines informations ou de lui délivrer un certificat médical* »[19].

---

[17] *Ibid.*

[18] L'absence de définition dans les énoncés normatifs est courante, elle se revèle être une technique au même titre que l'exercice de définition, elle peut notamment résulter d'une volonté de l'autorité normative de laisser aux destinataires de la norme une marge d'appréciation comme c'est notmament le cas pour les standards (V. CHAMPEIL-DESPLAT, *Méthodologies du droit et des sciences du droit*, *op. cit.*, n° 503). Les définitions légales sont plutôt rares comparé à l'importance qu'elles revêtent (pour un exemple d'inventaire des définitions codifié au sein du Code civil, du Code de procédure civil et du Code pénal : J.-L. Bergel, *Méthodologie juridique*, 5e éd., coll. Méthodes du droit, Presses universitaires de France, 2005, n°172, p. 230) dans la mesure où elles rendent possible le lien entre le fait et le droit. Ce lien est opéré par l'exercice de qualification, « *opération intellectuelle d'analyse juridique, outil essentiel de la pensée juridique* » (G. CORNU, *Vocabulaire juridique*, 9e éd., coll. Quadridge, PUF, 2011, *V°* « Qualification ») consistant à déterminer « *le régime et les conséquences juridiques* » (*Ibid.*) qui s'attachent à la situation ou au fait.

[19] D. ROMAN, « Le respect de la volonté du malade : une obligation limitée ? », *RDSS* 2005, p. 423.

Du devoir déontologique[20] serait née l'infraction. De l'infraction serait né un droit de la personne. Reconnu par la Cour européenne des droits de l'homme[21] et enteriné par le legislateur[22], il existerait désormais un « droit au respect du « secret médical » qui consisterait pour le patient, usager du système de santé, en une « maîtrise du secret ». Cette définition est devenue la *doxa*, le discours dominant que l'on trouve dans les manuels et monographies[23] et dans les articles de doctrine, souvent posée comme une réalité inattaquable[24]. Certains ont vu dans cette définition un argument confirmant l'idée selon laquelle le consentement du patient

---

[20] Le secret des médecins est d'essence axiologique. Le devoir du médecin fait partie, depuis des millenaires de la morale médicale et certains écrit et discours de déontologues sont. Cette essence permet, il nous semble, de comprendre que les problématiques qui ont occupées et occupent encore une majorité de la doctrine portent sur la légitimité du secret professionnel, non pas quant à son existence, mais quant à sa portée et qu'il est toujours question dans les discussions doctrinales de savoir si telle ou telle limitation de la portée de ce secret est légitime, si telle ou telle limitation d'un autre intérêt par le secret est légitime. De là également les débats intenses - mais relativement vains car jamais éteints- sur les fondements du secret professionnel, entre intérêt de la personne soigné ou intérêt du professionnel. Il n'est pas possible de reproduire ici la somme des arrêts et des débats y ayant donné lieu, Emile Garçon en donne déjà un aperçu, édifiant, dans ses commentaires du Code pénal (E. GARCON, Code pénal annoté, T. 2, Ed. refondue et mise à jour par M. ROUSSELET, M. PATIN et M. ANCEL, Sirey, Paris, 1956, art. 378). Nous ne manquerons pas de tirer de cette littérature gargantuesque ce qui nous est nécessaire au moment voulu.

[21] CEDH, 27 août 1997, M.S. c/ Suède, req. 20837/92, Rec. 1997-IV.

[22] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé : « *Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant* » (première version de l'article L. 1110-4, al. 1).

[23] Sans toutefois l'énoncer clairement mais traitant du *secret professionnel et médical* dans un chapitre consacré aux droits malades hospitalisés : C. BERGOIGNAN-ESPER et M. DUPONT, *Droit hospitalier*, 10e éd., coll. Cours, Dalloz, 2017, n° 864 et svt. ; V. également M. CONTIS, *Secret médical et évolutions du système de santé*, Préf. C. NEIRINCK, Coll. Thèses, 2010 ; A. LAUDE, B. MATHIEU et D. TABUTEAU, *Droit de la santé*, 3ème éd., coll. Thémis droit, PUF, n° 388 et svt. ; J.- C. SAINT-PAU, « Le droit au respect de la vie privée », *in* J.-C. SAINT-PAU, *Droits de la personnalité*, LexisNexis, 2013, n° 1192 et svt ; G. MEMETEAU et M. GIRER, *Cours de droit médical*, *op. cit.*, n° 396 et svt.

[24] Quelques exemples : « *Devoir du médecin, mais aussi droit du malade, le secret médical est la pierre angulaire de la relation entre médecin et malade sur laquelle se maintient la confiance réciproque indispensable aux soins* » (D. HOUSSIN, « Le secret médical dans les nouvelles pratiques et les nouveaux champs de la médecine », *D.* 2009 p. 2619) ; « *le secret médical n'est plus essentiellement conçu comme une obligation pesant sur les professionnels de la santé, mais comme un droit du patient* » (B. MATHIEU, « Les droits des personnes malades », *LPA*., 19 juin 2002, n° 122, p. 13) ; « *Il apparaît que le secret médical est en cours de mutation. De devoir du médecin conçu dans un but de protection de l'intérêt général, il tend à devenir un droit du patient établi dans son intérêt privé* » (M. CAUCHY et A. DIONISI-PEYRUSSE, « Le droit au secret médical et son application en matière d'assurances », *D.* 2005, p. 1313 ; « *le respect du secret professionnel est un droit du patient* » (M. DE FALLOIS, « Assurance et « droit à l'oubli » en matière de santé », *RDSS* 2017, p. 132) ; « *À l'origine conçu comme un droit du médecin, fondement de la confiance nécessaire du patient, il est aujourd'hui, et notamment sous l'impulsion de la loi « Kouchner » du 4 mars 2002 qui fait entrer l'idée de « démocratie » dans le système de santé, un droit du patient « maître du secret* » (S. ABRAVANEL-JOLLY, « Le secret médical en assurances de personnes », *RGDA* 2005, p. 887) ; M. COUTURIER, « Que reste-t-il du secret médical ? », *in Mélanges en l'honneur de Gérard Mémeteau. Droit médical et éthique médicale : regards contemporains*, LEH Édition, 2015, pp. 351-360.

pourrait désormais constituer un fait justificatif de la violation du secret professionnel[25]. Validé par quelques jurisprudences en matière civile et largement commentées en ce sens[26]. Cette présentation de la notion[27] par la doctrine permet de *classer* le « secret médical » parmi les droits de la personnalité. Alors renommé « *secret de l'état de santé* »[28], « *secret de santé* »[29], voire « *secret des informations de santé* »[30], il consisterait classiquement en un pouvoir de s'opposer aux investigations relatives à l'état de santé, auquel le droit pénal apporte le support de sa sanction en prohibant le fait d'obtenir ou de tenter d'obtenir la communication des informations visées à l'article l'article L. 1110-4-IV du Code de la santé publique[31]. Classiquement, encore, la personne pourrait s'opposer à la divulgation de son état de santé[32].

Ainsi, tout aurait été dit à propos du « secret médical »[33]. Les querelles doctrinales relatives au fondement du secret professionnel se seraient taries puisque ce dernier serait désormais délimité par le seul intérêt du malade, ce qui expliquerait par ailleurs la généralisation

---

[25] Monsieur Mémeteau résume ce point de vue : « *La loi du 4 mars 2002 suit cette logique de protection de la vie privée, la protection du secret de l'information étant liée à celle-ci (art. L. 1110-4, § 1, C.S.P. et L. 161-1-A C. séc. soc.). Dans une analyse des droits des malades, au chapitre préliminaire des « droits de la personne », la lecture du principe de secret ne pouvait que quitter le terrain de l'ordre public des devoirs du médecin. Ceci permet d'écrire que « le maître du secret est bien le malade, et non le médecin ». Ainsi est-ce exactement que, rappelant l'existence de l'article 9 du Code civil, sans doute suffisant pour protéger (civilement) ces secrets, l'on met l'accent sur ce respect de la vie privée dans le nouvel ensemble législatif. Le droit pénal intervient, mais pour ajouter à la sanction civile. Si l'on délimite le contenu de l'obligation au secret par la nature des informations plutôt que par la qualité des obligés*, *il devient logique de considérer que le secret s'interprète par son objet, la vie privée à dissimuler aux tiers* » (G. MEMETEAU et M. GIRER, *Cours de droit médical*, 5ème éd., LEH, 2010, n° 409).

[26] H. GROUTEL, « Preuve de la déclaration inexacte du risque et secret médical », *Resp. civ. et assur.* 2004, Étude n° 18 ; P. BICHOT, « Le secret médical : un outil redoutable à la disposition des assurés de mauvaise foi », *Revue Lamy Droit Civil* 2005, n° 12, 01-2005 ; M. CAUCHY et A. DIONISI-PEYRUSSE, « Le droit au secret médical et son application en matière d'assurance », *D.* 2005, chron. 1313 ; S. ABRAVANEL-JOLLY, « Le secret médical en assurance de personnes », RGDA. 2005, p. 889 ; B. CERVEAU, « Assurance et secret médical : un cadre juridique précis, une jurisprudence bien établie », *Gaz. Pal.* 2010, n° 43-44, p. 15.

[27] Nous utilisons le terme de notion sans le différencier de celui de concept car ils sont le plus souvent employés indifféremment et comme le souligne Madame Champeil-Desplats « *La distinction entre la notion et le concept est sans doute l'un de celles qui conduit aux réponses les plus embarrassées, floue et fuyantes*. […]. *« Notion » et « concept » sont parfois ainsi utilisés l'un pour l'autre ; peut être nommée « notion » par les uns ce que d'autres appellent « concept », et réciproquement. Par ailleurs, lorsqu'une distinction entre « notion » et « concept » est entrevue, n'est pas toujours jugée utile* » (M. CHAMPEIL-DESPLATS, *Méthodologies du droit et des sciences du droit*, 2e éd., coll. Méthodes du droit, Dalloz, n° 529).

[28] J.- C. SAINT-PAU, « Le droit au respect de la vie privée », *in* J.- C. SAINT-PAU, *Droits de la personnalité*, LexisNexis

[29] M. COUTURIER, « Que reste-t'il du secret médical ? », *op. cit.*, p. 358.

[30] *Ibid.*

[31] *Ibid.*

[32] J. – C. SAINT-PAU, « Le droit au respect de la vie privée », *op. cit.*, n° 1194.

[33] M. COUTURIER, « Que reste-t'il du secret médical », *op. cit.*, p. 352.

du secret professionnel à l'ensemble des personnes intervenant dans le sytème de santé[34]. Cela conduirait à « *délimiter le contenu de l'obligation au secret par la nature des informations plutôt que par la qualité des obligés* »[35], raison pour laquelle il serait désormais « *logique de considérer que le secret s'interprète par son objet, la vie privée à dissimuler au tiers* »[36].

3. Il nous semble toutefois, sans qu'il soit besoin de discuter longuement, que cette définition a pour objectif de désigner positivement certaines limites posées au secret professionnel des professionnels de santé. Madame Thouvenin affirmait, bien avant cette reconnaissance légale, que « *sous couvert de secret médical, c'est la circulation de l'information médicale relative à un malade qui est en cause. L'argumentation tirée de l'existence de l'infraction de l'article 378 a pour objet d'écarter l'accès à cette information* »[37]. Que le juge civil ait pu reconnaître que la personne pouvait « *renoncer au secret médical* »[38] ne signifie pas qu'elle « maitrise le secret », pas plus que cela ne confirme la définition. Le contour des notions résulte « *de choix et d'arbitrages entre les nécessités de faits, les valeurs dominantes, la présentation doctrinale qui a présidé à sa mise en perspective, les fluctuations sociales et historiques diverses…* »[39]. Cette définition pourrait, en quelque sorte, s'être superposée au choix du législateur de faire figurer l'article L. 1110-4 du Code de la santé publique au sein d'un chapitre relatif aux *droits des personnes*. La formule selon laquelle toute personne prise en charge par un professionnel intervenant dans le système de santé « *a droit au respect de sa vie privée et du secret des informations la concernant* » finissant de convaincre. Un arrêt de la Cour européenne des droits de l'Homme *rattachant* le « secret médical » à l'article 8 de la Convention ainsi qu'un courant jurisprudentiel en matière civil ont ensuite permis d'affirmer que le consentement du patient justifiait la violation du secret professionnel, validant l'interprétation du texte. Cette définition ne peut être tenue ni pour vraie, ni pour fausse : elle est simplement utile à certaines démonstration[40], « *la doctrine* [étant] *libre de bâtir*

---

[34] L. 1110-4 du Code de la santé publique.
[35] G. MEMETEAU et M. GIRER, *Cours de droit médical*, *op. cit.*, n° 401 ; dans le même sens M. CONTIS, *Secret médical et évolutions du système de santé*, *op. cit.*
[36] *Ibid.*
[37] D. THOUVENIN, *Le secret médical et l'information du malade*, PUF, 1982, p. 167.
[38] Pour un développement complet sur ces arrêt v. J. KULLMANN, *Rep. civ.*, « Assurance de personne : vie-prévoyance-Exécution du contrat d'assurance, Janv. 2013, (act. Juillet 2019).
[39] J. ROCHFELD, *Les grandes notions du droit privé*, *op. cit.*, p. 4.
[40] Les définitions stipulatives sont une forme de définition qui se distingue des définitions informatives. Ces dernières cherchent à correspondre à une « réalité » (V. CHAMPEIL-DESPLATS, *Méthodologies du droit et des*

les catégories qu'elle souhaite afin de rendre compte de celle du droit positif »[41]. Pour confirmer cette relativité, il faut ajouter que les auteurs « *se réfère*[nt] *à telle ou telle règle en la supposant dotée d'un sens déterminé* »[42] tandis que le législateur comme le juge ne maîtrisent pas complètement la façon dont seront compris les mots dont ils usent. La définition doctrinale donnée à une notion pendant une période n'épuise pas le sens des mots, ni les conceptions dont ils sont déjà chargés. Ce phénomène de sédimentation, sémantique et conceptuel, « *juxtapose et tient en réserve des analyses, des conceptions plus ou moins fondamentales, des propositions, des présupposés dont les origines sont extrêmement diverses* »[43].

4. Les notions juridiques : des constructions. Les notions juridiques[44], quelles qu'elles soient, ne sont pas immuables. Elles ne décrivent pas une « *réalité préexistante* »[45]. Yan Thomas le formule de façon fort éclairante s'agissant des catégories[46] : « *Les catégories du*

---

sciences du droit, *op. cit.*, n° 488) c'est pourquoi elles « *ne peuvent jamais être considérées comme vraies ou fausses. Elles sont ou non adéquates, opératoires en fonction de l'objetfi poursuivi par celui y recours. Leur formulation suppose une grande part de fiction et d'arbitraire dans la mesure où leur visée première n'est pas de correspondre à une vérité essentielle ni même à une réalité empirique mais de remplir certaines fonctions* » (Ibid. n° 497). Dans notre cas la définition doctrinale dominante du secret médical à au moins vocation à souligner la limitation de la portée du secret professionnel à l'égard des patients.

[41] G. TUSSEAU, « Critique d'une métanotion fonctionnelle », *RFDA* 2009, p. 641 ; « *le juriste de doctrine* […] *est appelé parfois à créer lui-même des concepts à contenu juridique qui lui servent à la connaissance et à l'analyse systématique du droit, mais qui ne sont pas posés par les sources du droit positif, ou dont la dénomination, même si elle est utilisée par « la pratique » pour des qualifications d'objets concrets, ne lie cette fois pas le juriste* » (C. EISENMANN,« Quelques problèmes de méthodologie des définitions et des classifications en science juridique », *Arch. ph. dr.*, n° 11, 1966, p. 25-43).

[42] C. ATIAS, *Questions et réponses en droit*, coll. L'interrogation philosophique, PUF, 2009, p. 172.

[43] C. ATIAS, *Questions et réponses en droit*, *op. cit.*, p. 173. Le phénomène de sédimentation est généralisé, il est essentiel aussi, à toutes reflexion sur la connaissance, le langage, la construction sociale v. notamment M. FOUCAULT, *Archéologie du savoir*, Gallimard, 1969 ; F. DE SAUSSURE, *Cours de linguistique générale*, 3e éd., Payot, 1931, spéc. p. 177 et svt. relatives à la linguistique diachronique ; M. MERLEAU-PONTY, *Parcours II*, 1951-1961, collection « Philosophie », Éditions Verdier, 2000, p. 13.

[44] Nous utilisons le terme de notion sans le différencier de celui de concept car ils sont le plus souvent employés indifféremment et comme le souligne Madame Champeil-Desplats « *La distinction entre la notion et le concept est sans doute l'un de celles qui conduit aux réponses les plus embarrassées, floue et fuyantes*. […]. *« Notion » et « concept » sont parfois ainsi utilisés l'un pour l'autre ; peut être nommée « notion » par les uns ce que d'autres appellent « concept », et réciproquement. Par ailleurs, lorsqu'une distinction entre « notion » et « concept » est entrevue, n'est pas toujours jugée utile* » (M. CHAMPEIL-DESPLATS, *Méthodologies du droit et des sciences du droit*, 2e éd., coll. Méthodes du droit, Dalloz, n° 529).

[45] « *Selon une telle vision des choses, les notions juridiques existeraient par elles-mêmes dans une sphère de réalité située hors d'atteinte des hommes. Ceux-ci ne pourraient que dégager, révéler ou découvrir ces réalités préexistantes et, tout au plus, en déduire des conséquences par des moyens strictement logiques* » (G. TUSSEAU, « Critique d'une métanotion fonctionnelle », *op. cit.*, n° 4 ; également J. ROCHFELD, *Les grandes notions du droit privé*, PUF, 2011, p. 2.

[46] De la même manière que *concept* et *notion*, *catégorie* et *concept* ou *notion* ne sont pas toujours employés de la même manière par les auteurs. Généralement, comme le souligne Madame Champeil-Desplats les juristes font une

droit sont, si je puis dire, neutres en soi et vides de sens. Elles sont des contenants, des formes forgées de longue date, offertes à tous les emplois possibles. Tout contenu est susceptible d'être réduit à une forme juridique ou une autre »[47]. Les mêmes remarques peuvent être formulées à l'égard des notions, si tant est qu'on les distingue[48]. Comme le signale Madame Rochfeld, les notions « *sont en partie celles de l'observateur* »[49]. Prenant l'exemple du patrimoine ou de la propriété, l'auteur explique que malgré la force de certains discours aucune de ces deux notions ne serait véritable ou unique. Encore, Monsieur Tusseau souligne, bien que son approche du droit soit différente[50], qu'un « *même terme voit sa signification changer selon les acteurs qui l'emploient, les contextes, les intérêts en jeu, etc. Il en résulte que deux concepts se succèdent l'un à l'autre, même si le fait que chacun soit nommé par le même terme conduit à s'illusionner sur la persistance d'une unique réalité juridique* ». Partant, à travers un même terme, plusieurs constructions sont possibles, bienq qu'elles soient parfois éloignées du sens commun des mots qui composent le terme. Les notions sont donc contingentes des contextes, des époques et des auteurs mais également des significations des termes employés pour les désigner.

5. Les questions qui demeurent. Malgré l'affirmation doctrinale selon laquelle la notion de « secret médical » serait désormais bien définie, les positions contraires ne sont pas rares. Les conceptions du « secret médical » dépendent, pour beaucoup, de l'angle sous lequel il est appréhendé. L'auteur qui proposerait une étude sous le prisme du droit pénal, c'est-à-dire en identifiant le « secret médical » au « secret professionnel des professionnels de santé » serait plutôt enclin, au regard de la position classique en droit pénal français, à démontrer que le secret professionnel a un fondement d'ordre public et à considérer que le consentement de la victime n'est pas un fait justificatif[51]. Cela amènerait par ailleurs à disqualifier l'usage de l'expression

---

différence de degrés entre le concept et la catégorie. La catégorie sera alors, selon les définitions données, subsumée sous la notion ou inversement (V. CHAMPEIL-DESPLATS, *Méthodologies du droit et des sciences du droit*, *op. cit.*, n° 527).

[47] Y. THOMAS, « Le sujet de droit, la personne et la nature », *Le débat* mai-août 1998, n° 100, p. 104.

[48] Par exemple : « *pour bien spécifier la catégorie, dont la différence avec la notion ne se laisse pas aisément percevoir, il faut insister sur son caractère opératoire car il s'agit moins de distinguer deux objets différents que d'observer le même sous un autre regard* » (M.-O. BARDEAU, *La notion de contrat unilatéral : analyse fonctionnelle*, LGDJ-Lextenso éditions, 2014, n° 10, *spéc.* n° 8 et 10).

[49] J. ROCHFELD, *Les grandes notions du droit privé*, *op.cit.*, p. 3.

[50] Il adopte une approche analytique du droit. L'on trouvera encore un exposé complet de cette approche dans l'ouvrage de Madame Champeil-Desplats précédemment cité (M. CHAMPEIL-DESPLATS, *Méthodologies du droit et des sciences du droit*, *op. cit.*, *spéc.* n° 203 et svt).

[51] En ce sens v. notamment : M.- L. RASSAT, *Droit pénal spécial*. *Infractions du Code pénal*, 8e éd., coll. précis, Dalloz, n° 510 ; P. MISTRETTA, *Droit pénal médical*, Ed. Cujas, 2013, n° 543 ; B. PY, « Secret professionnel – Révélation licite », *Rep. pén.*, Février 2003 (act. : Février 2017), n° 158-159.

« secret médical »[52]. Cette dernière critique, d'ordre terminologique, repose principalement sur le constat d'un emploi indifférencié des termes « secret médical » et « secret professionnel » pour viser l'infraction sanctionnant la violation du secret professionnel[53]. Un rapide passage en revue de la doctrine et de la jurisprudence suffit à s'en convaincre : l'expression « secret médical » est utilisée pour viser l'obligation de silence imposée aux médecins et professionnels de santé et dont la violation est incriminée à l'article 226-13 du Code pénal. La linguistique se trouve être un outil méthodologique important pour comprendre l'emploi de l'expression « secret médical » afin de désigner le secret professionnel dans le domaine de la santé. Dans l'opinion évoquée, l'usage de l'expression « secret médical » comme signifiant de secret des professionnels de santé (signifié)[54] est rejeté au profit de celle de secret professionnel médical. Il est toutefois des hypothèses où le syntagme n'est pas mentionné pour désigner le secret professionnel. Il faut dès lors admettre qu'une même expression peut désigner plusieurs concepts[55]. Cette représentation peut trouver son origine dans l'histoire du secret

---

[52] La critique d'ordre terminologique repose principalement sur le constat d'un emploi indifférencié des termes « secret médical » et « secret professionnel » pour viser l'infraction sanctionnant la violation du secret professionnel (B. PY, *Le secret professionnel*, L'Harmattan, 2005, p. 15 ; « Réquisitoire contre l'expression secret médical : plaidoyer pour l'expression secret professionnel », RDS 2013, n° 1, Pp. 161-166 ; Partageant notamment ce point de vue : P. MISTRETTA, *Droit pénal médical*, Ed. Cujas, 2013, n° 513 ; F. VIALLA, « Perspectives pour une culture commune du secret et de l'information partagée », *JA* 2013, n°474, p.30. L'on peut également citer les auteurs d'un dictionnaire de droit de la santé au sein duquel l'entrée *secret professionnel* figure (M.-F. CALLU, M. GIRER et G. ROUSSET, *Dictionnaire de droit de la santé*. *Secteur sanitaire, médico-social*, LexisNexis, 2017). Un rapide passage en revue de la doctrine et de la jurisprudence suffit à s'en convaincre : l'expression secret médical est utilisée pour viser l'obligation de silence imposée aux médecins et professionnels de santé, dont la violation est incriminée à l'article 226-13 du Code pénal. Il conviendrait alors, selon cette doctrine, de ne retenir que l'expression « secret professionnel médical » en ce qu'elle est plus exacte (Elle permettrait d'éviter certaines confusions : Que les médecins ont une forme de monopole du secret professionnel ; que seules sont des informations à caractère secret les *informations médicales* c'est-à-dire celles ayant trait à la santé des personnes ; qu'il n'y aurait pas de secret d'un médecin envers un autre (B. PY, « Réquisitoire contre l'expression secret médical : plaidoyer pour l'expression secret professionnel », *op.cit.*).

[53] B. PY, *Le secret professionnel*, L'Harmattan, 2005, p. 15 ; « Réquisitoire contre l'expression secret médical : plaidoyer pour l'expression secret professionnel », RDS 2013, n° 1, Pp. 161-166 ; Partageant notamment ce point de vue : P. MISTRETTA, *Droit pénal médical*, Ed. Cujas, 2013, n° 513 ; F. VIALLA, « Perspectives pour une culture commune du secret et de l'information partagée », *JA* 2013, n°474, p.30. L'on peut également citer les auteurs d'un dictionnaire de droit de la santé au sein duquel l'entrée *secret professionnel* figure (M.-F. CALLU, M. GIRER et G. ROUSSET, *Dictionnaire de droit de la santé*. *Secteurs sanitaire, médico-social*, LexisNexis, 2017).

[54] « […] un signe linguistique est une entité à deux faces, la face signifiante, ou signifiant du signe (plus brièvement nommée signifiant), et la face signifiée, ou signifié du signe (nommée signifié) » (G. CORNU, *Linguistique juridique*, 3e éd., coll. Domat droit privé, Montchrétien, 2005, p. 26, n° 8).

[55] G. TUSSEAU, « Critique d'une métanotion fonctionnelle », *RFDA*, 2009, p. 641. L'auteur ne fait pas différence entre *notion* et *concept*, ce qu'il signale au début de son étude.

professionnel : du devoir issu de l'éthique médicale plusieurs fois millénaire[56], le législateur a créé une infraction au regard de laquelle seules les professions médicales semblaient astreintes à une obligation de secret pénalement sanctionnée. Le grand pénaliste Emile Garçon opérait le lien de filiation entre le « secret médical » et l'infraction pénale sanctionnant la violation du secret professionnel en intitulant son étude du secret professionnel des médecins « secret médical ». Il l'introduisait par les propos suivants : « *Le secret médical remonte à l'antiquité et s'est maintenu à travers les âges. On le trouve dans le célèbre serment d'Hippocrate et dans les statuts de la vieille faculté de médecine* »[57]. Sans attribuer à la doctrine pénaliste la fusion terminologique entre « secret médical » et « secret des professionnels de santé », l'on peut au moins admettre que le « passage » de l'éthique médicale vers le droit pénal l'a facilité. Cette difficulté peut être évincée si l'on admet que le nom du concept peut renvoyer à plusieurs concepts. Pour expliquer cette distinction, Monsieur Tusseau prend l'exemple éclairant de la notion de « service public » :

> « *Face aux différents usages du terme « service public » qui apparaissaient dans la jurisprudence, les auteurs ont soit considéré qu'il n'y avait pas (ou plus) de notion de service public, soit qu'il s'agissait d'une notion fonctionnelle. L'obsession de la recherche d'une notion unique de service public peut s'expliquer par une forme de tentation platoniste consistant à considérer qu'un même terme ne peut nommer qu'un concept. Or une fois repoussé un tel postulat, il devient parfaitement admissible de considérer que le terme « service public » désigne, dans la jurisprudence, différents concepts* »[58].

---

[56] Le secret des médecins à une essence axiologique, le devoir du médecin fait partie, depuis des millenaires de la morale médicale et certains écrit et discours de déontologues sont. Cette essence permet, il nous semble, de comprendre que les problématiques qui ont occupées et occupent encore une majorité de la doctrine portent sur la légitimité du secret professionnel, non pas quant à son existence, mais quant à sa portée et qu'il est toujours question dans les discussions doctrinales de savoir si telle ou telle limitation de la portée de ce secret est légitime, si telle ou telle limitation d'un autre intérêt par le secret est légitime. De là également les débats intenses - mais relativement vains car jamais éteints- sur les fondements du secret professionnel, entre intérêt de la personne soigné ou intérêt du professionnel. Il n'est pas possible de reproduire ici la somme des arrêts et des débats y ayant donné lieu, Emile Garçon en donne déjà un aperçu, édifiant, dans ses commentaires du Code pénal (E. GARÇON, Code pénal annoté, T. 2, Ed. refondue et mise à jour par M. ROUSSELET, M. PATIN et M. ANCEL, Sirey, Paris, 1956, art. 378). Nous ne manquerons pas de tirer de cette littérature gargantuesque ce qui nous est nécessaire au moment voulu.

[57] (E. GARCON, Code pénal annoté, *op. cit.* art. 378, p. 520, n° 121).

[58] G. TUSSEAU, « Critique d'une métanotion fonctionnelle », *op. cit.*

6. Lorsque d'autres questions se font jour. « *Toutes ces notions « claires » et « simples » qui forment la base de la science moderne ne sont pas « claires » et « simples »* per se *et* in se*, mais en tant qu'elles font partie d'un certain ensemble de concepts et d'axiomes en dehors duquel elles ne sont pas « simples » du tout* »[59]. Il en est de même pour la construction des notions juridiques et le « secret médical » n'y échappe pas. Sorti du prisme sous lequel il est pensé, son analyse se fait plus complexe. On ne peut en effet qu'être frappé par l'obscurité et les contradictions qui jalonnent le discours de la doctrine lorsqu'il s'agit d'agrandir le champ de vision pour se placer dans le cadre d'évolutions contextuelles plus générales. Sur ce point, le discours sur le « secret médical » dans le contexte des technologies de l'information et de la communication et du droit régulant leur utilisation est particulièrement malaisé. Avant de s'expliquer sur ce point, qui constitue le chemin par lequel nous avons trouvé notre question, il nous faut traiter de notre deuxième objet.

§ 2 - Le second objet : Les technologies de l'information et de la communication

7. Dans la mesure où notre étude consiste en un rapport entre deux objets, il nous faut nécessairement définir le second objet (A) et plus spécifiquement ses rapports avec le droit (B).

A - Des technologies de l'information et de la communication

8. Un accord sur les mots : des technologies de l'information et de la communication ? Le terme *technologies* et, plus précisemment en ce qui nous concerne, l'expression technologies de l'information et de la communication sont entrés dans le langage courant. L'étude de leur usage est un vaste champ d'investigation pour les sociologues[60]. Les sciences de l'information

---

[59] A. KOYRÉ, *Etudes d'histoire de la pensée scientifiques*, coll. Bibliothèque des idées, NRF-Gallimard, PUF, 1973, p. 198 : cité par C. ATIAS, *Théorie contre arbitraire*, coll. les voies du droit, PUF, 1987, n° 49.

[60] Dans le champ de la sociologie et plus largement des sciences sociales, parmi les ouvrages de référence : J. ELLUL, *Le Bluff technologique*, préf. J.-L. PORQUET, coll. Pluriel, Hachette, 2012 ; P. BRETON et S. PROULX, *L'explosion de la communication. Introduction aux théories et aux pratiques de la communication*, coll. Repères, La découverte, 2012 ; F. JARRÉGUIBERRY et S. PROULX, *Usages et enjeux des technologies de communication*, coll. Poche-société, ERES, 2011 ; C. FONTAINE, *L'empire cybernétique. Des machines à penser à la pensée machine*, Seuil, 2014 ; en sciences politique également avec une vision très critique : L. SFEZ, *Technique et Idéologie. Un enjeu de pouvoir*, coll. La couleur des idées, Seuil, 2002.

et de la communication[61] les prennent pour objet. Les technologies de l'information et de la communication sont, par exemple, définies dans le langage courrant comme : « [l'] *'ensemble des technologies issues de la convergence de l'informatique et des techniques évoluées du multimédia et des télécommunications, qui ont permis l'émergence de moyens de communication plus efficaces, en améliorant le traitement, la mise en mémoire, la diffusion et l'échange de l'information* »[62]. Toutefois, nous emploierons le moins possible le terme *technologies*. Il désigne en effet plus un discours sur les techniques que les techniques elles-mêmes[63]. S'il n'est pas utile de faire preuve d'une rigueur excessive, il faut souligner que le terme *technologies* renvoie à des « *d'objets, outils et* dispositifs *techniques permettant l'interaction à distance et une réciprocité dans la communication* »[64] ou des *objets, outils ou dispositifs techniques* permettant de traiter de l'information. Il faut noter que certaines techniques ou outils sont bien plus que cela : leur fonction ne se résume pas à communiquer ou à traiter de l'information. Ces objets sont hétéroclites. Toute tentative de classification serait spécieuse. Il apparaît que la convergence des techniques est devenue si forte que les robots, les algorithmes (comme moyen), l'intelligence artificielle - tout ces objets qu'il faudrait, pour les étudier, individuellement conceptualiser au préalable- utilisent ou se caractérisent par une fonction d'information et/ou de communication. L'on utilise parfois distinctement le terme « numérique » qui « [s]*e dit, par opposition à* « analogique », *de la représentation discrète de données ou de grandeurs physiques au moyen de caractères (des chiffres généralement)* ; *se dit aussi des systèmes, dispositifs ou procédés employant ce mode de représentation* »[65]. Le numérique est donc une façon de représenter les données. Là encore, la convergence technologique a favorisé l'effacement des frontières. Sur un plan général, ces dispositifs

---

[61] Parmi les auteurs considérés comme penseurs des sciences de l'informations et de la communication : le mathématicien Norbert Wiener à l'origine de la théorie cybernetic dont l'ouvrage emblématique est *Control & Communication in the Animal & the Machine* ; et les linguistes Harold Innis et Marschall McLuhan (M. MCLUHAN, *Understanding Media: The Extensions of Man*, Corte Madera, California, Gingko Press, 2003) ainsi que Robert Escarpit le premier a proposer une théorie des sciences de l'information et de la communication en France (R. ESCARPIT, *Théorie générale de l'information et de la communication*, Hachette Université, 1976).

[62] *V°* « Technologies de l'information et de la communication », *Office québécois de la langue française, <http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8349341>* (dernière consultation le 08 oct. 2019).

[63] « *Science des techniques, étude systématique des procédés, des méthodes, des instruments ou des outils propres à un ou plusieurs domaine(s) technique(s), art(s) ou métier(s)* », *V°* « Technologies », TLFi, *op. cit.*,

[64] S'agissant des dispostifs techniques de la communication (F. JARRÉGUIBERRY et S. PROULX, *Usages et enjeux des technologies de communication*, coll. Poche-société, ERES, 2011, p. 10).

[65] Arrêté du 22 décembre 1981 relatif à l'enrichissement du vocabulaire de l'informatique, *JORF* du 17 janvier 1982.

techniques sont parfois également nommés « *nouvelles technologies de l'information et de la communication* ». À propos de l'utilisation de l'expression « *nouvelles technologies* », Monsieur Jeanneret disqualifie tant l'emploi de l'adjectif « nouvelles » que du substantif « technologies », soulignant qu'en son temps, l'écriture était une technique nouvelle, tout comme l'imprimerie. Par où l'on voit que l'étude des techniques de l'information et de la communication s'inscrit dans le temps. L'auteur remarque encore que le terme « technologies » renforce cette idée de nouveauté. L'expression aurait, en outre, une forte connotation idéologique qui empêcherait de penser ces objets : « [le] *fait premier est que ce discours, comme toute idéologie, masque ses propres conditions de production* » [66].

9. Représentations et jugement de valeur sur les technologies de l'information et de la communication. Les productions discursives sur les *technologies de l'information et de la communication*, s'accompagnent d'imaginaires et de fictions qui peuvent devenir de véritables mythes technologiques[67]. La doctrine juridique, pas plus d'ailleurs que le législateur, n'échappe à ces représentations. Monsieur Musso explique par exemple que les rapports d'informations sont l'occasion de tenir « *un discours d'encadrement sur la société technicienne* » qui participera à la « *construction progressive de l'imaginaire social* »[68]. Monsieur Scardigli a dressé une typologie des « *rêves et frayeurs* »[69] qui caractérisent la relation des individus aux technologies de l'information et de la communication. Il distingue sept concepts qui sont au centre de cette dualité : la liberté, le savoir, la sécurité, la justice, la communication humaine, la prospérité et la solidarité[70]. Sur ces rêves et frayeurs, la société construit l'image collective

---

[66] (Y. JEANNERET, *Chapitre 2. « Nouvelles technologies de l'information » : une expression mal formée* In : *Y-a-t-il (vraiment) des technologies de l'information ?* Nouvelle édition revue et corrigée [en ligne], Presses universitaires du Septentrion, 2011 (dernière consultation le 08 oct. 2019),
Disponible sur : <http://books.openedition.org/septentrion/13904>. ISBN : 9782757419106. DOI : 10.4000/books.septentrion.13904.)

[67] V. notamment : A. MOLES, « La fonction des mythes dynamiques dans la construction de l'imaginaire social », Cahiers de l'imaginaire, n°5/6, p. 9-33, 1990 ; V. SCARDIGLI, « Nouvelles technologies : l'imaginaire du progrès », *in* A. GRAS et S. POIROT-DELPECH (ss. la dir.), *L'imaginaire des techniques de pointe. Au doigt et à l'œil*, L'Harmattan, 1989, Pp. 31-34 ; Pour une synthèse éclairante v. P. MUSSO, « Usages et imaginaires des TIC », *in* C. LICOPPE (ss. la dir), *L'évolution des cultures numériques. De la mutation du lien social à l'organisation du travail*, coll. innovation, éditions Fyp, 2009, Pp. 201-210.

[68] *Ibid.*

[69] SCARDIGLI, « Nouvelles technologies : l'imaginaire du progrès », *in* A. GRAS et S. POIROT-DELPECH (ss. la dir.), *L'imaginaire des techniques de pointe. Au doigt et à l'œil*, L'Harmattan, 1989, Pp. 50-51

[70] *Ibid.*

de ces techniques. Le mythe du « *Big Brother informatique* » ou à l'inverse celui de la protection des biens et personnes par la surveillance en sont des exemples[71]. Il faut noter que les autres discours en sciences sociales ne sont pas exempts de ces biais. Nous pouvons par exemple souligner que Monsieur Mucchielli, précédemment cité, s'inscrit dans une approche des technologies de l'informations et de la communication héritée de l'Ecole de Palo-Alto fondée par les pères de la pensée cybernétique[72].

10. Outre ces aspect, l'usage d'un terme moins connoté permet de garder à l'esprit que ces dispositifs relèvent d'abord du fait ; que comme le droit, ils sont des techniques ; que ces dispositifs n'ont pas tous la même fonction. Nous développerons ces trois points successivement car ils permettent d'expliquer les rapports entre *droit et technologies* tels qu'ils sont traditionnellement présentés.

B - Les interactions entre droit et technologies de l'information et de la communication

11. Les technologies saisies par le droit. Les innovations scientifiques et leur mise en œuvre, les techniques[73], sont de l'ordre du fait[74]. L'une des manifestations des rapports entre « techniques » et « droit » est donc classiquement présentée par la formule selon laquelle une

---

[71] A. MUCCHIELLI, « introdution », *Les sciences de l'information et de la communication*, 4e éd., coll. Les Fondamentaux ; sous-coll. Sciences Humaines, Hachette Supérieur, 2006.

[72] La théorie cybernetique forgée par les premiers chercheurs, dont particulièrement Norber Wiener auquel l'on attribue sa paternité, de l'Ecole de Palo-Alto est d'abord interdisciplinaire. Elle réunit des mathématiciens, des sociologues, des psychologues, des économistes, des linguistes (parmi les plus illustres figure notamment Grégory Bateson, Norbert Wiener et Claude Shannon). Comme l'explique Madame Lafontaine, le choix du terme cybernetique est marqué par la volonté de Norbert Wiener de mettre « *l'accent sur le contrôle communicationnel* » il s'agit de « *suppléer aux faiblesses humaines en créant une machine capable de contrôler, de prévoir* » afin de « *lutter contre la désorganisation et le chaos qui menacent la société* » raison pour laquelle l'entropie qui est au centre de la théorie cybernétique conçoit la communication comme « *la source de toute organisation* », la vie est « *au principe informationnel* » (Céline Lafontaine, *L'empire cybernétique. Des machines à penser à la pensée machine*, Seuil, Pp. 40-43).

[73] La science étant de l'ordre de la connaissance du monde, la technique est sa réalisation. C'est le lien qu'opère Auguste Compte entre savoir pour prévoir, prévoir pour pouvoir. En caricaturant quelque peu, le savoir est la science, sa finalité est de prévoir tandis que le pouvoir, la technique, permet la réalisation : *« A l'une, il appartient de connaître et par suite de prévoir ; à l'autre, de pouvoir et par suite d'agir* » (A. COMTE, Cours de philosophie positive : première et deuxième leçon (cours en 72 leçons dispensés en 1926-1927 et publiées en 1830). Le document est accessible en version numérique (et non numérisée) sur <http://classiques.uqac.ca/classiques/Comte_auguste/cours_philo_positive/cours_philo_positive.html> (la citation est issue du document word, p. 64).

[74] Or l'objet même du droit est de régir le réel, les faits : L. LEVENEUR, « Le fait », *Arch. phil. dr.* 1991, T. 35, *Vocabulaire fondamental du droit*, p. 143.

chose, une technique, un objet du réel est « *saisi par le droit* ». Soit que le droit commun s'y applique, soit qu'il nécessite une adaptation à cette fin. L'adaptation du droit au fait serait pour la majorité de la doctrine une nécessité[75]. L'adaptation du droit aux sciences, techniques et aux objets qu'elles poduisent est en tout cas une constante[76]. Comme le remarque Monsieur Terré : « [d]*ans tous les domaines du savoir, on a vu les répercussions juridiques des découvertes scientifiques* »[77]. C'est que « *les nouvelles techniques génèrent nécessairement de nouvelles questions juridiques* »[78] et chaque question emporte une réflexion sur les modalités d'innovations du droit, de l'adaptation des règles existantes à la création de règles spécifiquement pensées pour encadrer ces faits alors, « nouveaux »[79]. S'agissant des techniques de l'information et de la communication, le droit commun s'applique généralement à leurs usages, bien qu'il nécessite parfois quelques aménagements. Pour l'internet qui peut être un « *support parmi d'autres d'expression et de diffusion de la pensée, d'informations, d'images, de sons* »[80], Madame Lepage constatait « *l'œuvre d'innovation et la part de tradition* »[81]. L'on connait également les applications et adaptations dont à fait l'objet le droit de la preuve en matière civile[82]. Ces techniques ont généré de nouvelles questions juridiques dans tous les

---

[75] Sur les disputes doctrinales à ce sujet v. D. LOUIS-CAPORAL, La distinction du fait et du droit en droit judiciaire privé, Th. dact., ss. la dir. de M.-L. MATHIEU, soutenue le 21 novembre 2014, Université Montpellier I.

[76] C.-A. COLLIARD, *La machine et le droit privé français contemporain*, *in Le droit privé français au milieu du XX^e siècle. Études offertes à Georges Ripert*, T. 1, LGDJ, 1950, p. 115 ; M.-A. HERMITTE, *La fondation juridique d'une société des sciences et des techniques par les crises et les risques*, *in Pour un droit commun de l'environnement, Mélanges en l'honneur de Michel Prieur*, Dalloz, 2007, p. 145 et s. ; L. WATRIN, *Les données scientifiques saisies par le droit*, th. dact., ss. la dir. de M.-E. PANCRAZI, soutenue le 9 déc. 2016, Université d'Aix-Marseille.

[77] F. TERRÉ, « Présentation », Arch. phil. dr. 1991, *Droit et science*, p. 5.

[78] V. LASSERRE, *Le nouvel ordre juridique. Le droit de la gouvernance*, LexisNexis, 2015, n° 12.

[79] Par exemple : I. DE LAMBERTERIE, « L'adaptation du droit au progrès technologique : l'exemple de la protection des logiciels », *Arch. phil. dr.*, p. 155 et s. ; v. également *Etudes à la mémoire du professeur Xavier Linant de Bellefond*. *Droit et technique,* Litec, 2007 ; Rapport de la Cours de cassation, *L'innovation technologique*, 2005, disponible sur < https://www.courdecassation.fr/IMG/pdf/cour_cassation-rapport_2005-3.pdf> (dernière consultation le 9 oct. 2019) ; De nombreux articles également, dont par exemple en propriété intellectuelle : J. AZEMA, « Modernisation et adaptation du droit des brevets en Europe », *RTD com.* 2000, p. 79 ; en droit du travail : C. RADÉ, « Nouvelles technologies de l'information et de la communication et nouvelles formes de subordination », *Droit social* 2002 p.26 ; ou encore en droit pénal spécial : A. LEPAGE, « Droit pénal et internet : la part de la tradition, l'oeuvre de l'innovation », *AJ pénal* 2005, p. 217 ; en témoigne encore, par exemple.

[80] *Ibid.*

[81] Elle relève par exemple les nécessités d'adaptation engendrées par des difficultés d'application du droit de la presse, l'excès de rigueur de certains textes ou les problèmes lié à l'application de la loi dans l'espace à l'internet qui, par nature, ne connait pas les frontières (*Ibid.*).

[82] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

domaines, en droit de la propriété intellectuelle par exemple[83], ou encore en droit commercial[84]. La question de l'application et de l'adaptation potentielle du droit civil à la robotique[85], de toutes les branches du droit à l'intelligence artificielle[86], est aujourd'hui largement investie par les juristes. La question du traitement des données y figure en bonne place[87].

12. Le droit saisi par la technique. Si le droit saisit les techniques, la relation ne serait toutefois pas unilatérale : « *le droit et la technique s'enchevêtrent de plusieurs manières* »[88]. Les techniques saisiraient également le droit, par exemple, « *lorsque le droit se décharge de sa fonction arbitrale traditionnelle et doit se baser sur des connaissances scientifiques pour parvenir à une décision* »[89] ou encore « *lorsque le Gouvernement par des mécanismes légaux, des décisions de l'exécutif et des contrats, sélectionne des buts scientifiques et maximise les contributions de la communauté scientifique* »[90].

13. Une concurrence. Le droit et les techniques entretiennent une relation non seulement en ce que le droit est également une technique[91] mais surtout en ce que les dispositifs techniques peuvent être des techniques de régulation des conduites au même titre que le droit lui-même[92]. C'est notamment ce que développe Monsieur Ost à l'occasion de son ouvrage *A quoi sert le*

---

[83] V. par exemple concernant des techniques que l'on ne qualifierait plus, aujourd'hui, de nouvelles : R. LEGEAIS, « Le droit d'auteur face aux nouvelles technologies », *RIDC* 1990, n° 42-2 , Pp. 677-692 ; Plus proche de notre époque

[84] V. par exemple O. CACHARD, *La régulation internationale du marché electronique*, Préf. de Philippe Fouchard, coll. Bibliothèque de droit privé, T. 365, LGDJ, 2002.

[85] X. DELPECH, « Vers un droit civil des robots », *AJ contrat* 2017, p.148 ; A. BENSAMOUN, « La personne robot », *D.* 2017, p. 2044 ; N. DEVEJEANS, *Traité de droit et d'éthique de la robotique civile*, coll. Science, éthique et société, LEH, 2017.

[86] V. notamment A. BENSAMOUN et G. LOISEAU (ss. la dir.), *Droit de l'intelligence artificielle*, coll. les intégrales, Vol. 15, LGDJ, 2019.

[87] A. DEBET, « Intelligence artificielle et données à caractère personnel », *in* A. BENSAMOUN et G. LOISEAU, *Ibid.*

[88] Cité par V. LASSERRE, *Le nouvel ordre juridique. Le droit de la gouvernance*, *op. cit.*, n°12. : R. SAVATIER, *Les métamorphoses économiques et sociales du droti civil aujourd'hui. L'universalisme renouvelé des disciplines juridiques,* 2ème éd., *Dalloz*, 1959, p. 49.

[89] Cité et trad. par V. LASSERRE, *ibid.* : D.-F. CAVERS, « Law and Sciences : Some Points of Confrontation », *in* H.-W. Jones (ss. la dir.), *Law and the social role of science*, The Rockefeller Universtity Press, 1966, p. 6.

[90] *Ibid.* Sur ce point, mais traitant particulièrement de la biomédecine, l'on pourra notamment se référer à la thèse de Monsieur Binet : J.-R. BINET, *Droit et progrès scientifique. Science du droit, valeurs et biomédecine*, coll. Partage du savoir, Le Monde-PUF, 2002.

[91] S'agissant du droit on se réfèrera évidemment à François Geny : F. GENY, *Science et technique en droit privé positif*, Sirey.

[92] « *De même qu'il ne suffit pas de dire qu'une pelle est un outil pour comprendre ce qu'est une pelle, il ne suffit pas de dire que le Droit est une technique pour comprendre la place qui est la sienne dans le vaste univers des techniques* » (A. SUPIOT, « Travail, droit et technique », *Droit social* 2002, p. 13).

droit ? Usages, fonctions, finalités[93] au sein duquel il explique notamment que certaines finalités classiquement assignées au droit (la justice, la démocratie et « *l'institution de l'humain* »[94]) peuvent être poursuivies par d'autres dispositifs également normatifs. Ces dispositifs ainsi que le droit sont en « *lutte pour le contrôle globale de la culture* »[95]. Si certains dispositifs sont connus, tels que la religion, la morale, la politique, Monsieur Ost souligne qu'à coté des discours normatifs s'observent « *les formes d'une régulation normalisatrice* »[96]. Il distingue parmi d'autres « *la normalisation par les dispositifs techniques inscrit dans les choses elles-mêmes (sur le modèle des ralentisseurs de vitesse ou des procédures obligées inscrites dans les logiciels d'ordinateurs)* »[97]. Au-delà des « interactions » entre le droit et les techniques, il pourrait donc également être observé une « concurrence » entre le droit et les techniques normalisatrice que peuvent constituer les outils de l'information et de la communication.

14. Les contours des objets de notre étude étant esquissé, il faut désormais présenter le chemin que nous avons suivi jusq'à notre sujet.

§ 3 - Le sujet : l'impact des techniques de l'information et de la communication sur le secret médical

15. Le discours sur le secret médical et les technologies de l'information et de la communcation en droit. Nous avons remarqué plus avant que le droit saisît la technique. C'est pourquoi certaines règles juridiques s'appliquent classiquement aux dispositifs techniques de l'information et de la communication, tandis que d'autres ont été adaptées[98]. Un ensemble de

---

[93] F. OST, *A quoi sert le droit ? Usages, fonctions et finalités*, coll. penser le droit, Brulant, 2016.
[94] « *Quant à l'« institution de l'humain », je la définis, en toute première approximation, par l'accès au langage et à l'odre du symbolique, du tiers institué, de la loi commune, et finalement de l'interdit et de la limite. Toutes ces réalités, qui font système, n'ont pas pour but d'enfermet l'homme dans un carcan, mais au contraire, de lui assurer identité et autonomie, de le préserver du fantasme d'être tout (et notamment l'auteur de la loi), de le garder ainsi de la folie et de la violence – bref de l'équiper pour activer, comme un être libre, le lien social qui le constitue* » (*Ibid.* p. 97).
[95] *Ibid.* p. 104 et svt.
[96] *Ibid*. p. 300.
[97] *Ibid.*
[98] L'adaptation peut revetir la forme d'une modification des textes légaux ou règlementaires, elle peut également être jurisprudentielle. L'on observe par exemple que certaines fonctions des dispositifs techniques de l'information et de la communication et notamment la possibilité de dissocier le support de l'information qui la représente ont permis au juge pénal de sanctionner l'appropriation frauduleuse d'informations ou de données (G. BEAUSSONIE,

règles a en outre été créé et s'applique spécifiquement au traitement des données à caractère personnel[99] dont les données de santé constituent une catégorie particulière. La rencontre entre le « secret médical » présenté comme un droit de la personne et les technologies de l'information et de la communication pourrait donc être appréhendé par les règles juridiques de droit commun. La question de leur confrontation serait en quelque sorte subsumée sous celle de l'application des règles relatives à la protection de la vie privée et de celles qui sont propres aux traitements des données à caractère personnel. Par ailleurs, l'usage des dispositifs de l'information et de la communication comme moyen de révélation ne recèle aucune particularité. Malgré cette apparente simplicité, le discours sur le droit semble souvent manquer son objectif qui est, en premier lieu, de permettre d'accéder à la connaissance du droit.

16. L'accès à une connaissance du sujet est sans doute rendu plus difficile par l'emploi de l'expression « secret médical » sans qu'aucun regard ne soit porté sur la polysémie du mot « secret ». Le malaise dû aux mots témoigne également des difficultés d'appréhension du sujet. En 1995, Monsieur Dubouis entreprenait une étude intitulée « *Feu le secret médical* »[100], à l'occasion de laquelle il expliquait que le « secret médical » était un droit du malade de « *seconde catégorie* »[101] en raison de la multiplication des fichiers. Il affirmait néanmoins qu'il demeurait « *un principe essentiel de notre droit. Mais un principe rongé par la double incertitude de son fondement et de ses limites* »[102]. Comment le « secret médical » pourrait-il à la fois occuper une place centrale et être rongé de toutes parts ? Ce qui est « rongé », si tant est qu'un concept puisse l'être, n'est-il pas voué à disparaître ? Toujours au sein de la doctrine du droit public, un auteur affirmait que la reconnaissance d'un fait justificatif spécial permettant aux médecins de transmettre des données de santé aux chercheurs. Cela constituait, selon lui, une manière de « *contourner le secret médical qui apparaît comme un obstacle au*

La prise en compte de la dématérialisation des biens par le droit pénal. Contribution à l'étude de la protection pénale de la propriété, Préf. de B. DE LAMY, coll. Bibliothèque de droit privé, T. 532, LGDJ, 2012, *spéc.* sur « information et informatique » v. n° 40, mais également sur l'ordinateur comme « bien contenant », n° 520 et svt.

[99] la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (plusieurs fois modifiées) et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[100] L. DUBOUIS, « Feu le secret médical ? », *in Mélanges en l'honneur du Professeur Gustave Peiser*, coll. Droit public, Presses Universitaire de Grenoble, 1995, p. 201.

[101] *Ibid.* p. 209.

[102] *Ibid.* p. 214.

développement des fichiers de santé publique »[103]. Plus récemment, un auteur constatait dans un article intitulé « *Confidentialité des données de santé* »[104] que « *le secret médical est à l'heure actuelle une règle parfaitement établie en droit. Depuis 1978, il bénéficie dans le domaine informatique d'une protection qui n'a cessé de se préciser* » pour expliquer peu après qu' : « [a]*u-delà des apparences, le secret médical se trouve en réalité dans une situation paradoxale. Alors que son principe a fait incontestablement l'objet d'une protection accrue dans le domaine informatique depuis quelques années, il apparaît qu'au nom des impératifs de la santé publique son aménagement juridique soit en passe de connaître une interprétation extensive qui le rend pour le moins incertain* »[105]. L'on ignore donc ce qui fait l'objet d'une protection ou d'un aménagement. Surtout, pourquoi ce discours semble traverser les époques ?

17. L'on peut selectionner quelques exemples de propos tenus en ce sens. Il est en effet soutenu, dans le même temps, un affaiblissement de la portée du secret professionnel médical en raison de la nécessaire circulation des données[106] et une redéfinition de celui-ci en raison de cette même circulation[107]. Qui redéfinit ? Au regard de quoi peut-on affirmer que le secret professionnel est redéfini ? L'utilisation de la formulation interrogative « [q]*ue reste-t-il de la protection pénale du secret médical ?* »[108] dans un article consacré au secret professionnel des personnes intervenant dans le système de santé interroge. Le *secret médical* est-il l'objet de la protection pénale ? En est-il le moyen ? Ou encore à l'occasion d'un article portant sur le secret professionnel médical intitulé « *Que reste-t'il du secret médical ?* »[109], il est consideré comme pertinant de « *forger un nouveau concept* »[110]. À l'appui de cette proposition l'auteur remarque le « *glissement contemporain des centres d'intérêt du droit positif en matière de protection des informations relatives aux malades* »[111] vers « *la protection de la confidentialité des informations de santé ou des données de santé* »[112]. En quoi un tel glissement justifie t-il de

---

[103] M.-C. PONTHOREAU, « La protection des personnes contre les abus de l'informatique », *RFDA* 1996, p. 796.
[104] P. SEGUR, « La confidentialité des données médicales », *AJDA* 2004, p. 858.
[105] *Ibid.*
[106] M. BENEJAT-GUERLIN, « Que reste-t-il de la protection pénale du secret médical ? », *AJ Pénal* 2017 p.368 ;
[107] *Ibid.*
[108] *Ibid.*
[109] M. COUTURIER, « Que reste-t-il du secret médical ? », *op.cit.*
[110] *Ibid.* p. 368.
[111] *Ibid.*
[112] *Ibid.*

forger un nouveau concept ? La confidentialité des données de santé a-t-elle le même objet que le secret professionnel ? Encore, à la lecture de cette question « [l]*e secret médical et les données personnelles sont-ils déclarés inviolables, tandis que le secret bancaire doit être éradiqué ?* »[113] apparaissent nécessairement d'autres questions : Pourquoi « secret médical » et *données personnelles* sont-il mis sur un même plan d'analyse ? Que doit-on entendre par inviolabilité ? A propos de l'*open data* dans le domaine de la santé on peut par exemple lire que certaines hésitations du législateur à l'ouverture de l'accès était imputable à la crainte d'atteinte « *à la vie privée et au secret médical, le risque de ré-identifiction du titulaire des données restant en effet toujours présent* »[114] : comment comprendre l'accumulation des deux expressions « vie privée » et « secret médical » ? En quoi la réidentification des données constitue-t-elle une atteinte au « secret médical » ? En introduction d'une étude sur « *la confidentialité des informations de santé* »[115], l'on peut lire que « [l]*e principe de confidentialité des données de santé est plus que jamais affirmé dans les textes nationaux. Le secret sur les données de santé est maintenant placé au rang des droits des personnes* »[116]. Secret et confidentialité sont-ils synonymes, et dans quel cadre de référence ? « *Secret des données de santé* » et « *secret médical* » sont-il également des synonymes ? Est-ce le même concept qui apparaît ? Mais ce qui transparaît surtout, c'est qu'à l'affirmation selon laquelle le « secret médical »*, des données de santé, des informations en santé* est protégé par le droit, est opposé le propos selon lequel le « secret médical » serait entrain de *disparaître, de s'affaiblir*. De plus en plus de travaux relatifs au « secret médical » octroient une place importante à la circulation des données (parfois dénommées « données médicales » ou « données de santé »[117]). Les exemples sont légion. Il apparaît néanmoins que la différenciation entre le nom de la notion et les notions auxquelles elle renvoie pourrait s'avérer fort utile pour analyser le discours de la doctrine.

---

[113] O. DE MAISON ROUGE, « Décryptage sur la protection juridique des informations sensibles », *Dalloz IP/IT* 2017, p. 273.
[114] L. MORLET-HAIDARA, « Le système national des données de santé et le nouveau régime d'accès aux données », *RDSS* 2018, p. 91.
[115] C. BERGOIGNAN-ESPER, « La confidentialité des informations de santé peut-elles tenir face à la protection d'autres intérêts légitimes ? », *D.* 2008, p. 1918.
[116] *Ibid.*
[117] Utilisant successivement et indifféremment les expressions « données de santé » et « données médicales », « secret médical » et « confidentialité » (C. BERGOIGNAN-ESPER, « Fasc. 14 : SECRET MÉDICAL. – Particularités en établissements publics de santé », *Feuillets mobiles Litec Droit médical et hospitalier*, 17 janv. 2012 (dernière modif. Le 3 mars 2016).

18. À cela s'ajoute le discours des déontologues, des spécalistes en science politique et des économistes : « *Le Cnom rappelle que la préservation du secret médical couvrant les données personnelles de santé doit être appliquée aux traitements des données massives et que leur exploitation ne doit pas permettre l'identification d'une personne, au risque de conduire à des discriminations* »[118]. Dans un article publié par un éditeur juridique : « *le secret médical est caduc et [il] vaudrait mieux en prendre son parti : le secret est partagé par les équipes, les données sont entrecroisées, il est battu en brèche par les pratiques de l'épidémiologie, de la santé publique, des études génétiques... Il s'oppose au progrès* »[119]. Également « *dans un contexte de médecine technicienne, faisant appel à des disciplines diverses, pourvoyeuses de données médicales sensibles, le tout associé à un développement de l'informatisation (réseau, télémédecine...), le partage de l'information peut cependant apparaître à haut risque : malgré la réaffirmation du principe du secret médical, celui-ci apparaît comme une gageure* »[120]. L'on peut encore citer « *Le développement de ces technologies nouvelles n'est bien sûr pas sans risque pour le secret médical. Les indiscrétions sont toujours possibles, la négligence peut être à l'origine de fuites aux conséquences parfois très importantes compte tenu de la masse de données qui peuvent être transmises ou détournées instantanément, l'intrusion délictuelle est un risque à ne pas négliger* »[121]. À propos de l'information médicale comme outil de pilotage des établissements de santé il a par exemple été écrit que « *Des questions sur les conditions d'accès et la préservation du secret médical se posent* »[122] dans le cadre de demandes d'accès aux données traitées par les établissements.

19. À l'inverse, dans les manuels de droit spécial concernant le droit à la protection des données, le rapport avec le « secret médical » est souvent éludé[123]. Il est par contre fait une

---

[118] CNOM, *Médecins et patients dans le monde des data, des algorithmes et de l'intelligence artificielle*, Analyses et recommandations, Janv. 2018, p. 60.
[119] A. KAHN, « Le secret médical : d'Hippocrate à internet », *D.* 2009, p. 2623.
[120] D. HOUSSIN, « Le secret médical dans les nouvelles pratiques et les nouveaux champs de la médecine », *D.* 2009, p. 2619.
[121] F. STEFANI, « Le secret médical à l'épreuve des nouvelles technologies », *D.* 2009, p. 2636.
[122] C. RIOU, J. FRESSON, G. MADELON (*et alii*), « Information médicale et pilotage des établissements de santé », *Journal de gestion et d'économie médicale*s 2016/1, Vol. 34, p. 45 à 64.
[123] Par ex. F. MATTATIA, *Le droit des données personnelles*, 2e éd., EYROLLES, 2016 ; Ne l'éludant pas mais utilisant successivement l'expression « secret médical » et « secret professionnel » sans distinguer le nom de la notion et la notion elle-même. ; Evoquant le « secret médical », toujours dans le cadre de la protection des données à caractère personnel sans expliquer le sens du syntagme : A. DEBET, J. MASSOT et N. METALLINOS (ss. la

place plus importante au secret professionnel mais cela s'explique notamment en ce que la loi informatique et libertés[124] et le Règlement général sur la protection des données à caractère personnel[125] connait des articulations avec le secret professionnel[126]. Par ailleurs, dans le vocabulaire spécifique de la protection des données à caractère personnel, la « confidentialité » désigne un moyen de protection des données. Les études de droit spécial font souvent l'économie d'une réflexion sur ce que recèle la synonymie et la polysémie de ces termes pour se consacrer uniquement à l'étude de la « confidentialité des données de santé ». L'étude des rapports avec le « secret médical » est donc démembrée et partielle. Lorsqu'elle est entreprise, l'on ne peut que constater son insuccès. L'outil méthodologique consistant à distinguer le nom du concept lui-même du concept s'avère là encore pertinent.

20. La doctrine de la Cnil. En tant que régulateur de l'activité de traitement des données à caractère personnel la Commission nationale de l'informatique et des liberté (Cnil) a pour principale mission de veiller *a priori* – bien que ce soit de moins en moins le cas – et *a posterori* au respect des dispositions relatives à la protection des données[127]. Pour ce faire elle est amenée à interpréter d'autres dispositions spéciales dont les champs d'application recoupent celui des dispositions relatives à la protection des données à caractère personnel. Ce faisant, elle en propose une articulation. Vis-à-vis des traitements mis en œuvre par l'Etat et ses démembrements, son contrôle est toutefois relativement restreint. Par ailleurs, au travers de sa mission d'information[128], elle est à l'origine d'une production discursive portant sur ses positions à l'égard du droit positif et sur la façon dont elle l'interprète. Enfin et surtout, elle produit des instruments de droit souple[129]. Ses décisions, le discours qu'elle produit sur la matière qui l'occupe ainsi que ses instruments sont des supports d'analyse essentiels pour mettre en parallèle les évolutions de ses raisonnements et celles du droit positif. Il apparaît

---

dir.), *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, coll. les intégrales, Lextenso, Vol. 10, 2015.

[124] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (plusieurs fois modifiées).

[125] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[126] Le premier, à notre connaissance, à en avoir proposé une étude sous l'angle du droit pénal spécial : J. FRAYSSINET, *Informatique, fichiers et liberté*, Litec, 1992 ; J. FRAYSSINET, « Un concurrent associé du secret professionnel : le droit de la confidentialité du traitement des données personnelles », *Revue juridique de l'Ouest* 2000, numéro spécial : *Les médecins libéraux face au secret médical*, Pp. 23-46.

[127] LIL art. 8 et art. 19 à 23.

[128] LIL art. 8.

[129] LIL art. 8 2° b).

qu'elle fait référence au « secret médical » de manière continue au travers de toutes ses productions qui n'ont toutefois jamais fait l'objet d'une analyse approfondie.

21. Les énoncés normatifs. Nous avons jusqu'ici principalement évoqué le discours de la doctrine mais n'avons pas posé notre regard sur les énoncés normatifs. Il apparaît d'abord que l'expression « secret médical » figure à de nombreuses reprises dans le Code de la santé publique et de manière encore plus importante dans des textes non codifiés[130]. L'on constate que la majorité des énoncés faisant référence au « secret médical » ont vocation à organiser le partage et l'échange des données. Il est également un certain nombre d'énoncés qui font référence à *l'accès* aux données. Il s'agit, en toutes hypothèses de mécanismes prévoyant les conditions de circulation des données. Ils meritent nénmoins une analyse différenciée, le *partage* et l'*échange* renvoyant au régime du secret professionnel tandis que l'*accès* est une notion « *traditionnellement associée au droit public* »[131]. Plusieurs arguments peuvent appuyer l'intérêt d'une telle étude.

22. En premier lieu, les énoncés normatifs du Code de la santé publique, comme d'autres ensembles de dispositions régulant des secteurs particuliers, sont souvent techniques et leur rédaction peut s'avérer de faible qualité[132]. L'on constate, en ce sens, la multiplication des renvois d'un texte à l'autre[133], concernant la circulation des données, entre le Code de la santé publique et le Code pénal d'une part, et la loi informatique et libertés, le Code de la santé publique et le Règlement relatif à la protection des données d'autre part. Cela a pour conséquence de rendre la règle moins accessible. Outre la qualité rédactionnelle des textes, il faut souligner, s'agissant des textes relatifs à la circulation des données, le phénomène désigné

---

[130] Une recherche sur le moteur de recherche de *Légifrance.fr* permet de se faire une idée de l'importance des occurrences mais, s'agissant des occurrences dans les Codes, ce type de recherche n'est pas suffisamment exclusive. En entrant l'expression « secret médical » dans le moteur de recherche celui-ci renvoi parfois à des textes utilisant, dans le même énoncé, les mots « secret » et « médical » et relève 166 occurences. Ce qui n'est pas significatif. Par contre, lorsque l'on cherche l'expression exacte au sein des textes législatifs et règlementaires l'on en trouve 333 occurrences exactes.

[131] *V°* « Accès (enjeux pratique) », *in* M. CORNU, F. ORSI et J. ROCHFELD, *Dictionnaire des biens communs*, coll. Quadrige, PUF, 2017.

[132] C'est notamment ce que remarque Monsieur Mistretta s'agissant du droit pénal médical au sein du Code de la santé publique mais ce constat s'étend à de nombreux textes du Code de la santé publique (P. MISTRETTA, *Droit pénal médical*, Éd. Cujas, 2013, n° 52).

[133] « […] *le renvoi externe soulève un problème d'accès à la règle, exigent du lecteur qu'il dispose des sources d'information évoquées par le texte initial* » (N. MOLFESSIS, « Le renvoi d'un texte à l'autre », *Les mots de la loi*, coll. Études juridiques, Economica, 1999, p. 69).

par Madame Lasserre comme une « technicisation » ou « scientifisation » du droit. Il traduirait « *l'impact des sciences et des techniques sur le système juridique et sa transformation subséquente* »[134]. L'auteur remarque encore que cette influence serait imputable à « *l'extrême technicité d'innombrables domaines juridiques qui subordonnent inévitablement le droit aux experts et génèrent des lois techniciennes ; sans parler du technicisme formel de lois qui ajoute au vice de technicité* »[135]. Cet ensemble d'éléments rend leur étude complexe et insuffisamment investie.

23. En deuxième lieu, le législateur « *exerce son pouvoir normatif sans se soucier des significations différentes que les traditions, les expériences et pratiques passées pourront donner aux mots qu'il emploie, aux notions, aux principes qu'il consacre* ». Le juge fait de même[136]. L'utilisation de l'expression « secret médical » par le législateur ou par le juge ne doit donc pas être comprise au prisme des concepts forgés par la doctrine. Il convient également de porter un regard sur le contexte des phrases dans lesquelles est employée l'expression « secret médical » afin de considérer sa signification. Sa signification peut être différente d'un contexte à l'autre. L'auteur qui n'y porterait pas attention pourrait se poser les mauvaises questions et apporter des réponses vaines. D'où l'intérêt de différencier, par exemple, le contexte d'une autorisation d'accès à un traitement de données, de celui du partage et de l'échange de données.

24. En troisième et dernier lieu, l'utilisation de l'expression « secret médical » peut constituer une ressource argumentaire pour le juge et le législateur. Si la rhétorique est principalement mobilisée par les juristes[137], elle n'est pas absente des méthodes du législateur. Comme a pu le souligner Madame Frison-Roche, « *la loi tient elle aussi sa légitimité de sa capacité à convaincre ses destinataires* »[138] car si elle « *campe sur son autorité formelle, elle ne pourra que se compliquer* »[139]. N'y a-t-il d'expression plus évocatrice et symbolique que celle de *secret médical* lorsque le principal destinataire de la norme est le professionnel de santé ? Il convient de l'avoir à l'esprit lorsqu'il s'agit d'analyser les textes et la jurisprudence.

---

[134] V. LASSERRE, *Le nouvel ordre juridique*. *Le droit de la gouvernance*, LexisNexis, 2015, n° 15.
[135] *Ibid.* V. également le numéro consacré à ce thème : *Les lois techniciennes*, *LPA*, 5 juill. 2007, n° 134 ; B. OPPETIT, « L'omnipotence technocratique et eurocratique », *in* B. OPPETIT, *Droit et modernité*, PUF, 1998, p. 31 et s.
[136] C. ATIAS, *Questions et réponses en droit*, coll. L'interrogation philosophique, PUF, 2009, p. 172.
[137] C. PERELMAN, *Logique juridique. Nouvelle rhétorique*, 2ème éd., coll. Méthodes du droit, Dalloz, 1979.
[138] M.-A. FRISON-ROCHE, « La rhétorique juridique », *in Argumentation et rhétorique (II)*, *Hermès, La Revue*, 1995, n° 16, p. 80.
[139] *Ibid.*

25. La question. Quel est l'impact des techniques de l'information et de la communication sur le « secret médical » ? C'est la question que nous avons investie au travers de cette étude. Le « pourquoi » de cette question ressort de nos développements précédents : elle est, certes, posée dans la production doctrinale. Mais l'absence de distinction entre le nom de la notion et les notions qu'elle désigne conduit bien souvent à des raisonnements circulaires et masque la question épistémologique. Cette dernière consiste à savoir ce que révèle le mouvement de fond qui fait pressentir que le « secret médical » est à la fois « protégé » par le droit et « atteint » par les techniques de l'information et de la communication. La définition classiquement admise du « secret médical » constitue un écran qui rend le mouvement à l'œuvre difficilement perceptible. C'est ce qui nous conduit à exposer notre démarche.

§ 4 - La démarche : Une distinction entre *objets* et *moyens*

26. L'inatteignable neutralité axiologique ? Nous avons expliqué les imaginaires et les mythes relatifs aux techniques de l'information et de la communication. La doctrine juridique est évidemment susceptible de déposer, dans son discours, des représentations de tous ordres. Ces représentations emportent bien souvent des prises de positions axiologiques, c'est-à-dire des jugements de valeur départageant entre le bien et le mal, le juste et l'injuste. Nous avons donc essayé, tout au long de notre démarche, de nous défaire des représentations habituelles afin que notre discours ne verse pas dans la critique des techniques ni à l'inverse dans un enthousiasme toute aussi partial. Cela ne nous interdit pas de faire référence aux discours les dont l'orientation axiologique est évidente afin de les souligner, nous ne les ferons pas nôtre pour autant. Mais, ainsi que le remarquait Monsieur Chevallier, derrière les postures intellectuelles, qu'elles soient doctrinales ou scientifiques[140], le juriste exprime toujours un point de vue « *qui comporte nécessairement une dimension subjective et est indissociable d'un ensemble de références, de valeurs présentes de manière explicite ou latente* »[141]. Nous ne sommes pas, quoi que l'on fasse, vierge de toute représentation. La dimension subjetive ne peut être totalement évacuée.

---

[140] Qu'il se considère comme prenant part à la construction du droit ou qu'il opère une distance avec son objet.
[141] J. CHEVALLIER, « Juriste engagé(e) ? », *in* V. CHAMPEIL-DESPLATS, N. FERRE (ss. la dir.), *Frontière du droit, critique des droits*, LGDJ, Coll. Droit et Société, 2007, Pp. 305-310.

27. Une analyse critique est en outre possible dès lors que l'on prend la distance nécessaire avec, d'une part, le discours sur le droit et d'autre part les énoncés normatifs. Distance nécessaire mais qui n'exclut pas de se référer aux concepts et classifications développées par la doctrine[142] car c'est par eux que l'étude est possible. Cette posture est nécessaire dans notre cas puisque nous ne prendrons pas appui sur la définition classiquement admise du « secret médical ». Proposer une analyse rénovée de notre question implique de distinguer le nom du concept et ce qu'il recouvre. Pour cela il nous faut mettre à la marge, sans l'ignorer, la sempiternelle interrogation relative au(x) fondement(s) du « secret médical ». Ces choix nous semblent devoir emporter une conséquence purement formelle : le syntagme « secret médical » sera toujours utilisé entre guillemets. Il en résulte également le besoin de trouver un autre cadre de pensée.

28. **Annonce de plan.** La distinction générale que la doctrine opère entre secret « objet » et secret « moyen » se prête à notre entreprise en ce qu'elle est suffisament générale pour nous offrir une certaine liberté de pensée mais également suffisamment précise pour que cette pensée ne se perde pas. Elle est d'autant plus adaptée que les dispositifs techniques sont également des « objets » saisis par le droit et des « moyens », eu égard à leur fonction comme instruments de l'Etat et à leur caractère normalisant. Le secret se trouve ainsi être successivement objet (**Partie 1**) et moyen (**Partie 2**).

[142] « *La sédimentation juridique est aussi le phénomène qui donne sens aux règles et aux notions juridiques. Par elle, leurs possibilités, leurs potentialités, sont tenues en attente de l'espèce qui fait surgir ou prévaloir telle strate oubliée ou estompée* » (C. ATIAS, *Questions et réponses en droit*, *op. cit.*, n° 353).

PARTIE I - LE SECRET COMME OBJET

29. Nous nous proposons d'envisager les rapports entre le « secret médical » et les technologies de l'information et de la communication. Ces dernières peuvent être employées pour percer le « secret », mais également pour le révéler. Cette distinction est classique[143] et emporte une réflexion, *a priori*, tout aussi classique, sur l'adaptation des règles juridiques à ces modes d'immixtion et de révélation du secret, objet protégé par le droit. Toutefois, ce n'est pas toujours par l'innovation juridique que le droit saisit les techniques. Dans le cadre de notre étude, le « principe » de neutralité technologique[144] des règles juridiques implique de rechercher, en premier lieu, à appliquer le droit commun, sans distinguer la nature des moyens d'intrusion ou de révélation. Ce premier temps a une vertu heuristique : il permet de saisir toutes les formes de protection que le droit commun offre au « secret médical », objet protégé **(Titre I)**. Par ailleurs, « *la technologie ne se contente pas de modifier les conditions d'application du droit. Elle fait émerger des situations complètement inédites, voire de nouveaux "objets" non identifiés et auxquels les règles classiques ne peuvent pas s'appliquer* »[145]. Dans la seconde moitié du XX^e^ siècle, les utilisations de l'informatique ont créé un « *besoin de droit* »[146] auquel il a été répondu par l'édiction de dispositions spécifiquement applicables au traitement mathématique de l'information[147]. La convergence entre l'informatique et l'internet, point de rencontre entre les technologies de l'information et celles de la communication, a ensuite nécessité la modification de ces dispositions. Elles forment aujourd'hui le droit de la protection des données à caractère personnel. Ce corps de règle s'articule de manière complexe avec les dispositions de droit commun afin de protéger le « secret médical » **(Titre II)**.

---

[143] Par exemple, en droit pénal : I. LOLIES, *La protection pénale de la vie privée*, préf. R. GASSIN, PUAM, 1998.
[144] « *La neutralité technologique renvoie à l'idée que la prise en compte des phénomènes technologiques nouveaux doit se faire sans introduire de nouvelles complexités dans la loi, c'est-à-dire (...) qu'il faut par priorité, chaque fois que cela est possible, préférer étendre aux activités nouvelles les dispositions déjà prévues par le droit pour les activités traditionnelles équivalentes* […] » (J. DIONIS DU SEJOUR, Rapport fait au nom de la commission des affaires économiques, de l'environnement et du territoire sur le projet de loi (n° 528), pour la confiance dans l'économie numérique, n° 612, 12 févr. 2013, p. 11).
[145] B. WARUSFEL, « Le droit des nouvelles technologies : entre technique et civilisation », *La lettre de la rue Saint-Guillaume – Revue des Anciens élèves de Sciences-Po*, n° 127, juin 2002, pp. 52-59, spéc. p. 54.
[146] P. CATALA, « Le formalisme et les nouvelles technologies », *Defrénois* 2000, p. 897.
[147] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

TITRE I. Le secret comme objet en droit commun

30. Les technologies de l'information et de la communication ne désignent pas une catégorie unitaire de dispositifs ou d'outils. Si, prises ensemble, elles constituent des moyens d'immixtion ou de révélation **(Chapitre 2)**, les seules technologies de l'information emportent des conséquences sur les rapports entre l'information et son support. Le secret objet du droit, consistant en des informations protégées, ces rapports et leur transformation doivent être étudiés **(Chapitre 1)**.

Chapitre 1 - Les rapports entre l'information et son support

31. L'étude des rapports entre l'information et son support permet d'envisager les modes de protection du « secret médical » par la protection du support sur lequel les informations sont représentées **(section 1)**. L'une des fonctions primaires de l'informatique consistant dans la possibilité de désolidariser l'information de son support il conviendra d'en évaluer les conséquences sur la protection du « secret médical » **(section 2)**.

Section 1 - La protection du secret par la protection du support

32. C'est par une action de représentation[148] que se noue le lien entre l'information et son support **(paragraphe 1)**. Ce lien donne une existence physique à l'information, le support de l'information secrète est alors protégé comme l'information secrète elle-même **(paragraphe 2)**.

§ 1 - L'information secrète représentée

33. Afin d'étudier la protection du secret par son support, il faut en premier lieu déterminer quelles sont les informations secrètes **(A)**. Il convient ensuite de préciser que la protection juridique du support comme incarnation des informations secrètes n'a été consacrée qu'en raison des exigences croissantes de formalisation dont elles sont l'objet **(B)**.

A - L'information à caractère secret

34. Déterminer les contours du « secret médical » objet de protection implique de revenir à la question des fondements du secret professionnel. Soit l'on considère que le secret professionnel médical est institué pour protéger le secret de la vie privée des malades, dans ce cas l'information secrète sera nécessairement une information relative à la vie privée. Le « secret médical », objet juridiquement protégé sera alors déterminé par son contenu **(1)**. Soit l'on admet que l'existence du « secret médical », objet protégé, dépend d'élement de contexte

[148] La représentation est l'action de représenter. Cette dernière consiste à rendre quelque chose « effectivement présent à la vue, à l'esprit de quelqu'un » (*V°* « Représenter », TLFi, *op. cit.*).

indifférent à la nature de l'information. Dans ce cas, les raisons de la protection de l'information par le moyen du secret professionnel déterminent son contenu **(2)**.

1 - Le secret déterminé par son contenu

35. L'infraction sanctionnant la violation du secret professionnel prohibe la « *révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire* ». Certains auteurs estiment que l'information à caractère secret constitue une condition préalable de l'infraction. Or, la condition préalable, si elle fait partie de la norme pénale, se distingue du comportement incriminé. L'information à caractère secret, condition préalable de l'infraction, représente alors la valeur sociale protégée[149]. A ce titre, la condition préalable de l'infraction est un élément préexistant[150], « *une situation juridique de droit ou de fait constitutive de l'incrimination et distincte de l'infraction* »[151]. Dans l'hypothèse où l'on admet que l'information à caractère secret est une condition préalable de l'infraction il devient nécessaire d'identifier la norme extra-pénale à laquelle le droit pénal apporte sa sanction. Cette démarche devrait alors permettre de cerner ce que recouvre le « secret médical » objet de protection **(a)**. L'indifférence quant à la nature, privée ou publique, de l'information incite néanmoins à relativiser cette conception de l'information à caractère secret **(b)**.

a - Le contenu de l'information

36. L'information secrète par nature. La notion d'information secrète par nature est d'un usage délicat. De nombreux auteurs rejettent la théorie selon laquelle les informations couvertes par le secret sont secrètes par nature[152], mais la référence à celle-ci existe dans la jurisprudence

---

[149] E. DREYER, *Droit pénal général,* Manuel, LexisNexis, 3e éd., n° 216 ;
[150] B. THELLIER DE PONCHEVILLE, *La condition préalable de l'infraction*, Préf. A. VARINARD, coll. Institut de Sciences pénale et de Criminologie, PUAM, 2010.
[151] *Ibid.*
[152] En ce sens : Concernant l'ensemble des secrets protégés à l'exception des secrets industriels et commerciaux et du secret défense, E. DREYER *Droit pénal spécial*, coll. Cours Magistral, Ellipses, 3ème éd., 2016, n° 390. Il faut préciser par ailleurs que le secret des délibérés est également considéré comme un secret par nature, ainsi Monsieur Mayaud affirme : « *L'obligation du secret qui s'impose aux jurés est générale et absolue, car le délibéré est secret par nature, et cette obligation immuable s'impose par elle-même, indépendamment du serment, à toute personne appelée par la loi à assister audit délibéré* » (Y. MAYAUD, « Le secret du délibéré, un secret professionnel absolu », obs. Crim. 25 mai 2016, n° 15-84.099, publié au Bulletin, *RSC* 2016 p. 265) ; M. VERON, *Droit pénal spécial*, coll. Université, Sirey, 14ème ed., 2012, n° 287 ; V. PELTIER, *Jcl. Pénal Code,* Art. 226-13 et 226-14, fasc. 20, « Révélation d'une information à caractère secret. - Conditions d'existence de l'infraction. -

sans que l'on en trouve aucune définition[153]. Un auteur expose, au travers d'une analyse attentive, les raisons pour lesquelles cette vision revêt une certaine importance sans emporter totalement la conviction[154]. Il énumère les raisons pour lesquelles la conception de l'information secrète par nature ne peut emporter adhésion. La première, selon lui, peut se déduire du fait que le choix opéré par le législateur lors de la rédaction du nouveau Code pénal, au moment de laquelle la formulation « *information à caractère secret* » est préférée à la formule consistant à affirmer qu'est secret tout ce que le professionnel a vu, entendu ou compris[155], ne peut suffire à convaincre d'une volonté de consacrer une telle vision du secret puisque le juge n'a jamais cessé d'affirmer le caractère général et absolu de certains secrets professionnels[156]. En effet, comme le souligne Madame Frison-Roche la conception d'un secret par nature, tenant au contenu de l'information, invite à envisager le secret sous l'angle de la vie privée et confirme son caractère relatif[157], puisque certaines informations échapperaient à la qualification de secret. Cela amènerait notamment le juge à déterminer ce qui est secret ou non. Par ailleurs, comme le rappelle Monsieur Dreyer, le droit pénal ne « *protège pas abstraitement des informations confidentielles par nature ; il lutte contre des comportements qui trahissent la confiance que l'on peut avoir dans un lieu, une chose ou un service, voire une personne* »[158] et souligne que « *Si l'on excepte la protection spécifique des secrets de la défense nationale (C. pén., art. 413-9 et s.) et du secret de fabrique (C. trav., art. L 1227-1.)* »[159]. La référence à

Pénalités », mai 2015 (mise à jour sept. 2016), n° 30 ; F. WAREMBOURG-AUQUE, « Réflexions sur le secret professionnel », *RSC* 1978, p. 237, n° 18.

[153] Cass. crim., 6 janv. 1855 : *DP* 1855, 1, p. 30 ; *S.* 1855, 1, p. 155 ; arrêt *Watelet*, Cass. crim., 18 déc. 1885, préc. ; Cass. civ., 1er mai 1899 : *DP* 1899, 1, p. 585, note M. PLANIOL ; *S.* 1901, 1, p. 161, note A. ESMEIN ; Cass. req., 18 juill. 1904 : *S.* 1905, 1, p. 233 ; *DP* 1905, 1, p. 43 ; Cass. civ., 13 juill. 1936 : *Gaz. Pal.* 1936, 2, J. 727 ; *S.* 1938, 1, p. 201, note A. LEGAL ; *JCP* 1937, II, 18, note A. PERRAUD-CHARMANTIER ; Cass. crim., 3 mars 1938 : *DH* 1938, p. 341 ; *S.* 1938, 1, p. 209, note H. ROUSSEAU ; Cass. crim., 6 déc. 1956 : *Bull. crim.,* n° 820 ; *D*. 1957, p. 193 ; *S*. 1957, p. 126 ; *Gaz. Pal.* 1957, 1, J. 164 ; Cass. crim., 7 févr. 1957 : *Bull. crim.* n° 129 ; *RSC* 1957, p. 640, obs. L. HUGUENEY ; CA Grenoble, 3 mars 1905 : *D*. 1907, 2, p. 194 ; CA Grenoble, 22 mai 1952 : *D*. 1952, p. 445 ; TGI Avesne sur Helpe, 2 avr. 1951 : *JCP* 1951, IV, 128.

[154] M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, th. dact. ss. la dir. d'A. PROTHAIS, 2004, Université Lille II, n° 42 et svt.

[155] *Ibid.,* n° 43.

[156] « *La Cour de cassation a d'ailleurs maintenu, après l'entrée en vigueur du Code pénal nouveau, sa formule classique selon laquelle le secret professionnel, en matière médicale, est un devoir « général et absolu ». Or, cette affirmation est en soi contradictoire avec la notion de secret par nature puisqu'elle renvoie* […] *à la conception du secret d'ordre public, c'est-à-dire à la jurisprudence du secret appris, compris ou entendu* » (*Ibid.,* n° 46).

[157] M.-A. FRISON-ROCHE (ss. la dir.), *Secrets professionnels*, éd. Autrement, 1999, p. 24

[158] E. DREYER *Droit pénal spécial*, *op. cit.,* n° 390.

[159] *Ibid*.

la confiance renvoie à la conception de l'information secrète par la profession du déposant[160]. Pour l'auteur donc, seuls certains secrets particuliers protègent des informations secrètes par nature, le secret professionnel ne faisant pas partie de cette catégorie[161]. Toutefois, une partie minoritaire de la doctrine considère que l'information à caractère secret s'entend des informations relatives à la vie privée. Ce serait donc la nature de l'information qui permet de qualifier l'information de *secrète*. Mesdames Thouvenin et Rassat considèrent ainsi que ne sont des informations à caractère secret que les « *secret*[s] *au sens exact du terme* »[162]. Les critiques adressées à cette conception du secret, rappelées et suivies par Monsieur Couturier, permettent à l'auteur d'affirmer que le vocable choisi par le législateur « *signifie simplement que certaines choses ne sont pas ou ne doivent pas être révélées sans fixer le moindre critère de ce qui relève ou non de cette catégorie* »[163].

37. Difficulté à qualifier l'information secrète selon le critère de la vie privée. La principale critique adressée par une grande partie de la doctrine à la conception de l'information à caractère secret comme « secret par nature » tient à la difficulté de dégager un critère qui permette d'en fixer les limites. La vie privée est souvent invoquée comme l'étalon de mesure permettant de définir le contenu de l'information. Il est, en effet, certaines décisions qui, sans faire mention d'un « secret par nature », déterminent le caractère secret de l'information par rapport à la vie privée[164]. Par ailleurs, si la dualité des fondements du secret professionnel est largement admise, certains auteurs considèrent que c'est la référence à la vie privée qui permet de déterminer ce qui est secret et ce qui ne l'est pas[165]. S'il ne fait pas de doute que les

---

[160] V. *infra* n° 259 et svt.

[161] Dans le même sens : V. PELTIER, *Jcl. Pénal Code*, Art. 226-13 et 226-14, Fasc. 20 : « Révélation d'une information à caractère secret. – Conditions d'existence de l'infraction. – Pénalités », mai 2015 (mise à jour sept. 2016), n° 30.

[162] D. THOUVENIN, « Le secret médical – Droit pénal », *Droit médical et hospitalier* (Litec), fasc. 11, 1998, n° 6 ; *Jcl. Pénal Code,* art. 226-13 et 226-14, fasc. 10 : « Révélation d'une information à caractère secret. Conditions d'existence de l'infraction », 1998, n° 65 et s. ; v. également M.-L. RASSAT, *Droit pénal spécial. Infractions des et contre les particuliers*, 5ème éd., coll. Précis, Dalloz, 2006, n° 431.

[163] M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*, n° 46.

[164] Par exemple : Cass. crim., 24 avril 2007, n° 06-88.051, *Bull. crim*., n° 108 ; *AJ pénal* 2007, p. 331, obs. C. SAAS ; *RSC* 2007, p.815, obs. Y. MAYAUD.

[165] Ainsi, Monsieur Py soutient que ces informations sont « *tous les faits de la vie privée que les intéressés tiennent en général, pour des raisons quelconques, à dissimuler* […] » (B. PY, *Rép. pén.*, *V°* « Secret professionnel », févr. 2003 (mise à jour févr. 2017), n° 53 ; M. CAUCHY, A. DIONISI-PEYRUSSE « Le droit au secret médical et son application en matière d'assurances », *D.* 2005 p. 1313. Les auteurs affirment que l'objectif du « secret médical » est la protection de la vie privée.

informations relatives à l'intimité, noyau de la vie privée[166], sont des informations à caractère secret dès lors qu'elle ont été obtenues à l'occasion de l'activité de la personne soumise au secret, le concept de *vie privée* est incertain et « *évolutif* » dans son contenu. Incertain, car les tentatives de la doctrine pour délimiter la vie privée n'ont jamais été totalement opérantes, qu'il s'agisse d'en tracer les contours par distinction avec la vie publique[167] ou de dresser la liste des éléments de celle-ci en fonction d'une jurisprudence casuistique[168]. Enfin, la distinction entre ce qui relève de la vie privée protégée et d'autres éléments de la personnalité n'est pas aisée[169]. Les hésitations jurisprudentielles ont amené la doctrine majoritaire à refuser la conception d'une information qualifiée de secrète en raison de sa nature privée. Pour Madame Frison-Roche, « *La variation* [du contenu de la notion] *est si nette dans le temps et dans l'espace* […] *qu'il faut en tout cas regarder la frontière du privé et du public avec suspicion* »[170]. Notons, par ailleurs, qu'il est habituellement argué la place de l'infraction dans le Code pénal, laquelle figure, non pas dans la section relative aux atteintes à la vie privée, mais dans celle relative au secret[171]. Enfin, le dernier argument avancé pour rejeter la conception d'une infraction punissant l'atteinte à la vie privée tient à la particularité du secret professionnel en ce qu'il en est conçu, par les personnes qui y sont soumises, comme une *règle d'action* leur permettant d'opposer le secret à quiconque souhaiterait connaître des informations détenues par eux. Ce que l'on désigne sous l'expression *opposabilité du secret professionnel* concentre la majorité des litiges opposant les personnes tenues au secret et l'administration ou la justice. C'est pourquoi les théories juridiques relatives au secret professionnel se sont construites sur la

---

[166] Madame Chauvet, dans sa thèse de doctorat, distingue la « *vie privée réduite à l'intimité* » et les extensions de la vie privée (D. CHAUVET, *La vie privée – Etude de droit privé*, th. dact. sous la dir. de E. DREYER, soutenue le 5 sept. 2014, Université Paris-Sud).

[167] R. BADINTER, « Le droit au respect de la vie privée », *JCP* 1968, I, 2136 ; R. LINDON, « La presse et la vie privée », *JCP G* 1965, I, 1887 ; *contra* F. RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, *in* La protection de la vie privée dans la société de l'information, ss la dir. de P. TABATONI, t. 6, 7 et 8, PUF, coll. « Cahier des sciences morales et politiques », 2002, p. 724, n° 647 ; M. PATIN, « La répression des délits de presse », *RSC* 1954, p. 449 ; D. CHAUVET, *La vie privée – Etude de droit privée*, *op. cit.*, n° 16 ; A. BATTEUR, *Droit des personnes, des familles et des majeurs protégés*, 9ème éd., coll. Manuel, LGDJ, 2017, n° 200 ; J.-C. SAINT-PAU, « Le droit au respect de la vie privée – Définition conceptuelle du droit au respect de la vie privée », *in* J.-C. SAINT-PAU (ss la dir.), *Droits de la personnalité*, coll. Traités, LexisNexis, 2013, n° 1170.

[168] A. BATTEUR, *Droit des personnes, des familles et des majeurs protégés*, *op. cit.,* n°200 ; J.-C. SAINT-PAU, *Le droit au respect de la vie privée- Définition conceptuelle du droit au respect de la vie privée*, *in Droits de la personnalité*, *op. cit.,* n° 1170.

[169] Il en va ainsi de la distinction entre vie privée et identité.

[170] M.-A. FRISON-ROCHE (ss. la dir.), *Secrets professionnels*, éd. Autrement, 1999, p. 39.

[171] Bien que dans un chapitre consacré aux atteintes à la personnalités (Chap. VI, Titre II, Livre II).

base de la jurisprudence civile et administrative. Un auteur relève que cette possibilité d'opposer le secret exclut celle d'admettre la vie privée comme critère de qualification de l'information puisque, pour savoir si une information porte sur la vie privée d'une personne, il faut qu'elle ait été révélée[172]. Une telle détermination est donc impossible dans les cas où le professionnel oppose son « *droit au silence* »[173], ce qui est l'hypothèse la plus fréquemment rencontrée en jurisprudence. En effet, dans le cas où le juge est face à un refus de témoigner ou dans celui de la saisie d'informations, cette détermination intervient seulement lorsqu'il a été pris connaissance des informations dont dispose la personne soumise au secret professionnel. L'auteur en déduit que la conception d'un secret par nature, basée sur le concept de vie privée, est inopérante[174]. Le point de vue défendu par Monsieur Couturier, nous semble critiquable notamment au regard des choix que l'auteur opère. Il considère, en effet que « l'information à caractère secret » est une condition préalable de l'infraction. Or, si l'on soutient l'idée selon laquelle le secret professionnel n'a pas pour finalité de punir les atteintes à la vie privée, la seule condition préalable devrait être la soumission au secret de la personne[175]. C'est finalement la variabilité et la complexité de la notion de vie privée et le caractère erratique de la jurisprudence qui semble figer les conceptions de l'information à caractère secret.

38. La vie privée, un critère de l'information à caractère secret. Si l'on se tient éloigné des limites mouvantes de la notion de vie privée[176] pour s'en tenir à son cœur, l'intime, il ne fait aucun doute qu'est secrète toute information relative à cette sphère de la vie privée de l'individu dès lors qu'elle est obtenue en raison de l'activité professionnelle de celui qui est soumis au secret. En effet, l'obligation de garder le secret et la sanction pénale qui y est attachée

---

[172] M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*, n° 49.
[173] J.-L. BAUDOUIN, *Secret professionnel et droit au secret dans le droit de la preuve*. *Etude de droit québécois comparé au droit français et à la common law*, coll. Bibliothèque de droit privé canadien, t. III, LGDJ, 1965.
[174] « *Certes, la notion de secret par nature n'est pas nécessairement erronée dans son essence car il est assurément des informations dont on peut estimer qu'elles requièrent plus de discrétion que d'autres. Cependant, cette conception demeure trop complexe et variable pour prétendre à l'efficience. Dès lors, elle ne peut, pour cette raison, constituer en elle-même le critère véritable de l'information secrète au sens de l'article 226-13 du Code pénal* » (M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*, n° 49).
[175] Il convient en effet de rappeler que les conditions préalables sont « *des situations dénuées de coloration pénale qui préexistent à l'acte matériel et qui constituent, en quelque sorte le cadre de certaines infractions* » (X. PIN, *Le consentement en matière pénale*, préf. J. MAISTRE DU CHAMBON, coll. Bibliothèque de droit pénal, LGDJ, 2002, n° 199).
[176] Au gré d'une jurisprudence casuistique, les juges ont dessiné les contours de la vie privée, ceux-ci restent donc mouvants. Pour quelques études récentes sur la notion de vie privée, v. D. CHAUVET, *La vie privée – Etude de droit privé*, th. dact. ss la dir. de E. DREYER, soutenue le 5 sept. 2014, Université Paris-Sud ; J.-C. SAINT-PAU (ss la dir.), *Droits de la personnalité*, *op. cit*.

constituent un mode de protection de l'intimité des personnes, tandis que d'autres secrets n'ont pas cette fonction[177]. Qu'importe que cette protection ne soit qu'incidente selon que l'on adopte l'une ou l'autre des conceptions du secret professionnel, qu'elle ne soit qu'une fonction[178], faute d'être admise comme sa finalité. Ainsi, l'intimité de la vie privée[179] peut correspondre au contenu de l'information secrète, et si la divulgation de cette intimité peut engager la responsabilité civile de tout individu sur le fondement de l'article 9 du Code civil, cette divulgation pourra engager la responsabilité pénale de la personne soumise au secret professionnel. Si l'on distingue, comme le fait un auteur, les actions et les informations relatives à l'intimité[180], notre propos n'intéresse que les informations relatives à l'intimité puisque les *actions* relatives à l'intimité sont l'objet d'une prérogative qui consiste dans une liberté civile ou publique. Dans cette hypothèse « *la vie privée s'entend d'une action personnelle, d'une sphère d'activité dont le titulaire invoque l'inviolabilité* »[181]. S'agissant des informations entrant dans la sphère de l'intimité de la vie privée, l'intimité corporelle, implique la possibilité

---

[177] Ainsi en est-il du secret des affaires, du secret de fabrique ou encore du secret de l'instruction. D'abord, le secret des affaires est composite. Sous ce vocable, c'est le secret de fabrique et le délit d'initié qui sont souvent désignés. Le secret de l'instruction, quant à lui, est considéré, par certains, comme un secret par nature dont la révélation devrait faire l'objet d'une infraction spécifique (J. PRADEL, « Procédure pénale », pan., *D.* 2016, p. 1727, citant un arrêt de la chambre criminelle énonçant que « *l'obligation au secret qui s'impose aux jurés est générale et absolue car le délibéré est secret par nature* », « *cette obligation immuable s'impose par elle-même, indépendamment du serment, à toute personne appelée par la loi à assister audit délibéré* » (Cass. crim., 25 janv. 1968, *Bull. crim*., n° 25 ; *D*. 1968, p. 153, rapp. J.-C. COSTA ; *JCP* 1968, II, 15425 ; *Gaz*. *Pal*. 1968, I, p. 164 ; *RSC* 1968, p. 344, obs. G. LEVASSEUR). Par ailleurs, le secret de l'instruction est fondé sur la nécessaire indépendance des juges – principe constitutionnel –, leur impartialité et l'autorité des décisions (J. PRADEL, *op. cit.*).

[178] Mathias Couturier considère ainsi que la protection de la vie privée est la fonction exprimée du secret professionnel tandis que la protection des professionns serait la fonction latente (M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*).

[179] L'intimité de la vie privée n'est, en réalité, pas aisée à définir, les auteurs le soulignent d'ailleurs (I. LOLIES, *La protection pénale de la vie privée*, coll. « Institut de Sciences Pénales et de Criminologie » PUAM, 1999, p. 39, n° 23 ; A. CHAVANNE, « Les atteintes à l'intimité de la vie privée au sens de l'article 368 du Code pénal », *in Actes du 8e Congrès de l'Association de droit pénal,* Economica, 1985, p. 24 ; G. LEVASSEUR, « La protection pénale de la vie privée *», in Études offertes à P. Kayser*, t. 2, PUAM, 1979, p. 107 s., spéc. p. 114). La jurisprudence et la doctrine se sont toutefois évertuées à en définir le contenu et à le circonscrire à des moments et des lieux ou des situations de la vie des individus (D. CHAUVET, *La vie privée – Etude de droit privé*, *op. cit.*, spéc. n° 60 et svt).

[180] J.-C. SAINT-PAU, « Le droit au respect de la vie privée », *in* J.-C. SAINT-PAU (ss. la dir) *Droits de la personnalité*, *op. cit.*, n° 1171 : « *Lorsqu'une personne invoque une ingérence dans la liberté de la vie privée, c'est-à-dire une liberté civile ou publique, la vie privée s'entend d'une action personnelle, d'une sphère d'activité dont le titulaire invoque l'inviolabilité. Lorsqu'un individu souffre d'une atteinte au secret de la vie privée, la notion s'entend d'une information personnelle dont le titulaire invoque la confidentialité, ou plus largement la maîtrise.* »

[181] *Ibid*.

de s'opposer à toutes divulgations d'images du corps de la personne. Font également partie de l'intimité corporelle, les information génétiques, l'état de santé, les mœurs et l'intimité sexuelle, les sentiments, les convictions religieuses, politiques et philosophiques[182]. L'intimité familiale, c'est-à-dire les relations sentimentales et ou conjugales, l'état de grossesse, la naissance, les liens de parenté, les relations familiales, le divorce. Toutes ces informations, dont le secret doit être respecté par tous, sont des informations à caractère secret pour les personnes qui sont soumises au secret professionnel. Si la vie privée n'est pas l'unique critère de qualification de l'information à caractère secret, il en est *l'un* des critères.

39. La vie privée, l'identité et l'information à caractère secret. L'hypothèse selon laquelle la vie privée serait le critère de détermination de l'information à caractère secret se heurte à une résistance s'agissant de l'identité[183]. Alors qu'il est admis, en droit interne, que le nom patronymique ne peut entrer dans cette sphère[184], la Cour européenne des droits de l'homme, dans une approche extensive de la notion de vie privée, considère que le nom d'une personne est constitutif de sa vie privée[185]. De même, Madame Lepage souligne que « *la mention du nom permet l'identification de la personne, identification qui est une condition d'application des droits de la personnalité, notamment du droit au respect de la vie privée* »[186]. Aussi l'information est-elle secrète dès lors que le nom permet d'identifier la personne concernée par l'information. L'identité de la personne est parfois envisagée comme un de ses éléments[187] tandis qu'un auteur invoque, par exemple, l'intérêt de consacrer un droit subjectif autonome sur l'identité afin de « *recentrer le droit au respect de la vie privée sur l'intimité des personnes, conformément à la lettre de l'article 9 du Code civil, et d'éviter ainsi d'inutiles concours de qualifications légales, en matière pénale tout particulièrement* »[188]. Affirmer que

---

[182] *Ibid.*
[183] Pour une étude complète : D. GUTMANN, *Le sentiment d'identité*, préf. F. TERRE, coll. Bibliothèque de droit privé, t. 327, LGDJ, 2000.
[184] Paris, 30 oct. 1998, *D.* 1998, IR, p. 259 ; *RTD civ*. 1999, p. 61, obs. J. HAUSER ; TGI Nanterre, 27 avr. 2006, *Légipresse* 2006, I, p. 125 ; TGI Paris, 3 mars 2003, *Légipresse* 2003, I, p. 123.
[185] CEDH, 24 oct. 1996, Guillot c/ France, *RTD civ.* 1997, p. 551, obs. J.-P. MARGUENAUD.
[186] A. LEPAGE, *Rép. civ*., *V°* « Personnalité (droits de la) », sept. 2009 (mise à jour nov. 2017), n° 77.
[187] Le droit à l'anonymat qu'implique le droit au respect de la vie privée peut se concevoir comme la possibilité de s'opposer à la divulgation de « […] *l'identité civile, physique ou économique de la personne.* […] *Cette perspective s'inscrit dans la jurisprudence européenne qui précise que la notion de vie privée peut parfois englober des aspects de l'identité physique et sociale de l'individu* » (J.-C. SAINT-PAU, « Le droit au respect de la vie privée – Définition conceptuelle du droit au respect de la vie privée », *in* J.-C. SAINT-PAU (ss. la dir.), *Droits de la personnalité*, *op. cit.*, n° 1173).
[188] M. BENEJAT, « Les droits sur l'identité – Les droits sur les données personnelles », *in* J.- C. SAINT-PAU (ss la dir.), *Droit de la personnalité*, *op. cit.*, n° 924.

l'information secrète est une information relative à la vie privée imposerait donc nécessairement d'opérer un choix quant à savoir si l'identité constitue ou non une information à caractère secret[189]. Or, concernant par exemple l'identité, la Cour de cassation a admis que la révélation du nom d'un client d'un laboratoire d'analyses médicales à un organisme de recouvrement n'était pas constitutive d'une violation du secret professionnel dès lors que l'information portait sur le seul nom et non sur le type d'analyses pratiquées[190]. A l'inverse, s'agissant par exemple du secret professionnel des avocats[191] ou encore de celui des banquiers[192], l'identité du client a pu être qualifiée d'information à caractère secret. Il en est de même concernant le secret professionnel des professionnels de santé, quelques arrêts confirmant que l'identité du patient n'est pas une information à caractère secret opposable à l'administration fiscale[193]. Toutefois, certaines décisions vont dans le sens contraire[194]. Le caractère secret de l'identité du malade diffère donc selon le contexte. Ainsi, la consultation

---

[189] C'est notamment une question traitée par Madame Chauvet dans sa thèse de doctorat (D. CHAUVET, *La vie privée – Etude de droit privé*, *op. cit.*).

[190] Cass. crim., 31 janv. 1995, n° 94-80562 ; d'autres décisions ont été rendues en ce sens : Cass. crim., 11 févr. 1960, *Bull. crim*., n° 85 ; *JCP* 1960, II, 11604, note R. SAVATIER ; *D.* 1960, p. 258, note J.-M. R. ; Cass. crim., 1er févr. 1977, *Bull. crim*. n° 40 ; Cass. crim., 21 mai 1979, *Bull. crim*., n° 178 ; *RSC* 1980, p. 439, obs. G. LEVASSEUR.

[191] A propos du secret des avocats et de leur possibilité de refuser de donner l'identité de leurs clients à l'administration fiscale : CE, 10ème et 9ème ch. réunies, 4 mai 2016, n° 387466, *Dalloz act.,* 10 mai 2016, obs. A. PORTMANN.

[192] L'identité du bénéficiaire d'un chèque est une information couverte par le secret professionnel bancaire : Cass. com., 8 juill. 2003, n° 00-11993, *RTD com.* 2003, p. 783, obs. M. CABRILLAC ; *D.* 2003, *AJ* p. 2170, obs. V. AVENA-ROBARDET.

[193] Cass. crim., 21 mai 1979, n° 78-92205*, RSC* 1980, p. 439, obs. G. LEVASSEUR ; Cass. crim., 29 avr. 1996, n° 95-82478.

[194] Rennes, ch. corr., 13 janv. 1992, *JCP E* 1993, II, 432, note C. GAVALDA, à propos de la diffusion d'une liste de client à des commerçants. Dans le même sens, Cass. civ. 1re, 18 mars 1997, *Bull. civ*. I, n° 99 ; JCP 1997, II ; 22829, concl. P. SARGOS ; *D.* 1997, somm. p. 315, note J. PENNEAU : « *les dispositions relatives au secret professionnel font obstacle à ce que l'identité d'un malade soit divulguée sans son consentement* ». En matière fiscale encore, Monsieur Couturier établit une liste d'arrêts du Conseil d'Etat allant également en ce sens : CE, 20 nov. 1959, *Rec*. p. 613, *JCP* 1960, II, 11431, concl. POUSSIERE ; *D*. 1960, p. 157, note R. SAVATIER ; CE ass., 12 mars 1982, *Conseil national de l'ordre des médecins, RJF* 1982, comm. 475, concl. VERNY ; *JCP* 1982, II, 19857, note J. DUFFAR ; *Dr. fisc.* 1982, comm. 225 ; C. DAVID, O. FOUQUET, B. PLAGNET et J.-F. RACINE, *Les grands arrêts de la jurisprudence fiscale*, 4ème éd. Dalloz, 2003, n° 8, p. 156 ; CE, 20 janv. 1999, *Méas* ; *Procédures* 1999, comm. 221, obs. J.-L. PIERRE ; v. également TA Lyon, 28 oct. 2004, *Gaz. Pal.* 14-16 nov. 2004, p. 22, note J.-J. ISRAEL (M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, th. dact. ss. la dir. d'A. PROTHAIS, 2004, Université Lille II, n° 343). Pour une décision récente : CE, 9ème et 10ème SSR, 24 juin 2015, n° 367288. Pourtant il faut noter qu'il est désormais acquis que l'administration fiscale peut accéder à des informations relatives à l'identité des patients dès lors que d'autres informations concernant les prestations offertes ne sont pas également connues du contrôleur fiscal. Ce n'est pas l'identité du patient qui est secrète mais l'identité mise en contexte, grâce à d'autres informations.

d'un oncologue ou d'un psychiatre donne une information supplémentaire sur la situation du patient, et porte ainsi atteinte au respect de sa vie privée, tandis que le fait de consulter un généraliste n'apporte aucune information supplémentaire. Comme le souligne un auteur, le secret professionnel n'a pas vocation à sanctionner une atteinte aux droits sur l'identité mais, dans la mesure où l'identité peut constituer un élément de la vie privée dès lors qu'elle est mise en contexte, cette protection est incidente[195].

b - L'indifférence quant à la nature de l'information

40. Information déjà connue du public. L'information sera qualifiée d'information à caractère secret, que celle-ci soit déjà connue du public ou non. D'ailleurs, l'étendue de la connaissance de ce fait, par le public, importe peu. Qu'il s'agisse de faits évoqués par la rumeur publique ou connus de manière plus certaine et que la révélation ne vient que confirmer, la révélation sera punissable[196]. Il faut aussi relever que le caractère positif ou négatif d'un tel fait importe peu[197].

2 - Les raisons du secret déterminant son caractère

41. Le secret confié. La première conception de l'information secrète découle de la formulation de l'article 378 du Code pénal ancien définissant comme secrètes les informations confiées au professionnel. Sous l'empire de cet article, et durant une grande partie du XIX^{ème} siècle, la jurisprudence comme la doctrine ont parfois considéré qu'étaient secrètes les informations confiées au professionnel « *sous le sceau du secret* »[198]. Il s'agissait alors, pour celui qui confiait l'information, de faire une « *recommandation spéciale de garder le silence* »[199]. Cette vision de l'information secrète n'a toutefois jamais été ni majoritaire ni

---

[195] M. BENEJAT, « Les droits sur l'identité – Les droits sur les données personnelles », *in* J.- C. SAINT-PAU (ss la dir.), *Droit de la personnalité*, *op. cit.*, n° 911.
[196] Par exemple : Cass. crim., 7 mars 1989, *JCP* 1989, IV, 200.
[197] Divulgation d'un certificat médical attestant de l'absence de maladie : Crim., 9 nov. 1901, *D.* 1902, 1, p. 235 ; P. CONTE, *Droit pénal spécial*, 5ème éd., coll. Manuels, LexisNexis, 2016, n° 243.
[198] Quelques exemples de décisions où l'expression est formulée explicitement : Crim., 9 oct. 1978, n° 76-92075 ; crim., 19 nov. 1985, n° 83-92813, *Bull. crim*., n° 364 ; crim., 28 sept. 1999, n° 98-86762, *RSC* 2000 p. 202, obs. Y. MAYAUD.
[199] E. GARCON, *Code pénal annoté*, t. 2, éd. refondue et mise à jour par M. ROUSSELET, M. PATIN et M. ANCEL, Sirey, 1956, art. 378, p. 520, n° 31.

exempte de critiques[200]. D'abord parce que les arrêts admettant une telle vision du secret portaient sur des hypothèses dans lesquelles un professionnel avait refusé de déposer devant le juge, il est ainsi « *probable que la jurisprudence n'a jamais entendu en faire une application excédant le cadre de la dispense de témoignage* »[201]. Ensuite, en raison de son caractère bien trop restrictif, car si les secrets confiés sont, sans aucun doute, des informations secrètes, « *la condition de la discrétion n'est pas nécessairement expresse ; elle peut être tacite* »[202]. Si la doctrine semble s'accorder sur l'abandon d'une telle vision de l'information secrète[203], il faut se garder de toute affirmation car elle a persisté, de manière sporadique, dans la jurisprudence du XX^{ème} siècle[204]. Cette vision du secret doit être mise en lien avec la théorie du fondement contractuel du secret, consistant à interpréter strictement les termes employés par l'article 378 du Code pénal ancien, selon lesquels le professionnel est « *dépositaire* » d'un secret. L'incrimination du secret professionnel viendrait sanctionner une faute d'origine contractuelle[205]. Fonder le secret sur un contrat entre déposant et dépositaire laisse au déposant la liberté de déterminer ce qui doit ou non être gardé secret[206], il aurait donc la possibilité de délier le débiteur du secret[207]. Deux conséquences découlent d'une vision du secret professionnel fondé sur le contrat : la valeur protégée par l'infraction est d'ordre privé et individuel[208]; le dépositaire ayant la possibilité de déterminer la valeur de celui-ci, le secret professionnel est relatif[209]. Mais si cette thèse fut abandonnée à cause de son inefficacité à fonder le secret professionnel, il est indéniable que les secrets expressément confiés sont des informations à caractère secret au sens de la loi. De plus, il faut remarquer que « *les évolutions*

---

[200] Emile Garçon a parfaitement résumé les critiques déjà vives à son époque : E. GARCON, *Code pénal annoté*, *op. cit.*, pp. 516-517, n° 6 et svt.
[201] M. COUTURIER, *Pour une analyse fonctionnelle du secret professionnel*, *op. cit.*, p. 40, n° 8.
[202] E. GARCON, *Code pénal annoté*, t. 2, *op. cit.,* p. 521, n° 32.
[203] B. PY, *Rép. pén.*, *V°* « Secret professionnel », févr. 2003 (mise à jour févr. 2017), n° 51.
[204] A ce sujet, Monsieur Couturier prend pour exemple les arrêts dans lesquels est utilisée la formule « *secret confié* » (M. COUTURIER, *Pour une analyse fonctionnelle du secret professionnel*, *op. cit.*, n° 9 et svt.). Cela ne signifie pas, selon nous, que seules les informations confiées constituent des informations à caractère secret. Dans ces cas d'espèce, il était toutefois évident qu'il s'agissait de confidence. La formulation utilisée semble avoir une valeur pédagogique.
[205] E. GARCON, *Code pénal annoté*, *op. cit.*, pp. 516-517, n° 6 et svt.
[206] *Ibid.*
[207] *Ibid.*
[208] D. THOUVENIN, *Jcl. pénal,* art. 226-13 et 226-14, fasc. 10 : *Révélation d'une information à caractère secret. Conditions d'existence de l'infraction*, 1998, n° 7.
[209] E. GARCON, *Code pénal annoté*, *op. cit.*, pp. 516-517, n° 6 et svt.

législatives les plus récentes tendent à « privatiser » le secret de manière croissante afin de renforcer les droits du patient. La loi n° 2002-303 du 4 mars 2002 relative à la santé et aux droits des malades a ainsi clairement entendu déplacer le curseur au profit du patient afin de lui permettre de recouvrer, autant que possible, la maîtrise du droit à l'information que le pouvoir médical avait réussi à lui soustraire au fil du temps. On peut alors suggérer que ce texte confère une vigueur renouvelée à cette théorie du fondement contractuel »[210]. Cette idée ne nous semble toutefois pas pertinente dans la mesure où l'accès de la personne aux informations la concernant n'atteste pas d'un regain du secret professionnel fondé sur le contrat. D'abord parce que le droit à l'information du patient et de certains tiers est une prérogative indépendante de l'existence d'un contrat. Ensuite parce que ce droit concerne non seulement les informations confiées, mais également toutes les informations relatives à la prise en charge du malade. Le modèle du contrat de dépôt n'apparaît donc pas convaincant. L'idée d'un renouveau du fondement contractuel du secret professionnel, qui trouverait son expression dans la maîtrise de l'information par le patient et dont l'espace numérique de santé[211] serait le fer de lance, tient en partie à la *confusion entre droit à l'information et secret professionnel*. Cette idée sera réexaminée au regard de l'analyse de l'influence des droits reconnus aux personnes sur leurs données.

42. L'information secrète par la profession du dépositaire. Des conceptions de l'information à caractère secret, il s'agit sans doute de celle qui a rencontré le plus de succès et qui a emporté l'adhésion de la doctrine et de la jurisprudence. Affirmer que l'information est secrète par la profession de celui qui la reçoit revient à considérer qu'il n'y a pas d'information secrète mais que l'information est secrète dès lors que les professionnels assujettis en prennent connaissance. Cette vision de la notion d'information à caractère secret est le fruit d'une évolution historique[212] dont l'arrêt *Watelet*[213]est l'illustration la plus fameuse. Si les informations sont secrètes, c'est parce que la loi soumet certains professionnels à un devoir de

[210] F. ALT-MAES, « Les deux faces de l'information médicale : vers un nouvel équilibre des relations médecin-malade après la loi du 4 mars 2002 », *Gaz. Pal.* 14-16 déc. 2003, p. 3 ; *Adde* S. ABRAVANEL-JOLLY, « Le secret médical en assurance de personnes », *RGDA* 2005, p. 889.
[211] V. *infra,* n°360.
[212] Sur cette évolution v. M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit*., n° 25 et svt.
[213] Crim., 19 déc. 1885, *S.* 1886, 1, p. 86, rapport TANON ; *DP* 1886, 1, 347.

silence[214], le secret étant alors *général* dans la mesure où il ne concerne pas seulement les informations confiées. La loi du 4 mars 2002[215], tenant compte de la jurisprudence antérieure, est venue consacrer cette vision du secret : selon l'article L. 1110-4 du Code de la santé publique, « *ce secret couvre l'ensemble des informations concernant la personne venue à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes* ». L'information à caractère secret ainsi conçue se trouve également dans les codes de déontologie des professions médicales[216] et paramédicales[217] sous la formule consacrée selon laquelle le secret couvre non seulement ce qui a été confié au professionnel, mais également « *ce qu'il a vu, entendu ou compris* ». Cette conception de l'information secrète a pour conséquence de fonder le secret sur l'ordre public pénal[218]. En effet, la profession comme critère de qualification de l'information renvoie à la relation de confiance qui doit exister entre certains professionnels et les individus qui les sollicitent[219].

---

[214] Crim., 4 nov. 1999, n° 99-80157. En l'espèce, était poursuivi un employé de France télécom qui avait révélé à des personnes que leur ligne téléphonique avait été mise sur écoute. Dans cette espèce, la révélation n'est pas faite à un tiers mais à la personne concernée par l'information. La haute juridiction précisait que l'information avait été apprise dans le cadre de ses fonctions, ce qui suffisait à qualifier l'information de secrète. Par ailleurs, à l'occasion d'un arrêt statuant sur une QPC formulée comme suit : « *L'article 226-13 du code pénal porte-t-il atteinte aux droits et libertés garantis par la Constitution, et notamment au principe de légalité des délits et des peines en ce qu'il ne pose pas une définition suffisamment claire et précise de la notion d'information à caractère secret ?* », Madame Lazerges, conseiller rapporteur, a rappelé que l'information était secrète par la profession du déposant, ce qui justifie qu'il n'est pas besoin de la définir (crim., 5 sept. 2012, n° 12-90045, *CCC* nov. 2012, comm. 127, obs. A. LEPAGE).

[215] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (*JORF*, 5 mars 2002, p. 4118).

[216] CSP, art. R. 4127-4 concernant les médecins ; CSP, art. R. 4127-206 concernant les chirurgiens-dentistes ; CSP, art. R. 4127-303 concernant les sages-femmes.

[217] CSP, art. R. 4321-55 concernant les kinésithérapeutes.

[218] P. MISTRETTA, *Droit pénal médical*, éd. Cujas, 2013, n° 512.

[219] La protection de la confiance qui est au centre des relations entre les confidents nécessaires et les individus est ainsi résumée par Emile Garçon : « […] *le secret professionnel a uniquement pour base un intérêt social. Sans doute la violation de ce secret peut causer un préjudice aux particuliers, mais cette raison ne suffirait pas pour en justifier l'incrimination et la loi l'a punie seulement parce que l'intérêt général l'exige. Le bon fonctionnement de la société veut que le malade trouve un médecin, le plaideur un défenseur, le catholique un confesseur ; mais ni le médecin, ni l'avocat, ni le prêtre ne pourraient accomplir leur mission, si les confidences qui leur sont faites n'étaient assurées d'un secret inviolable. Il importe donc à l'ordre social que ces confidents nécessaires soient astreints à la discrétion et que le silence leur soit imposé sans condition ni réserve, car personne n'oserait plus s'adresser à eux si on pouvait craindre la divulgation du secret confié. Ainsi, l'article 378 a pour but, moins de protéger la confidence d'un particulier, que de garantir un devoir professionnel indispensable à tous. Ce secret est donc absolu et d'ordre public »* (E. GARCON, *Code pénal annoté,* 2ème éd. par M. ROUSSELET, M. PATIN et M. ANCEL, Sirey, 1959, art. 378, n° 7).

43. Ces observations relatives aux diverses conceptions de la notion *d'information à caractère secret* ne pouvaient être éludées dans la mesure où elles ont vocation à nous permettre d'identifier ce que recouvre le « *secret* » dans un premier sens, c'est-à-dire comme un *fait* qui doit être réservé, tant en raison de sa nature que de la soumission au secret du dépositaire. Le *fait* secret est ainsi *objet du secret*[220], le secret étant entendu comme l'obligation de se taire, c'est-à-dire *l'attitude*.

B - La représentation et la formalisation de l'information

44. Représentation de l'information à caractère secret. Il n'est pas un ouvrage sur le « secret médical » qui ne fasse une place introductive au serment d'Hippocrate. Cette démarche a généralement vocation à souligner l'ancienneté de ce devoir qui fonde l'éthique médicale depuis plus de deux millénaires. Bien que le texte ait fait l'objet de multiples traductions qui sont encore l'objet de discussions[221], la formule relative au devoir de secret qui incombe au médecin contient toujours le même verbe : « *taire* ». Le médecin doit taire ce qu'il voit ou entend. L'usage du verbe renvoie à la tradition orale dans laquelle était inscrite le rapport entre le médecin et son patient. La représentation des informations relatives au patient n'est toutefois pas récente, les historiens faisant remonter son origine à la naissance de la médecine clinique[222]. A cette époque, les écrits rassemblant des informations sur les patients ont surtout une vocation d'enseignement[223] ; ils auront, par la suite, des fonctions multiples. Il n'est pas utile de retraçer l'Histoire de la médecine et celle des documents médicaux relatifs aux patients[224]. Il nous importe seulement de mettre en lumière les différents emplois du mot : le secret constitue, dans un premier sens, un ensemble de « *connaissances, d'informations réservées à des initiés, des confidents* […] »[225], c'est-à-dire un *fait* qui n'est connu que d'un certain nombre d'individus[226]

---

[220] C'est la formule utilisée par P. MISTRETTA, *Droit pénal médical*, *op. cit.*, n° 517.
[221] J. DUCATILLON, « Le serment d'Hippocrate, problèmes et interprétations », *Bulletin de l'association Guillaume Budé*, 2001, pp. 34-61.
[222] Dont les représentants les plus illustre sont Rhazès (865-925), Avicenne (930-1037) ou Avenzoar (1073-1162) (J.-C. SOURNIA, *Histoire de la médecine*, coll. Poche/Sciences humaines et sociales, La Découverte, 2004, pp. 56-103).
[223] L'on peut, par exemple, citer le *Continens* qui rassemble les observations cliniques de Rhazès, formant une sorte d'encyclopédie médicale (*Ibid.,* p. 76).
[224] L'on pourra se reporter aux ouvrages historiques et notamment : J.-C. SOURNIA, *Histoire de la médecine*, *op. cit.*
[225] TLFi, *V°* « Secret », forme adjectivale.
[226] V. PELTIER, *Le secret des correspondances*, préf. P. CONTE, PUAM, 1999, n° 3.

(secret objet) et suppose une *attitude* de secret (secret moyen), afin de préserver l'*état* de secret (également secret objet), c'est-à-dire : « *Ce qui ne peut être connu ou compris parce que volontairement caché à ceux qui ne sont pas initiés ou confidents*»[227]. A s'en tenir à une approche de la relation entre la personne concernée par l'information et le professionnel qui est soumis au secret professionnel fondée sur la parole, l'*attitude,* qui est intimement liée à l'existence du *secret-fait,* est suffisante pour préserver le *secret-état*, celui-ci existe à l'égard des tiers. Dès lors que les informations relatives aux personnes se confiant à un professionnel soumis au secret sont représentées sur un support, le *secret-état* d'une chose, d'une situation ou d'une information, n'est plus seulement dépendant d'une *attitude* de silence, il nécessite également une protection du support sur lequel est représentée l'information. En d'autres termes, le passage du *logos* au *graphe* a pour première implication, en ce qui nous concerne, de rendre insuffisant le *secret-attitude* qui consiste à garder le silence, à se taire, et implique de préserver également le support, car le *secret-fait* est désormais accessible aux tiers pour lesquels il existe un *secret-état*.

45. La possibilité d'appréhender l'information par son support. Envisageant l'information comme un bien[228], Monsieur Beaussonie a parfaitement expliqué le lien entre l'information et son support comme relation entre le « *bien incorporel et la matière* »[229]. L'auteur développe notamment la question de l'accessibilité du *bien incorporel* à travers son support par le jeu de la représentation. Sans nous prononcer sur la question de savoir si l'information est ou non un bien, le raisonnement de cet auteur est transposable à l'information secrète représentée : le support assure l'incarnation de l'information et « *apparaît conséquemment aux yeux de tous comme son équivalent* »[230]. Le parallèle peut être poursuivi puisque, selon le même auteur, « *il reste nécessaire, pour disposer du bien incorporel, de disposer également de son support matériel. Simplement, par l'effet de la représentation, seul le bien représenté sera alors, à ce titre, engagé* »[231]. Le phénomène décrit par Monsieur

---

[227] TLFi, *V°* « Secret », subst. masc.
[228] Sur cette conception, v. *infra*, n° ¤.
[229] G. BEAUSSONIE, *La prise en compte de la dématérialisation des biens par le droit pénal. Contribution à l'étude de la protection pénale de la propriété*, préf. B. DE LAMY, coll. Bibliothèque de droit privé, t. 532, LGDJ, 2012, n° 380 et svt.
[230] *Ibid.,* n° 381.
[231] *Ibid.*.

Beaussonie permet d'expliquer que le *secret-fait* soit perçu au travers de son support, et accessible à travers lui. Pour disposer de l'information, il faut disposer du support ; le support est alors identifié au *secret-fait*. C'est à notre sens la raison pour laquelle se trouvent, à tous les niveaux de discours, des références à la « *protection du secret médical* » ou à la « *protection des informations couvertes par le secret* » sans que ne soit visé le secret professionnel. Cela explique également que se retrouve régulièrement l'expression « *atteinte au secret médical* »[232] pour décrire un accès indu au support et donc à l'information qu'il représente[233], l'atteinte visant ici le *secret-état*. Outre la représentation de l'information, il faut évoquer sa formalisation.

46. Formalisation et accessibilité. La formalisation est le resultat de l'action de *formaliser*, le verbe est notamment utilisé en logique et en mathématiques pour désigner l'action qui consiste à « *Donner, au cours de l'analyse, une forme logique aux éléments d'un problème, abstraction faite de la matière ou du contenu* »[234]. La formalisation nécessite une action qui va au-delà de la simple représentation puisqu'il ne s'agit plus seulement de « *correspondre à quelque chose d'autre, en être le signe, le symbole ou le terme corrélatif* »[235] ou encore de « *représenter aux sens, d'une manière actuelle et concrète, l'image d'une chose* […] *impossible à percevoir directement* »[236]. Elle implique qu'il existe des conventions communes de langages. Se superpose donc à la représentation, comme relation liant le support à l'information, la formalisation qui consiste dans l'action du professionnel à donner une forme particulière à l'écrit. Pourtant, certaines instances en ont donné une définition plus large qui rapprocherait la formalisation de la représentation, puisqu'il s'agirait simplement de « *donner un support* »[237].

---

[232] Par ex., TA Montreuil, 14 juin 2012, n° 1009924.
[233] L'article L. 311-6 du Code des relations entre le public est l'administration traite des documents dont la communication porterait « atteinte au secret médical ».
[234] TLFi, *V°* « Formaliser ».
[235] *V°* « Représentation », Sens C., *in* A. LALANDE, *Vocabulaire technique et critique de la philosophie*, coll. Quadrige, PUF, 3e éd., 2010.
[236] *V°* « Représentation », Sens D., *in* A. LALANDE, *op. cit.*
[237] « […] *il s'agit des informations auxquelles est donné un support (écrit, photographie, enregistrement, etc.) avec l'intention de les conserver et sans lequel elles seraient objectivement inaccessibles. Ces informations sont destinées à être réunies dans ce qu'il est habituel d'appeler le dossier de la personne* » (*Recommandations pour la pratique clinique relatives à l'accès aux informations concernant la santé d'une personne*, élaborées par le service des recommandation professionnelles de l'ANAES, févr. 2004, mise en ligne le 24 mars 2004, <www.anaes.fr>). Selon l'explication donnée par deux auteurs, portant spécifiquement sur le fait de savoir si les notes du médecin peuvent être considérées comme des documents formalisés et, en ce sens, être intégrées au dossier du patient : « *La plupart des dictionnaires donnent du verbe formaliser la définition suivante : mettre en forme (de l'anglais to formalize). L'écriture étant définie communément comme la formalisation de la pensée, la représentation d'un langage oral. Le manuscrit, quant à lui, consistant en une écriture manuelle. On le voit, donc, l'écriture manuelle est bien une formalisation du travail de réflexion d'amont du professionnel de santé et devrait,*

En toute hypothèse, il apparaît que la formalisation des informations, au sens le plus strict, suppose une forme qui en permet la compréhension. Ainsi, représentation et formalisation sont les conditions sans lesquelles l'information ne peut être accessible. Cette accessibilité potentielle implique la protection du *secret-fait* et impose, au-delà du silence du professionnel, une attitude positive. En outre, la formalisation des informations étant le fruit de la pensée du professionnel, la question de la propriété des informations a pu être discutée[238].

§ 2 - La protection du support

47. Le couple représentation/formalisation rend possible l'accès à l'information, ce qui implique, en droit, que pour maintenir l'état de secret à l'égard des tiers à la relation, le *secret-fait* – soit l'information secrète représentée et formalisée – doit être spécifiquement spécifiquement protégé. Il importe donc d'en contrôler l'*accès*. Depuis la loi du 17 juillet 1978, les citoyens se sont vu reconnaître droit d'accès à certains documents, support de l'information secrète. Leur double qualification de documents administratifs et d'informations couvertes par le secret entraîne un contrôle strict des accès **(A)**. D'autres mécanismes imposent la préservation du support de l'information secrète **(B)**.

à ce titre, être communicable. Les textes litigieux d'ailleurs font à plusieurs reprises référence à des écrits intégrant expressément le dossier du patient sans distinguer si ces écrits reçoivent une forme dactylographiée ou restent à l'état manuscrit (d'échanges écrits entre professionnels de santé, feuilles de surveillance, correspondances entre professionnels de santé, la lettre du médecin qui est à l'origine de la consultation ou de l'admission...).La maxime latine ubi lex non distinguit nec nos non distinguere debemus, nous incline, alors, à ne pas distinguer entre les différentes formalisations, la loi n'ayant pas réalisé un tel distinguo. » (F. VIALLA et E. TERRIER, « Existe-t-il des notes personnelles ? Points de vue divergents », *RDS* 2005, n° 5, p. 201).

[238] La question de la qualification des notes personnelles du médecin a été débattue. Les professionnels de santé, et particulièrement les médecins, souhaitaient que leur soit refusée la qualification de document administratif nominatif, ce qui aurait pour effet d'empêcher le malade concerné par les notes d'y avoir accès (CSP, art. R. 4127-5 tel que modifié par le décret n° 2012-694 du 7 mai 2012 portant modification du code de déontologie médicale). La CADA affirme de manière constante que les notes doivent être communiquées dès lors qu'elles ont participé à l'élaboration du diagnostic (Conseil du 15 avr. 2004, n° 20041645-MNC ; Avis n° 20150229, Séance du 19 mars 2015 ; CAA, Paris, 30 sept. 2004, req. n° 03PA01769 ; *RDS* 2005, n°5, p. 201, obs. F. VIALLA et E. TERRIER, « Existe-t-il des notes personnelles ? Points de divergents », ; N. MALLET-PUJOL « Droit à et droit sur l'information de santé », *in Le droit des données de santé*, *RGDM* 2004, p. 89, actes du colloques de l'Association Française de Droit de la Santé, Paris, 25 mars 2004 ; N. VIGNAL, « L'accès au dossier médical », *LPA* 19 juin 2002, n° 122, p. 19 ; C. KOUCHNER, A. LAUDE et D. TABUTEAU, *Rapport sur le droit des malades,* Presses de L'EHESP, 2009 ; J. MORET-BAILLY, « La déontologie médicale, de la résistance à la contre-offensive (à propos du décret du 7 mai 2012 portant modification du code de déontologie médicale) », *RDSS* 2012, p. 1074).

A - Le contrôle de l'accès aux documents administratifs

48. Le contrôle de l'accès aux documents administratifs est le corollaire de la reconnaissance d'un droit des personnes à accéder aux documents administratifs les concernant. Le pendant de cette reconnaissance consiste dans une limitation du « secret des papiers » de l'administration **(1)**. La mise en œuvre de cette protection peut être analysée au regard de la doctrine de la Commission d'accès aux documents admninistratifs **(2)**.

1 - La limitation du *secret des papiers*

49. Secrets de l'administration. Comme l'avait formulé le conseiller d'Etat Louis Fougere en 1967, l'administration, dresse à l'égard des personnes qui souhaitent accéder à des informations « *un double barrage légal : le mutisme de ses agents et le secret de ses papiers* »[239]. Le premier de ces barrages est le secret professionnel – le *secret-attitude* – auquel sont soumis tous les agents de la fonction publique[240] et qui protège les secrets des administrés ; il se double d'un devoir de discrétion, qui constitue également un rempart à la connaissance de certaines informations[241]. Le second barrage, le *secret des papiers*, ne renvoie pas, quant à lui, à l'*attitude* de silence que doivent adopter les agents : « *Par secrets des documents, on entend les secrets opposables au droit d'accès aux documents administratifs* »[242] . Autrement dit, *l'attitude de silence* se double d'une préservation des supports. Si la communication de documents secrets peut engager la responsabilité des agents pour violation du secret professionnel[243], le *secret des papiers* ne se confond pas avec lui. Celui-ci ne vise pas la relation entre les agents et les usagers mais la relation entre l'administration et les usagers[244]. Il est

---

[239] L. FOUGERE, « Les secrets de l'administration », *Bull.* II AP, 1967, p. 21; l'expression est reprise par : F. MODERNE « Conception et élaboration de la loi du 17 juillet 1978 » *in Transparence et secret*, 16 et 17 oct. 2003, La documentation française, p. 19 et svt. ; O. BUI-XIAN, « Les secrets de l'administration », *RDP* 2012, p. 1119.

[240] J. GROSCLAUDE, « L'obligation de discrétion professionnelle », *Rev. adm*. 1967, p. 127 et s.

[241] « *L'obligation de discrétion professionnelle est instituée dans l'intérêt du service, pour protéger les "secrets de l'administration"* […] *dont la divulgation pourrait nuire au bon accomplissement de ses tâches. A la différence de l'obligation de réserve qui impose la retenue dans l'extériorisation des opinions, l'obligation de discrétion professionnelle est une obligation de "non-divulgation"* » (R. CHAPUS, *Droit administratif général*, t. II, 10ème éd., Montchrestien, 1997, p. 280).

[242] En ce sens, v. O. BUI-XIAN, « Les secrets de l'administration », *op. cit*.

[243] La violation du secret professionnel implique une révélation volontaire, la forme de la révélation importe peu : v. notamment P. MISTRETTA, *Droit pénal médical*, *op. cit.*, n° 526.

[244] Pour des travaux généraux sur cette question : D. MAILLARD DESGREES DU LOU, *Droit des relations de l'administration avec les usagers,* PUF, 2000.

l'exception à un droit d'accès reconnu aux administrés par les lois dites de transparence[245]. La collecte des informations, essentielle à l'efficacité des politiques de l'Etat et au fonctionnement des administrations[246], impose en premier lieu que l'information soit représentée et formalisée. Le système de santé n'échappe pas à l'inflation de la production des informations. La représentation de l'information, qu'il s'agisse d'informations médicales, administratives ou médico-administratives, s'explique par le besoin des administrations d'utiliser les informations pour assurer leur fonctionnement. Madame Thouvenin a mis en évidence l'importance du statut de l'information secrète, considérant qu'elle se trouve au cœur des difficultés relatives au « secret médical »[247]. Le statut des documents, c'est-à-dire des supports qui incarnent l'information, permet d'apporter un éclairage à nos propos.

50. La qualification de documents administratifs et les dossiers patients. Les informations recueillies par un agent soumis au secret, dès lors qu'elles sont représentées sur un support, deviennent *des documents administratifs*[248]. La notion de document administratif a d'abord été définie à l'article 1 de la loi du 17 juillet 1978[249], lequel a dressé une liste des documents de nature administrative[250] et précisé leur forme[251]. Deux ordonnances sont venues successivement modifier cette définition, la première en date du 6 juin 2005[252] et la seconde le 29 avril 2009[253]. Les modifications opérées ont eu pour effet d'élargir la définition en supprimant les mentions relatives à la forme du document, précisant simplement que « *Sont*

---

[245] J.- D. BREDIN, « Secret, transparence et démocratie », *Pouvoirs* 2001, n° 97, « Transparence et secret », p. 5.
[246] Sur la puissance de l'information comme mode de légitimation et d'évaluation de l'action publique v° V. LASSERRE, *Le nouvel ordre juridique- Le droit de la gouvernance*, LexisNexis, 2015, n° 76 à 97.
[247] D. THOUVENIN, *Le secret médical et l'information du malade*, Presses Universitaire de Lyon, 1982.
[248] B. EVEN, « La notion de document administratif », *AJDA* 1985, p. 521.
[249] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal (*JORF*, 18 juill. 1978, p. 2851).
[250] Loi du 17 juillet 1978, art. 1, al. 2 : « *Sont considérés comme documents administratifs au sens du présent titre tous les documents produits ou reçus par l'administration qu'ils se présentent sous forme écrite (dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, directives, instructions, circulaires...), sous forme d'enregistrement sonore ou visuel ou sous forme numérique ou informatique. Sont également concernées les informations contenues dans des fichiers informatiques et qui peuvent en être extraites par un traitement automatisé d'usage courant* […] ».
[251] Loi du 17 juillet 1978, art. 1, al. 2 : « […] *revêtant la forme d'écrits, d'enregistrements sonores ou visuels, de traitements automatisés d'informations non nominatives* ».
[252] Ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques (*JORF* n° 131, 7 juin 2005, p. 10022).
[253] Ordonnance n° 2009-483 du 29 avril 2009 prise en application de l'article 35 de la loi n° 2008-696 du 15 juillet 2008 relative aux archives (*JORF* n° 0101, 30 avr. 2009, p. 7327).

*considérés comme documents administratifs, (…), quels que soient leur date, leur lieu de conservation, leur forme et leur support, les documents élaborés ou détenus par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées de la gestion d'un service public, dans le cadre de leur mission de service public. Constituent de tels documents notamment les dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, directives, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions et décisio*ns »[254]. Le texte a ensuite fait l'objet d'une codification[255] avant d'être modifié à nouveau par la loi du 7 octobre 2016 pour une République numérique[256]. Au regard de ce qui vient d'être rappelé, ce qui caractérise les *documents administratifs,* outre leur source, n'est pas tant leur forme que le fait qu'elles aient une forme, entendu comme synonyme de support. Les informations recueillies par les professionnels de santé, mais également par tous les professionnels de l'action sociale et ceux exerçant dans un établissement public ou privé ayant des missions de service public, dès lors qu'elles sont formalisées[257], constituent des *documents administratifs*. La formalisation des documents permet une telle qualification lorsqu'ils sont *élaborés ou détenus* par les administrations. Ainsi, les informations confiées à un professionnel soumis au secret dans le cadre d'une prise en charge médicale ou médico-sociale sont des *documents administratifs* spécifiquement protégés. L'existence de supports de l'information est donc centrale et entraîne la nécessité de protéger spécifiquement le *secret-fait* incarné dans le support : si *l'attitude* est une manière *d'être*, une position prise par l'être, la protection du support est, en quelque sorte, une manière *d'avoir*, c'est-à-dire de détenir, de conserver, de maîtriser l'accès.

---

[254] CRPA, art. L. 300-2.
[255] Par l'ordonnance n° 2015-1341 du 23 octobre 2015, il figure désormais à l'article L. 300-2 du Code des relations entre le public et l'administration.
[256] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (*JORF* n° 0235, 8 oct. 2016).
[257] Le terme est notamment utilisé par la CADA pour définir les informations à caractère médical, informations qui constituent des documents administratifs dont l'accès peut être sollicité auprès de la CADA et à propos desquels la Commission précise : « *Les informations à caractère médical sont définies comme l'ensemble des informations concernant la santé [d'une personne] détenues par des professionnels et établissements de santé, qui sont formalisées* » (Fiche thématique, « Informations à caractère médicale », disponible sur le site <www.cada.fr>, dernière consultation le 12 mai 2018).

Au regard de ce qui vient d'être rappelé, les documents contenus dans le dossier médical[258] sont des documents administratifs, et il en est de même du dossier administratif[259]. Depuis la loi du 4 mars 2002, l'article L. 1111-7 du Code de la santé publique prévoit par ailleurs les modalités d'accès direct par le malade, et l'article L. 1110-4 dispose de l'accès par des tiers dans certains cas précisés par le texte[260]. Ces dispositions tracent les contours des restrictions de cet accès[261]. La maîtrise de l'accès est donc à la fois la condition de la mise en œuvre d'un droit et la condition de la protection du secret des informations.

2 - Analyse de la doctrine de la CADA

51. Le *secret médical* exception au droit d'accès aux documents administratifs. L'expression « secret médical » est utilisée par le législateur pour désigner les documents dont le droit d'accès est restreint. Nous nous appliquerons à démontrer que cet usage peut se comprendre au regard de la polysémie du mot *secret* que nous nous sommes astreint à déployer.

---

[258] Le dossier médical dont il est ici question ne se confond pas avec le Dossier médical partagé (DMP). Il s'agit d'un dossier ouvert et tenu par les professionnels prenant en charge le patient dans chaque établissement public ou privé au moment de son séjour. Pour ne pas être confondu avec le DMP, le dossier médical établi au sein de chaque établissement est parfois nommé « dossier patient ». Il est prévu, dans les années à venir, une fusion des dossiers médicaux et du DMP. Toutefois, pour l'instant, il n'est pas rare qu'il existe un dossier papier ou dématérialisé pour un patient dans un ou plusieurs établissements et que celui-ci ait en même temps un DMP qui est, dès sa création, dématérialisé. S'agissant du dossier médical, il est défini, ainsi que son contenu, à l'article R. 1112-2 du Code de la santé publique dans une section consacrée aux « informations des personnes accueillies ». L'article liste les informations devant être formalisées afin de constituer le contenu du dossier médical communicable et précise que les informations recueillies auprès d'un tiers n'intervenant pas dans la prise en charge ne peuvent pas être communiquées à la personne concernée par le dossier médical. Cette disposition constitue une limite au droit d'accès protégeant, cette fois, la vie privée des tiers à la relation de soin (sur ce point, v. notamment CADA, avis n° 20142528, Séance du 18 sept. 2014).

[259] Sur le contenu du dossier administratif v. *Feuill. Mob. Litec Droit médical et hospitalier*, M. DUPONT, Fasc. 9-30 « dossier médical. – Dossier en établissement de santé. Dossier dématérialisé », 16 nov. 2016.

[260] Depuis la loi du 4 mars 2002, l'accès aux dossiers médicaux détenus par les établissements publics de santé et les établissements privés participant au service public de santé est régi par les dispositions combinées de la loi du 17 juillet 1978 et de l'article L. 1111-7 du Code de la santé publique ; aussi, ce dernier régit exclusivement l'accès aux dossiers médicaux détenus par les établissements privés (CADA, 27 févr. 2003, Conseil président commission dptale et spéciale Lozèze : Rapp. 2003, p. 62. – V. également CAA Paris, 29 janv. 2003, AP-HP : Rec. CE 2003, tables, p. 788) - *Adde* J.-Y. VINCENT, « Accès aux documents administratifs- Régime spéciaux- Fichiers-Archives », *Jcl. Adm.* Fasc. 109-20, Nov. 2010 (mis à jour du 17 oct. 2016 par J.-B. AUBY et V. TCHEN).

[261] S'agissant notamment de l'accès au dossier médical des personnes faisant l'objet d'une hospitalisation sans consentement : CE, 9ème et 10ème SSR, 10 avr. 2009, n° 289793, n° 289794 n° 289795, *RDS* 2009, n° 30, p. 341, comm. F. VIALLA (spéc. l'arrêt n° 289794) ; *RDSS* 2009, p. 688, note F. DIEU.

Comme il l'a été évoqué, un droit d'accès aux documents administratifs est reconnu par la loi du 17 juillet 1978[262]. Cette loi, généralement présentée, avec la loi informatique et libertés [263], comme une *loi de transparence,* a eu pour ambition d'améliorer les relations entre l'administration et le public en mettant fin à l'opacité administrative qualifiée de « *manie du secret* » dans les travaux préparatoires de la loi[264]. Pour ce faire, le législateur a affirmé le droit d'accès aux documents administratifs[265] dont les citoyens-administrés[266] sont titulaires, et a créé la Commission d'Accès aux Documents Administratifs[267] chargée de la mise en œuvre de ce droit[268]. L'accès aux documents administratifs est devenu la règle, le *secret des papiers*

---

[262] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, *JORF* du 18 juillet 1978 p. 2851.
[263] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* du 7 janvier 1978 p. 227.
[264] J. THYRAUD, *Avis au nom de la Commission des Lois constitutionnelles, de Législation, du Suffrage universel, du Règlement et d'Administration générale (1), sur le projet de loi*, adopté par l'Assemblée nationale*, portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal*, 1978, n° 378, p. 6.
[265] Pour une étude récente sur la notion de droit d'accès aux documents administratifs et tendant à démontrer que ce droit est élevé au rang de droit fondamental de l'Union européenne : A. GARIN, *Le droit d'accès aux documents : en quête d'un nouveau droit fondamental dans l'Union européenne*, Ed. A. Pedone, 2017.
[266] Le terme est notamment utilisé par F. MODERNE (« Conception et élaboration de la loi du 17 juillet 1978 » *in Transparence et secret*, 16 et 17 octobre 2003 publié à la Documentation française, p. 32) et souligne l'émergence de la démocratie administrative (sur ce point v. V. LASSERE, *Le nouvel ordre juridique. Le droit de la gouvernance*, *op.cit.*, n° 74) et la consécration de la transparence analysée dès les année soixante par J. RIVERO (J. RIVERO, « A propos des métamorphoses de l'Administration d'aujourd'hui : démocratie et administration », *in Mél. Offerts à R. Savatier*, Dalloz, 1965, p. 821 et s.).
[267] Sur le rôle de la CADA et son rapport à la démocratie administrative v. J. – P. LECLERC, « Le rôle de la commission d'accès aux documents administratifs », *RFPA*, 2011, n° 137-138, p. 328.
[268] Ces mécanismes ont fait l'objet d'une abondante littérature. De manière non exhaustive : B. LASSERRE, N. LENOIR et B. STIRN, *La transparence administrative*, coll. Politique d'aujourd'hui, PUF, 1987 ; A.- L. MIE, *L'administration et le droit à l'information : Le secret en question*, coll. L'administration nouvelle, Berger-Levrault, 1985; H. MAISL, *Le droit des données publiques*, coll. Systèmes, LGDJ, 1996 ; D. MAILLARD DESGREEES DU LOU, *Droit des relations de l'administration avec ses usagers*, PUF, 2000, p. 408 et svt. ; B. DELAUNAY, *L'amélioration des rapports entre l'administration et les administrés*, LGDJ, 1993, p. 525 et svt. ; J.- J. GLEIZAL, *Figures du secret*, Presses universitaires de Grenoble, 1986 ; A. de LAUBADÈRE, « Relations entre l'administration et le public », *AJDA* 1978, p. 495; P. DIBOUT, « La liberté d'accès aux documents administratifs », *Rev. adm.* 1979, p. 23 ; J. LAVEISSIÈRE, « Le pouvoir, ses archives et ses secrets », *D.* 1984, chron. p. 63 ; J. LAVEISSIÈRE, « En marge de la transparence administrative : le statut juridique du secret », *in Etudes offertes à Jean-Marie A*uby, Dalloz 1992, p. 181 ; « La communication administration-administrés », *in* D. COLAS (ss. la dir.), *L'État et les corporatisme*s, coll. Droit et sciences politiques, PUF, 1988 ; « Le droit à l'information à l'épreuve du contentieux. A propos de l'accès aux documents administratifs », *D.* 1987, chron., p. 275 ; J. LEMASURIER, « Vers une démocratie administrative : du refus d'informer au droit d'être informé », *RDP* 1980, p. 1239 ; B. LASSERRE, « La Commission d'accès aux documents administratifs », *Et. et doc. CE* 1981-1982, p. 33 ; « Six ans après le vote de la loi du 17 juillet 1978 : une administration plus transparente ? », *Et. et doc. CE* 1983, p. 99 ; Y. GAUDEMET, « L'administration au grand jour : France », *in Journées de la Société de législation comparée*, 1983, p. 39 ; G. BRAIBANT, « Droit d'accès et droit à l'information », *in Mélanges offerts au professeur Robert-Edouard Charlier*, éd. de l'Université et de l'enseignement moderne, 1981, p. 703 ; A. HOLLEAUX, « Les lois de la troisième génération des droits de l'homme : ébauche d'étude comparative », *Rev. franç. adm. publ.* 1980, n° 15, p. 45 ; A. ROUX, « La transparence administrative en France », in *Ann. eur.*

l'exception[269] comme en atteste le succès de la formule « *transparence administrative* »[270]. Les articles 2 et suivants de la loi du 17 juillet 1978[271] prévoyaient les conditions d'accès aux documents administratifs. Désormais codifié aux article L. 311-1 et suivants du Code des relations entre le public et l'administration, ce droit connaît des limites à son étendue, tenant à l'intérêt public[272] mais également au respect de certains secrets. Ainsi, l'article L. 311-6 du même code prévoit : « *Ne sont communicables qu'à l'intéressé les documents administratifs :* 1° *Dont la communication porterait atteinte à la protection de la vie privée, au* ***secret médical*** *et au secret en matière commerciale et industrielle* (…) »[273]. Au travers des documents administratifs, le droit administratif protège le *secret des informations relatives à la personne*. Est visé ici le *secret-état*, lequel est garanti par le refus de communiquer le document auquel

---

Actes du colloque pour le XXVe anniversaire de la loi du 17 juillet 1978 sur l'accès aux documents administratifs adm. publ., éd. CNRS, 1989, p. 57 *;* D. LINOTTE, « Chronique des réformes administratives françaises », *RDP* 1978, p. 1417 ; P. SADRAN, « Le miroir sans tain. Réflexions sur la communication entre l'administration et les administrés », *in Mélanges en hommage à Jacques Ellul*, PUF, 1983, p. 802 ; B. EVEN, « La notion de document administratif », *AJDA*, 1985, p. 521 ; CE, « La transparence et le secret », *Rapport public,* 1995, *Et.et doc*. *CE,* 1996, p. 17 ; CE, *Pour une meilleure transparence de l'administration. Etude sur l'accès des citoyens aux données publique*s, La documentation française, 1997 ; F. MODERNE, « Conception et élaboration de la loi du 17 juillet 1978 » *in Transparence et secret*, 16 et 17 oct. 2003, La documentation française, p. 19.

[269] O. BUI-XIAN, « Les secrets de l'administration », *RDP* 2012, p. 1119.

[270] H. MAISL, *Le droit des données publiques, op. cit*., p. 3 et svt.

[271] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, *op. cit.*.

[272] L'article L. 311-5 du CRPA prévoit en effet que ne sont pas communicables « *Les avis du Conseil d'Etat et des juridictions administratives, les documents de la Cour des comptes mentionnés à l'article L. 141-10 du code des juridictions financières et les documents des chambres régionales des comptes mentionnés à l'article L. 241-6 du même code, les documents élaborés ou détenus par l'Autorité de la concurrence dans le cadre de l'exercice de ses pouvoirs d'enquête, d'instruction et de décision, les documents élaborés ou détenus par la Haute Autorité pour la transparence de la vie publique dans le cadre des missions prévues à l'article 20 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique, les documents préalables à l'élaboration du rapport d'accréditation des établissements de santé prévu à l'article L. 6113-6 du code de la santé publique, les documents préalables à l'accréditation des personnels de santé prévue à l'article L. 1414-3-3 du code de la santé publique, les rapports d'audit des établissements de santé mentionnés à l'article 40 de la loi n° 2000-1257 du 23 décembre 2000 de financement de la sécurité sociale pour 2001 et les documents réalisés en exécution d'un contrat de prestation de services exécuté pour le compte d'une ou de plusieurs personnes déterminées ; 2° Les autres documents administratifs dont la consultation ou la communication porterait atteinte : a) Au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif ; b) Au secret de la défense nationale ; c) A la conduite de la politique extérieure de la France ; d) A la sûreté de l'Etat, à la sécurité publique ou à la sécurité des personnes ; e) A la monnaie et au crédit public ; f) Au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, sauf autorisation donnée par l'autorité compétente ; g) A la recherche, par les services compétents, des infractions fiscales et douanières ; h) Ou sous réserve de l'article L. 124-4 du code de l'environnement, aux autres secrets protégés par la loi* ». Pour un développement exhaustif concernant les limites du droit d'accès, v. A. LALLET, *Rép. cont. admin.*, *V°* « Documents administratifs : accès et réutilisation », déc. 2014 (mise à jour déc. 2017).

[273] Nous soulignons.

est identifié le *secret-fait*. Le droit saisit plus aisément ce qui est matériel[274] et la première fonction des dispositifs techniques de l'information les plus archaïques consiste dans l'opération de donner corps à ce qui est incorporel pour garder mémoire et communiquer[275]. Le *secret* s'incarne ainsi dans les documents constituant le dossier médical[276]. La restriction d'accès – à coté du *secret-attitud*e – aux documents administratifs constitue donc un mode de protection du *secret médical – secret-état* –, donc nécessairement du *secret des informations relatives à la personne – secret-fait* confondu avec son support – tel que prévu à l'article L. 1110-4 du Code de la santé publique.

52. Contrôle de la CADA et atteinte au « secret médical ». La CADA a une mission de renseignement et rend des avis constituant une voie de recours précontentieuse[277] pour les personnes auxquelles l'accès à des documents administratifs est refusé. Le discours de la Commission, dans ses avis et rapports, semble confirmer l'idée selon laquelle le document est identifié au *secret-fait,* et qu'à travers lui, le *secret-état* est préservé. Les rapports font notamment mention « *des documents relevant du secret médical* »[278], « *d'informations couvertes par le secret médical* »[279]. A titre d'exemple, la Commission a précisé, dans un rapport d'activité, que les documents médicaux n'étaient pas communicables aux tiers car cette « *communication violerait également le secret médical, protégé à deux reprises par l'article 6 de la loi, dans son sixième alinéa, qui envisage le cas du « secret des dossiers médicaux », et*

---

[274] « *Les rapports du droit et de la matière sont une vieille lune. C'est à se demander s'ils ne commencent pas avec le droit lui-même, qui est tout pétri de mesure* » (F. ZENATI, « L'immatériel et les choses », *Arch. phil. dr.*, t. 43, 1999, p. 79). La conception que l'on se fait du droit a pu être décrite comme « *infestée de matérialisme* » (M. VILLEY, « Préface historique », *in Les biens et les choses en droit*, *Arch. phil. dr.*, t. 24, 1979, p. 2).

[275] Sur ce point, l'analyse de Monsieur Jeanneret, en sciences de l'information et de la communication, est éclairante. Elle dépasse largement notre sujet d'étude, mais au cours de celle-ci, l'auteur souligne la distanciation qui s'opère entre la parole et l'écrit et les supports : « *objets fabriqués qui ont pour propriété d'introduire une médiation entre les hommes dans la production et le partage de la culture et de permettre l'inscription matérielle des productions* » (Y. JEANNERET, *Y-a-t-il (vraiment) des technologies de l'information*, coll. Savoirs Mieux, Presses universitaires du Septentrion, 2017, p. 23 et svt.).

[276] Bien que l'ouvrage soit désormais daté, il conserve un intérêt pour la mise en contexte historique du dossier médical ou dossier patient : O. DUPUY, *Le dossier médical*, 2ème éd., coll. Essentiel, LEH, 2005, p. 149 et svt. ; Par ailleurs, selon la CADA, ne sont pas des documents médicaux les documents établis par une autorité administrative, tels qu'un arrêté d'hospitalisation d'office ou le rapport d'un psychologue ou d'un travailleur social, à moins qu'ils ne soient intégrés à un dossier médical (CADA, 4ème et 8ème Rapp., 1986 et 1995, qui dressent un inventaire des documents médicaux et les distinguent des documents sociaux).

[277] CRPA art. L. 342-1 et svt.

[278] CADA, *Rapport d'activité de la commission d'accès aux documents administratifs*, 1984-1985.

[279] CADA, *Rapport d'activité de la commission d'accès aux document administratifs*, 1999-2000, La Documentation française, 2001, p. 34 ; CADA, *Rapport d'activité de la commission d'accès aux document administratifs*, 2002, p. 45, disponible sur <www.cada.fr>.

dans le neuvième, qui vise plus largement les « secrets protégés par la loi » »[280] ou encore l'utilisation des termes « *les informations couvertes par le secret médical* »[281], « *données relatives au secret médical qui figurent à ce dossier* »[282]. Il faut remarquer encore que les registres d'entrées et de sorties des établissements hospitaliers sont, au sens de la loi du 17 juillet 1978, des documents administratifs, dont la communication n'est que rarement autorisée, que ce soit aux personnes concernées par ces hospitalisations ou aux tiers. La CADA rappelle « *qu'afin de préserver le secret médical, seuls les registres d'entrées et de sorties des établissements hospitaliers antérieurs à 1890 sont communicables dans leur intégralité* » en raison de l'application de la loi relative aux archives. L'emploi de ces diverses expressions nous semble montrer que ce n'est pas tant l'attitude du professionnel qui est visée que les mécanismes mis en œuvre pour préserver le *secret-fait* au travers du document qui le représente.

53. La responsabilité de l'administration, un exemple du discours de la doctrine. En dehors de la responsabilité pénale et disciplinaire des agents, *l'atteinte au secret-état*, peut constituer une faute de l'administration, laquelle résulte d'une erreur dans l'organisation du service[283] dans le cas où l'administration n'a pas réussi à protéger les informations secrètes, mais « *elle peut aussi être le résultat d'un dysfonctionnement commis par l'un de ses agents qui, malgré les procédures mises en place, ont divulgué ou laissé fuiter une information* »[284]. Il est ainsi confirmé que l'atteinte au secret des informations n'est pas seulement le fait d'une révélation volontaire de la part de l'agent. Dès lors qu'il existe un support de l'information secrète, cette atteinte peut être le fait d'un dysfonctionnement dont résulte *une fuite*. Un agent qui n'a pas connaissance des informations contenues dans un document peut l'avoir transmis par erreur ; dans une telle hypothèse, l'infraction de violation du secret professionnel ne sera

---

[280] CADA, *Huitième rapport d'activité de la commission d'accès aux documents administratifs*, La Documentation française, 1995, p. 42.
[281] CADA, *Rapport d'activité de la commission d'accès aux documents administratifs*, 2009, p. 12 ; CADA, *Rapport d'activité de la commission d'accès aux document administratifs*, 2012, p. 31.
[282] CADA, Avis du 22 avr. 2010, n° 20101534.
[283] Dans des affaires ne concernant pas spécifiquement la communication indue du dossier médical : CAA, Nancy, 30 mai 2002, *Centre hospitalier Général Maillot*, *AJDA* 2003, p. 35, chron. P. ROUSSELLE ; TA Nice, 9 mars 2007, *AJDA* 2007, n° 0404779, p. 1089, comm. F. DIEU. Sur la responsabilité d'un département, engagée à la suite de la divulgation d'informations relatives à l'identité d'un enfant adopté : CE, 17 oct. 2012, n° 348440 ; *AJDA* 2013, p. 362, note H. RIHAL ; *JCP A* 2013, 2025, note C. VOCANSON ; *RDSS* 2015, p. 440, obs. E. PECHILLON.
[284] E. PECHILLON, *op. cit.*

pas qualifiée mais la personne concernée par les documents en cause pourra engager la responsabilité de l'administration[285] afin que celle-ci l'indemnise du préjudice qu'elle a subi du fait de la communication des documents. Il faut, par ailleurs, souligner l'emploi, dans l'article de Monsieur Péchillon, d'expressions qui trahissent implicitement la différence entre secret professionnel et maintien du *secret-état* par la protection du *secret-fait* au travers de son support : « *la faute de l'administration peut consister en une erreur dans l'organisation du service qui n'est pas parvenu à protéger le « secret »* »[286]. L'auteur utilise les guillemets pour signaler, sans doute, que le terme ainsi employé ne fait pas référence au secret professionnel.

54. Limite à l'accès aux archives publiques et protection du « secret médical ». Les archives publiques sont définies à l'article L. 211-1 du Code du patrimoine. La loi du 17 juillet 1978[287] n'est pas l'unique loi de transparence qui prévoit un droit d'accès à certains documents et, corollairement, des restrictions à l'accès. En effet, la loi n° 79-18 du 3 janvier 1979, désormais intégrée au Code du patrimoine, prévoit la possibilité pour toute personne de consulter librement les documents d'archives publiques en érigeant un certain nombre de délais en fonction de la sensibilité des documents. C'est encore la CADA qui est compétente pour mettre en œuvre ce droit d'accès au travers de ses avis. A l'instar de la loi relative à l'accès aux documents administratifs, le législateur prévoit le droit d'accès aux archives publiques, limité par un certain nombre de restrictions lorsque les documents d'archives présentent un caractère sensible. Avant de préciser ce point, il faut remarquer que les textes relatifs aux archives publiques s'articulent avec les dispositions relatives à l'accès aux documents administratifs – en raison d'une identité de nature –, mais aussi avec le Code de la santé publique[288] et la loi informatique et libertés[289]. Ainsi, l'article L. 211-1 du Code du patrimoine définit les archives comme « *l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu*

---

[285] Ainsi, un établissement hospitalier commet une faute en communiquant le dossier médical d'un patient au médecin-expert d'un compagnie d'assurance, le juge administratif décide « *qu'aux termes de l'article 6 de la loi 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal : « [...] II- Ne sont communicables qu'à l'intéressé les documents administratifs : - dont la communication porterait atteinte au secret de la vie privée et des dossiers personnels, au secret médical [...] »* […] *le centre hospitalier d'Antibes a donc transmis le dossier médical de M. D. en violation des dispositions légales relatives à la protection du secret médical, et a donc commis une faute* » (TA Nice, 9 mars 2007, préc.).

[286] E. PECHILLON, *op. cit*.

[287] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, *op. cit.*.

[288] CSP, art. L. 1111-7.

[289] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité ». L'article L. 211-4 du même code dispose que sont des archives publiques les documents issus de l'activité de l'Etat, des collectivités territoriales, des établissements publics ; des autres personnes morales de droit public ou des personnes de droit privé chargées de la gestion d'un service public, dans le cadre de leur mission de service public. Ces définitions particulièrement larges autorisent deux constats : la forme par laquelle sont représentées les informations importe peu, et les documents administratifs sont nécessairement des archives publiques : « *la qualité d'archives ne s'acquiert pas : les documents naissent archives, ils ne le deviennent pas avec le temps* »[290]. Les dossiers médicaux conservés par les établissements publics et privés participant à une mission de service public de santé sont donc également protégés par le Code du patrimoine. Toutefois, les dossiers médicaux ne sont pas indéfiniment conservés par les établissements. A l'expiration des délais de conservation, l'établissement public ou privé peut détruire les dossiers à condition que l'administration des archives publiques ne souhaite pas conserver ceux qui présenteraient un intérêt scientifique, statistique ou historique[291]. Dans tous les cas, que le dossier ait été conservé par l'établissement ou par l'administration des archives, l'article L. 213-2, I, 2° du Code du patrimoine prévoit un délai de communication de « *vingt-cinq ans après le décès de l'intéressé*, *pour les documents dont la communication porte* ***atteinte au secret médical****. Si la date du décès n'est pas connue, le délai est de 120 ans à compter de la date de naissance de la personne en cause* »[292]. Le « secret médical » – état – est donc préservé au-delà du décès de l'intéressé, ce qui le distingue de la protection accordée au secret de la vie privée au regard des délais de consultation des archives[293]. En effet, l'article

---

[290] C. GUYON, « Le concept d'archives : d'une définition à l'autre », disponible sur <https://hal.archives-ouvertes.fr/hal> (dernière consultation le 21 mai 2019), p. 1.
[291] CSP, art. R. 1112-7.
[292] Code du patrimoine, art. L. 213-2.
[293] Cette distinction est nette concernant le droit à l'anonymat du don de gamète et résultant d'un accouchement sous X. Ceux-ci relèvent d'une prérogative inhérente au droit au respect de la vie privée (droit à l'anonymat) et les délais d'accès aux informations sont ceux fixés par le texte en matière d'atteinte à la vie privée, c'est-à-dire cinquante ans à compter de la date d'élaboration du document : TA Montreuil, 14 juin 2012, n° 1009924, *AJDA* 2012, p. 1188 ; *D.* 2012, p. 1618, obs. A. MIRKOVIC ; *AJ fam.* 2012, p. 408, obs. C. XEMARD ; Cons. const., 16 mai 2012, n° 2012-248 QPC ; *AJDA* 2012, p. 1036 ; *AJ fam.* 2012, p. 406, obs. F. CHENEDE ; *RDSS* 2012, p. 750, note D. ROMAN ; *RTD civ.* 2012, p. 520, obs. J. HAUSER ; CE, 10ème et 9ème SSR, 12 nov. 2015, n° 372121 ; *AJDA* 2015, p. 2175 ; *D.* 2015, p. 2382 ; *D.* 2016, p. 752, obs. J.-C. GALLOUX et H. GAUMONT-PRAT ;

L. 213-2, I, 3° prévoit un délai de « *cinquante ans à compter de la date du document ou du document le plus récent inclus dans le dossier, pour les documents dont la communication porte atteinte* […] *à la sécurité des personnes ou à la protection de la vie privée* »[294]. Cette protection des faits secrets au travers de leur support ne concerne pas uniquement les dossiers médicaux mais toutes les informations formalisées, telles que les registres des établissements de santé, qu'il s'agisse des registres de naissance, de décès, d'entrée et de destination des corps, lesquels ne sont librement communicables qu'une fois les délais expirés pour toutes les personnes mentionnées sur ces registres[295]. Car, selon le Conseil d'Etat[296], lorsque les documents comportent des informations sur la nature et la durée des l'affection des patients et dont l'occultation est impossible en raison de la nature et du volume des documents, ceux-ci doivent être regardés comme portant sur des informations relatives à la santé « *dont la communication serait susceptible de porter atteinte au secret médical* »[297]. Le terme de « secret médical » vise bien, ici encore, le *secret des informations relatives à la prise en charge des personnes par les professionnels intervenant dans le système de santé*, c'est-à-dire un état dont le maintien dépend de la protection du support.

55. Un rempart à la transparence. La préservation du secret des documents et des archives en matière administrative constitue donc une limite à la transparence de l'administration. Si l'exigence de transparence est un gage de l'amélioration entre les administrés et l'administration[298] celle-ci ne doit pas porter atteinte aux individus dont les informations sont recueillies et formalisées, l'excès de transparence est nuisible comme l'excès de secret. La préservation du *secret-fait* n'est toutefois nécessaire qu'en raison de l'existence d'un média. La représentation de l'information secrète nécessite une protection spécifique du secret-fait au travers de celui-ci.

AJ fam. 2015, p. 639, obs. A. DIONISI-PEYRUSSE ; *Dr. fam.* 2016, étude 1, obs. J.-R. BINET ; *JCP G* 2016, 62, note A. MIRKOVIC ; *RTD civ.* 2016, p. 334, obs. J. HAUSER.

[294] Code du patrimoine, art. L. 213-2, I, 3°. Pour un exemple d'avis de la CADA concernant la demande de communication d'un ascendant et de l'avis favorable en raison de l'expiration du délai de vingt-cinq ans à compter de la date du décès : CADA, Avis du 16 avril 2009, n° 20091253.

[295] CADA, Avis du 31 mars 2005, n° 20051366-LV ; CADA, Conseil du 21 déc. 2010, n° 20104684.

[296] CE, 10ème et 9ème SSR, 19 juill. 2010, *Fristot et Charpy*, n° 334014 ; *Dr. adm.* 2010, n° 11, p. 41, note P. RAIMBAULT ; *AJDA* 2010, p. 1930, chron. D. BOTTEGHI et A. LALLET.

[297] CADA, Conseil du 21 déc. 2010, n° 20104684.

[298] B. DELAUNAY, *L'amélioration des rapports entre l'administration et les administrés*, LGDJ, 1993, p. 525 et svt.

B - La protection juridique et déontologique du support

56. Il s'agira d'envisager les mécanismes de protection des documents contenant des informations secrètes inscrit dans le Code de la santé publique **(1)** ainsi que le devoir déontologique imposant de préserver la confidentialité des documents **(2)**.

1 - La protection des documents dans le Code de la santé publique

57. Protection des documents contre la curiosité des tiers. L'article 38 du décret du 17 avril 1943[299] pose, pour la première fois, une obligation de protection des documents afin de garantir le *secret* à l'égard des tiers : « *Le dossier médical du malade est conservé dans le service de l'hôpital, sous la responsabilité du médecin chef de service* […] *Toutes mesures seront prises pour que le secret médical soit rigoureusement observé.* ». Les conditions de conservation des dossiers médicaux sont ensuite prévues par un arrêté interministériel du 11 mars 1968 portant règlement des archives hospitalières[300]. Il mentionne par exemple, dans son article 8, qu'un local spécifique et fermé à clef doit être affecté aux archives. L'article R. 1112-7 du Code de la santé publique est ensuite venu confirmer cette obligation, dont le directeur est débiteur, tant pour les établissements publics que privés[301] : « […] *le directeur de l'établissement veille à ce que les dispositions soient prises pour assurer la garde et la* ***confidentialité*** *des informations de santé* […] *conservées* »[302].

58. De la confidentialité. Le terme *confidentialité* est apparu au XX^e^ siècle, issu de l'anglais *confidentiality*, qui est *l'état* d'une information ou d'une chose[303]. Cet *état* est synonyme de

---

[299] Décret n° 43-891 portant règlement d'administration publique pour l'application de la loi du 21 décembre 1941 relative aux hôpitaux et hospices publics (*JORF,* 27 avr. 1943).
[300] Arrêté interministériel du 11 mars 1968 portant règlement des archives hospitalières (*JORF*, 25 oct. 1968, p. 10039).
[301] L'article R. 1112-7 du Code de la santé publique, plusieurs fois modifié, opérait une distinction, dans sa rédaction initiale (Décret n° 2002-637 du 29 avril 2002), entre les établissements publics de santé et les établissements privés participant à l'exécution des services hospitaliers d'une part, et les établissements privés ne participant pas à une telle mission, d'autre part. Cette distinction a ensuite été supprimée. Par un décret du 4 janvier 2006 (Décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique (*JORF*, 5 janv. 2006)), un ajout a été opéré et l'article vise désormais « *la garde et la confidentialité des informations ainsi conservées ou hébergées* ». Sur l'hébergement des données de santé.
[302] CSP, art. R. 1112-7 (Nous soulignons).
[303] TLFi, *V°* « Confidentialité ».

secret mais vise spécifiquement, dans un premier sens, les documents et les conditions de leur utilisation[304]. En ce sens, il nous semble que la confidentialité des informations correspond au fait d'assurer le *secret-état* par la protection du support, *secret-fait*. Nous verrons ultérieurement qu'à l'instar du *secret*, le mot est polysémique et qu'il est doté d'un sens spécifique, mais proche, en matière de traitement de données[305]. La confidentialité a parfois été assimilée à la vie privée[306], sa polysémie le rendant propre à tous les emplois. Si la rigueur terminologique s'impose au juriste, celle-ci ne doit pas être vaine. Le plaisir du mot juste ne peut, seul, guider sa recherche. Or, s'agissant du secret professionnel et de ses avatars, le risque de confusions impose cette rigueur[307], en premier lieu pour ceux qui ont le devoir de respecter ces règles juridiques. Certains auteurs ont pu affirmer, par exemple, que la confidentialité consistait dans la protection des informations circulant entre les professionnels dans le cadre du secret partagé[308]. Madame Zorn définit, quant à elle, la confidentialité en la distinguant du secret professionnel : elle affirme que « *le respect de la confidentialité* […] *est une obligation pesant sur toute personne en vertu de l'article 9 du Code civil* »[309] , contrairement, selon elle, au secret professionnel. Cette assimilation de la confidentialité à la matrice de la vie privée n'est pas, à notre sens, satisfaisante, de même que l'idée selon laquelle la confidentialité serait propre à la communication. S'agissant de la confidentialité comme conséquence du respect de la vie privée, l'exemple de la confidentialité des correspondances des avocats – devoir déontologique – permet d'apporter un éclairage nouveau. Ce devoir s'applique, en effet, indépendamment de

---

[304] « *[En parlant d'un document et des conditions de son utilisation] Privé, secret. Document, dossier confidentiel ; note confidentielle* » (TLFi, *V°* « Confidentialité »).
[305] Ce que nous envisagerons ultérieurement.
[306] C. ZORN, *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, coll. « Santé, qualité de vie et handicap », PUN, 2010, n° 32 et svt.
[307] La jurisprudence offre deux exemples de cette confusion entre le devoir de confidentialité des correspondances qui incombe aux avocats (Règlement intérieur national de la profession d'avocat , art. 3) et le secret professionnel auquel les avocats sont soumis : à propos de la communication d'un avis déontologique par un avocat dans le cadre d'un contentieux de droit commun qui l'opposait à un confrère, la Cour de cassation utilise successivement les deux termes pour répondre à une question portant uniquement sur la confidentialité des correspondances (civ. 1re, 22 sept. 2011, n° 10-21219, *Bull. civ.* I, n° 148 ; *JCP G* 2011, 1643, note Y. REPIQUET ; *Gaz. Pal.,* 25 oct. 2011, p. 13, chron. F.-X. MATTEOLI ; 8 nov. 2011, p. 12, note D. PIAU ; 11 déc. 2011, p. 16, note J. VILLACEQUE ; *D.* 2011, jur., p. 2979, note Y. AVRIL ; *D.* 2013, p. 136, pan. T. WICKERS). Dans une affaire plus ancienne, concernant la possibilité pour un avocat de verser aux débats des correspondances adressées à un confrère : civ. 1re, 4 févr. 2003, 00-10057, *Bull. civ.* I, n° 33 ; *JCP G* 2003, 400, note J. SAINTE-ROSE ; 717, obs. L. CADIET ; *Gaz. Pal.,* 6 mai 2003, p. 6, chron. B. VAN DE MOORTEL, « Confidentialité et secret professionnel – Pour en finir avec la confusion ».
[308] J.-M. VARAUT et L. RUET, « Secret professionnel et confidentialité dans les professions juridiques et judiciaires », *Gaz. Pal.*, 12 août 1997, p.1054.
[309] C. ZORN, *Données de santé et secret partagé- Pour un droit de la personne à la protection de ses données de santé partagées*, *op. cit.*, n° 33.

toute référence à la vie privée en ce qu'il concerne en premier lieu les échanges entre confrères, ces échanges pouvant porter sur n'importe quel sujet sur lequel souhaitent s'entretenir les professionnels sans qu'il ait nécessairement un lien direct avec un client ou une affaire. Le contenu de la correspondance importe donc peu. Cette idée est confortée par une exception : la mention « officielle » retire à la correspondance son caractère confidentiel[310]. De manière plus générale, Madame Peltier souligne que le secret des correspondances est un secret subjectif[311] : ce n'est pas tant son contenu qui importe que la volonté des individus de s'adresser à une personne déterminée[312]. Si un individu envoie, dans une correspondance, un article de presse ou une recette de cuisine, cette correspondance n'en sera pas moins confidentielle. La confidentialité désigne bien, alors, les conditions de l'utilisation du document, le mode d'expression choisi. La violation de la confidentialité pourra ainsi être réprimée au regard de l'article 226-15 du Code pénal[313]. Ensuite, le point de vue selon lequel « *la confidentialité elle-même est faite pour communiquer* »[314] n'est pas, à notre sens, exact. La confidentialité des informations est relative à la *forme d'expression*. En ce sens, la confidentialité est donc la protection de la forme de l'expression[315], une telle protection ne suppose pas nécessairement le partage d'une information. Ainsi posé, le lien entre la confidentialité et le mode d'expression explique que la préservation du *secret-fait* peut être assurée par la confidentialité des documents qui en sont le support. Si les définitions ne sont pas transposables d'une discipline à une autre

---

[310] La confusion entre secret professionnel et confidentialité s'exprime également dans la rédaction de l'article 3 du Règlement intérieur de la profession d'avocat qui dispose que l'apposition de la mention officielle est une « *exception au secret professionnel* ». Il n'en est pourtant rien puisque, comme l'exprime un auteur, « *C'est la confidentialité, et non le secret professionnel, qui interdit de remettre au client le double d'une lettre adressée au confrère adverse ou reçue de lui. C'est le secret professionnel, et non la confidentialité, qui interdit a priori la saisie d'une correspondance échangée avec le confrère adverse. Tandis que le secret professionnel protège la confidence faite par le client et est opposable au confrère adverse, la confidentialité protège la confidence faite par le confrère adverse et est opposable au client* ». Cet auteur propose, par ailleurs, de supprimer la mention du « secret professionnel » de l'article 3.2 du RIN (B. VAN DE MOORTEL, « Confidentialité et secret professionnel – Pour en finir avec la confusion », *op. cit.*).

[311] V. PELTIER, *Le secret des correspondances*, préf. P. CONTE, PUAM, 1999, n° 11.

[312] *Ibid.*

[313] C. pén. art. 226-15.

[314] B. VAN DE MOORTEL, « Confidentialité et secret professionnel- Pour en finir avec la confusion », *op. cit.*

[315] En ce sens, v. E. DREYER, *Droit pénal spécial*, 3ème éd., coll. Cours magistral, Ellipses, 2016, n° 437 : à propos d'un des éléments constitutifs de l'infraction prévue à l'article 226-1 du Code pénal qui punit, entre autres, la captation de parole sans le consentement de la personne qui les prononce. Peut encore être citée à titre d'exemple la classification des documents couverts par le secret de la défense : la mention « Confidentiel défense » ne constitue qu'une gradation du secret, elle relève donc d'un mode d'expression plus ou moins discret dont découlent les conditions de son utilisation.

– et même, parfois, d'une branche du droit à une autre –, notre propos peut néanmoins trouver une illustration en procédure pénale. L'article R. 57-6-1 du Code de procédure pénale relatif à la confidentialité des documents dans l'établissement pénitentiaires dispose : « *Une personne détenue peut, à tout moment, remettre au greffe de l'établissement pénitentiaire, sous pli fermé, en vue de leur conservation et de la préservation de leur caractère confidentiel tous documents personnels, dont elle est détentrice lors de son écrou ou qui lui sont adressés ou remis pendant sa détention* […] »[316]. La confidentialité, ainsi conçue, ne concerne pas uniquement des communications mais s'applique nécessairement à des informations représentées et dont les conditions d'utilisation sont définies subjectivement. L'obligation de garantir la confidentialité qui incombe au directeur d'un établissement de santé s'entend alors comme l'obligation de veiller à protéger le mode d'expression, c'est-à-dire, dans notre hypothèse, le support.

2 - La confidentialité des documents, un devoir déontologique

59. Le devoir de veiller à la confidentialité des documents. Les codes de déontologie des professionnels de santé[317], à l'instar du Code de déontologie des médecins[318], posent un devoir de protection de la confidentialité des documents représentant des informations concernant les personnes prises en charge. Ils doivent, à ce titre, « *garantir le secret* […] *par rapport aux documents médicaux* »[319]. Il importe, même s'ils ne sont pas partagés ou échangés, que les documents bénéficient d'une protection que l'on pourrait qualifier de *technique*. Les professionnels de santé doivent « *protéger contre toute indiscrétion* […] *le contenu et le support de ces informations* »[320]. La garantie de la confidentialité est un moyen de protection du *secret-fait*, incarné dans un support et conservé. Ce devoir est donc intimement lié à la représentation des informations secrètes et s'impose même pour les notes personnelles du

---

[316] CPP, art. R. 57-6-1.
[317] S'agissant des infirmiers et infirmières, l'article R. 4312-28 du Code de la santé publique dispose : « *L'infirmier ou l'infirmière, quel que soit son mode d'exercice, doit veiller à la protection contre toute indiscrétion de ses fiches de soins et des documents qu'il peut détenir concernant les patients qu'il prend en charge* » ; ou encore s'agissant des chirurgiens-dentistes, l'article R. 4127-208 : « *En vue de respecter le secret professionnel, tout chirurgien-dentiste doit veiller à la protection contre toute indiscrétion des fiches cliniques, des documents et des supports informatiques qu'il peut détenir ou utiliser concernant des patients* ».
[318] Le devoir de confidentialité se décline, dans le Code de déontologie des médecins, de deux manières : en veillant « *qu'aucune atteinte ne soit portée par son entourage au secret qui s'attache à sa correspondance professionnelle* » (CSP, art. R. 4127-72) et en protégeant « *contre toute indiscrétion les documents médicaux, concernant les personnes qu'il a soignées ou examinées, quels que soient le contenu et le support de ces documents* ».
[319] M. GIRER, « Droits des patients et exercice en société », *RDSS* 2014, p. 434.
[320] *Ibid.*

médecin[321], lesquelles ne sont pas vouées à circuler. En somme, l'obligation de confidentialité pourrait s'analyser comme le pendant du *secret-attitude* : l'extériorité du support de l'écrit « *vis-à-vis du support strictement biologique de la parole* »[322] implique une mise en œuvre positive. Le secret « objet » représenté est doonc protégé par des mécanismes différents du secret professionnel.

Section 2 - La dissociation du support et des informations

60. Les supports de l'information secrète, puisqu'ils incorporent celle-ci, sont également protégés de l'attitude des tiers. A cet effet, le droit pénal spécial offre des ressources complémentaires bien que non spécifiques à notre objet **(paragraphe 1)**. Les dispositifs techniques de l'information et de la communication permettant de se saisir de l'information à distance sans se saisir de son support. Pour sanctionner ces faits le droit pénal spécial à fait l'objet d'adaptations tant législatives que prétoriennes **(paragraphe 2)**.

§ 1 - La soustraction du support de l'information secrète

61. Deux infractions permettent de sanctionner l'appréhension du support de l'information secrète. Le vol **(A)** et l'infraction sanctionnant l'atteinte au secret des correspondance **(B)**.

A - Le vol du document fixant des informations secrètes

62. La chose soustraite, chose d'autrui, condition préalable de l'infraction. La jurisprudence a développé une conception large de la chose susceptible de vol. Il doit s'agir d'un « *objet matériel* »[323] approprié. La preuve de la propriété n'est toutefois pas exigée, il

---

[321] CSP, art. R. 4127-73.
[322] Y. JEANNERET, *Y-a-t-il (vraiment) des technologies de l'information ?*, *op. cit.*, pp. 23-56.
[323] E. DREYER, *Droit pénal spécial*, *op. cit.*, n° 880 ; *Contra* crim., 20 mai 2015, n° 14-81336, *Bull. crim.*, n° 119 ; *D.* 2015, p. 1466, note L. SAENKO ; *ibid.* p. 2465, obs. G. ROUJOU DE BOUBEE, T. GARE, C. GINEST, M.-H. GOZZI et S. MIRABAIL ; *AJ pénal* 2015, p. 413, note E. DREYER ; *JCP G* 2015, 887, note G. BEAUSSONIE ; *Dr. pén.* 2015, comm. 107, note M. VERON ; *ibid.* comm. 123, note P. CONTE ; *ibid.* chron. 10, obs. A. LEPAGE ; *Gaz. Pal*. 18 juin 2015, p. 8, note S. DETRAZ ; *RSC* 2015, p. 860, obs. H. MATSOPOULOU ; *Ibid.* p. 887, obs. J. FRANCILLON ; *RTD com.* 2015, p. 600, obs. B. BOULOC ; *RTD eur.* 2016, p. 374, obs. E. MATRINGE ; *RDC* 2015, p. 951, note P. BERLIOZ ; *LPA*, 29 juill. 2015, n° 150, p. 15, obs. E. CHAUVIN ; *PI* janv. 2016, p. 97, obs. M. VIVANT.

suffit, pour entrer en voie de condamnation, que la chose soit appropriée par une personne[324], qu'importe que son propriétaire ne soit pas identifié[325]. Toutefois, la chose doit nécessairement appartenir à autrui, sans quoi l'infraction n'est pas constituée[326]. A l'instar du dossier pénal, si la nature des documents médicaux et plus spécifiquement celle du dossier médical est pertinente **(1)**, seule la question de son appropriation mérite d'être posée afin de déterminer la possibilité de sa soustraction **(2)**.

1 - Le dossier médical, un bien

63. La valeur du dossier médical en question. A l'occasion d'une étude portant sur la communication du dossier pénal, Monsieur Ribeyre[327] propose d'analyser la question de la propriété du dossier pénal en s'intéressant en premier lieu à sa valeur pour en déduire sa qualification de bien. L'auteur explique notamment que le support physique de l'information – papier – ne présente pas de valeur particulière. Il faudrait alors rechercher la valeur du dossier – médical ou pénal – ailleurs que dans son support. Aussi souligne-t-il que « *ce qui confère une valeur bien supérieure à ces objets réside dans leur contenu* […]. *L'information contenue dans un dossier* […] *revêt incontestablement une certaine valeur, l'économie reconnaissant la valeur de l'immatériel* »[328]. L'auteur précise encore que la valeur reconnue à l'immatériel suffirait à reconnaître l'information comme un bien[329] dès lors que celle-ci est utile et rare et de déduire sa rareté de son caractère secret[330]. La valeur de l'information contenue dans le dossier pénal – objet de son étude – tiendrait également au fait qu'elles sont constituées de données formalisées : « *Les informations brutes acquièrent une valeur ajoutée, plus-value qu'on peut qualifier de documentaire* »[331]. Précisément, l'auteur démontre la valeur du dossier pénal au

---

[324] Crim., 26 juill. 1928*, Bull. crim*., n° 226. ; crim., 11 mars 1942*, Bull. crim*., n° 23.
[325] Crim., 25 oct. 2000, *Dr. pén.* 2001, comm. 18, note M. VERON ; *JCP G* 2001, II, p. 10566, note P. MISTRETTA ; *D.* 2001, p. 1052, note T. GARE.
[326] Ainsi, les *res nullius* (Bordeaux, 29 nov. 1893, *DP* 1894, 2, p. 86 ; T. corr. Montbéliard, 28 juin 1963, *S.* 1963, p. 299, *D.* 1963, p. 544 ; Bordeaux, 25 juill. 1856, *Journ. dr. crim*. p. 630 ; E. GARÇON, *op. cit.*, sous art. 379, n° 511 ; T. corr. Avignon, 30 sept. 1965, *Gaz. Pal.* 1965, 2, p. 347 ; *D.* 1966, somm. 11) et les *res derelictae* (Crim., 12 avr. 1850, *DP* 1850, 1, p. 142 ; Colmar, 13 déc. 1951, *D.* 1952, p. 132) ne sont pas susceptible de faire l'objet d'un vol.
[327] C. RIBEYRE, *La communication du dossier pénal*, préf. P. MAISTRE DU CHAMBON, PUAM, 2007, sur la propriété du dossier pénal, spéc. n° 546 à 582.
[328] *Ibid.*, n° 548.
[329] F. ZENATI, « L'immatériel et les choses », *Arch. phil. dr*., *Le droit de l'immatériel*, t. 43, 1999, p. 82.
[330] C. RIBEYRE, *La communication du dossier pénal*, *op. cit.*, n° 549 : « *La rareté de l'information créant la valeur, n'importe quel dossier secret présente une valeur.* »
[331] *Ibid.,* n° 552.

détour de la valeur de l'information secrète et enrichie « *à la suite de sa sélection, de sa compilation, de son classement, de sa corrélation* »[332]. Cette approche pourrait tout à fait être transposée au dossier médical et aux documents contenant des informations relatives au malade. Les informations qu'ils contiennent sont également secrètes et formalisées puis rassemblées au sein du dossier, de sorte que la valeur économique que l'auteur reconnaît aux informations contenues dans le dossier pénal peut également être reconnue au dossier médical. Toutefois, il nous semble que la valeur du dossier, pénal ou médical, peut plus simplement être déduite de la valeur du support. Dès lors qu'est admise l'existence de biens à valeur *négative*[333], rien ne permet de dénier, *a fortiori*, cette qualification à une chose en raison de la faiblesse de cette valeur. Plus simplement, le fait que l'information ne soit pas légalement déterminée comme un bien et le refus de certains auteurs de la qualifier comme telle[334] ne doit pas empêcher d'affirmer que le dossier médical est un bien. De plus, la valeur ne doit sans doute pas s'analyser uniquement sur le plan économique[335], mais comme le rapport entre la rareté et l'utilité[336]. En ce sens, le dossier médical est utile et rare : sa valeur découle de l'opération intellectuelle effectuée par les professionnels à partir des données, opération qui permet de formaliser le dossier médical. Le problème pourrait également être résolu plus simplement encore selon Madame Rassat, en considérant que la matérialité du dossier permet d'emblée de le qualifier de

---

[332] *Ibid*.

[333] « *Pendant longtemps, la question de la valeur ne se posait pas en matière de biens, où régnait une équivalence simple : un bien est nécessairement une chose de valeur, cela seul justifiant sa possible insertion dans les échanges ; en sens inverse, une chose dépourvue de valeur ne pouvait pas constituer un bien, car nul ne pouvait décemment désirer l'acquérir – à moins que ce ne soit pour des raisons affectives.* […] *Peu à peu, la dynamique des échanges montrait néanmoins que cette équivalence longtemps maintenue entre bien et valeur n'allait plus de soi, et que l'on pouvait insérer des choses à valeur négative dans le processus de circulation des biens* » (R. LIBCHABER, *Rép. civ, V°* « Biens », mai 2016, n° 16-17) ; *Adde* D. CHILSTEIN, « Les biens à valeur vénale négative », *RTD civ*. 2006, p. 663 ; M. RENOUF*, Contribution à l'analyse juridique de la notion de valeur : essai sur les biens à valeur négative*, th. dact., ss la dir. de M. AUDIT, 2012, Université de Caen Basse-Normandie.

[334] Par exemple : E. DREYER, *Droit pénal spécial*, *op. cit.*, n° 880 ; N. MALLET-POUJOL, « Appropriation de l'information : l'éternelle chimère », *D.* 1997, p. 330 ; A. LUCAS, *Droit de l'informatique et de l'Internet*, coll. Thémis, PUF, 2001, n° 470 et svt. ; J.-C. GALLOUX, « Ebauche d'une définition juridique de l'information », *D.* 1994, chron. p. 230, n° 10 ; E. DARAGON, « Etude sur le statut juridique de l'information », *D*. 1998, chron. p. 63, n° 3 ; J. PASSA « La propriété de l'information : un malentendu ? », *Dr et patr.*, mars 2001, p. 64 et svt.

[335] L'argument de la faiblesse de la valeur économique ne nous semble, en outre, pas pertinent car, même faible, cette valeur existe.

[336] R. SAVATIER, *Les métamorphoses économiques et sociales du droit privé d'aujourd'hui*, 3ème série, *Approfondissement d'un droit renouvelé*, 1959, Dalloz, n° 494 et svt. ; J.-M. MOUSSERON, « Valeurs, biens, droits », *in Mélanges en hommage à A. Breton et F. Derrida*, Dalloz, 1991, p. 277.

chose, ce qui suffirait à déterminer l'objet du vol[337]. La question de la propriété du dossier médical et plus généralement des documents médicaux contenant des informations secrètes doit toutefois être posée.

2 - L'appropriation du dossier médical

64. La propriété du dossier médical, plusieurs hypothèses. La difficulté de déterminer le propriétaire du dossier médical tient à la particularité de l'objet, les informations contenues dans le dossier sont relatives à la personne prise en charge, tandis que le dossier lui-même est formalisé, créé par les professionnels qui participent à cette prise en charge, le matériel utilisé pour sa création est celui de l'établissement ou du professionnel libéral selon le cas. Le malaise est perceptible tant l'information et son contenant sont confondus. Certains auteurs ont ainsi affirmé que le patient était « propriétaire » du dossier médical[338], ce que d'autres refusent en raison de la particularité de ces mêmes informations[339]. Toutefois, la plupart des auteurs ne justifient pas leur position sur ce point, tout au plus peut-on lire que « *le patient ne dispose d'aucun droit de propriété sur son dossier, droit qui pourrait en effet entraîner celui de le conserver personnellement à son domicile, voire de le détruire* »[340]. Les médecins ont, eux-mêmes, pu revendiquer un droit de propriété sur le dossier médical et sur les documents médicaux qu'ils conservent. Madame Thouvenin, analysant une jurisprudence aujourd'hui

---

[337] Madame Rassat remarque, sur ce point, que le propre de l'infraction de vol est de porter sur une chose et non sur un bien. L'auteur affirme ainsi que si le bien à une valeur mais « *peut avoir n'importe quel aspect, la chose doit, au contraire, être tangible mais n'a pas besoin d'avoir une valeur appréciable* » (M.-L. RASSAT, *Droit pénal spécial. Infractions du Code pénal*, 8ème éd., coll. Précis, Dalloz, 2018, n° 106).

[338] En ce sens, v. L. DUBOUIS, « Convention nationale. Dossier de suivi médical », *RDSS* 1994, p. 433 ; P. PEDROT, « Le dossier de suivi médical et le carnet médical », *RDSS* 1995, p. 610 ; M. PENNEAU, « Saisie du dossier médical », *D.* 1996, p. 296 ; C. DAVER, « La télémédecine entre progrès techniques et responsabilités », *D.* 2000, p. 527 ; J.-F. FORGERON et V. SEGUINOT, « Le dossier médical personnel : l'activité d'hébergeur de données de santé (2ème partie) », *Gaz. Pal.*, 26 janv. 2006, p. 10 ; C. CHABERT, M. DENANT-BOEMONT, « La généralisation du dossier médical personnel en question », *Gaz. Pal.,* 19 avr. 2007, p. 22. Une telle affirmation est d'ailleurs courante dans les conventions de formation des fédérations sportives (par exemple : Arrêté du 14 nov. 2002 approuvant la convention type de formation de la Fédération française de football (*JORF*, 23 nov. 2002) ; Arrêté du 20 mai 2007 approuvant la convention type de formation de la Fédération française de rugby à XV ; Arrêté du 20 octobre 2010 approuvant la convention type de formation de la Fédération française de rugby (*JORF*, 29 oct. 2010), et dans plusieurs textes de valeurs diverses, par exemple : Circulaire CNAMTS n° 13-96 du 29 octobre 1996 relative à la mise en œuvre du carnet de santé, institué par l'ordonnance n° 96-345 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins et par le décret n° 96-925 du 18 octobre 1996. Les textes affirmant la propriété de la personne sur le dossier médical sont toutefois peu nombreux.

[339] En ce qu'elles sont rattachées à la personne.

[340] M. DUPONT, Feuillets mobiles Litec, Droit médical et hospitalier, Fasc. 9-30 : *Dossier médical. – Dossier en établissement de santé. Dossier dématérialisé*, nov. 2016, n° 12. Sur la question de la maîtrise des données et de l'autodétermination informationnelle comme *troisième voie*, v. n° 341.

datée[341], a affirmé que le dossier patient et plus largement tous les documents produits[342] par plusieurs professionnels devaient s'analyser comme des « *œuvres collectives* »[343], tandis que les dossiers ou documents produits par un professionnel libéral, « *conséquence du travail de décodage d'un médecin* »[344], étaient la propriété du médecin[345]. Une circulaire ancienne affirmait en outre que le dossier médical était la propriété de l'établissement public[346]. Cette dernière hypothèse rejoint les développements de Monsieur Ribeyre relatifs au dossier pénal, à propos duquel il défend l'idée d'une propriété étatique relevant du domaine public en raison de son affectation à un service public[347]. Une telle hypothèse pourrait trouver à s'appliquer au dossier médical puisque le point de départ du raisonnement tient dans le fait que les informations du dossier pénal sont produites par les agents du service public[348], or c'est également le cas pour le dossier médical, du moins en milieu hospitalier et dans les établissements médico-sociaux. De plus, l'on pourrait considérer que, tout comme le dossier pénal, le dossier médical, et plus généralement les documents comportant des informations relatives à la santé, peuvent être des biens publics[349] appartenant au domaine public en raison

---

[341] Civ. 1re, 28 oct. 1970, cité et commenté par D. THOUVENIN, *Le secret médical et l'information du malade*, PUL, 1982, p. 174.

[342] L'auteur utilise le terme de fichiers ou de fiches soulignant que : « *Le terme de dossier vise un ensemble de pièces placées dans une chemise, celui de fichier désigne une collection de données quelle que soit son organisation, celui de document concerne tout écrit constituant un élément d'information. Pour des raisons de commodité de langage nous utiliserons le terme de fichier ; il a l'avantage d'être générique et ne prend pas en compte le support de l'information* » (D. THOUVENIN, *op. cit.*, p. 171). Nous ne partageons pas cette opinion. Le terme « fichier » renvoie à la loi informatique et libertés et constitue un traitement de données, cette qualification emporte des conséquences précises. Notre propos tenant plus simplement à affirmer la protection du secret des informations par la protection du support, les termes de « dossier » et de « document » sont appropriés.

[343] *Ibid.*, p. 174.

[344] *Ibid.*, p. 172.

[345] D. THOUVENIN, « Le secret médical : droit ou devoir du professionnel ? », *RDSS* 1982, p. 601.

[346] Circulaire n° 44-24 du 1er février 1944 prise en application du décret n° 43-891 du 17 avril 1943.

[347] C. RIBEYRE, *La communication du dossier pénal*, *op. cit.*, spéc. n° 556 et svt. L'affectation consiste à « *soumettre un bien à un usage déterminé* » (S. GUINCHARD, *L'affectation des biens en droit privé français*, préf. R. Nerson, coll. Bibliothèque de droit privé, t. CXLV, LGDJ, 1976, n° 15). Cet usage, s'agissant du domaine public, doit répondre à l'intérêt général. Tout comme pour le dossier pénal, la qualification de bien public appliquée au dossier médical découlerait par ailleurs de leur qualité d'archives publiques : « *c'est la nature même de papiers publics qui en fait une propriété publique* » (J. LAVEISSIERE, « Le statut des archives en France », *Rev. adm.* 1980, n° 195, p. 256).

[348] C. RIBEYRE, *La communication du dossier pénal*, *op. cit.*, n° 563.

[349] Sur la notion de bien public, v. F. ZENATI-CASTAING, T. REVET, *Les biens*, 3ème éd., coll. Droit fondamental, PUF, 2008, n° 40 et svt., spéc. n° 41 : « *Les biens dépendant du domaine public sont, par nature, rebelles au commerce ; alors que le commerce vise à faire circuler une utilité réservée, ils offrent, quant à eux, une utilité accessible à tous. Leur usage commun est, comme celui des copropriétés archaïques dont ils procèdent,*

de leur affectation à l'intérêt général[350]. Le régime juridique qui découle de cette qualification de « *bien public, indisponible car affecté à l'usage collectif* »[351], trouve d'ailleurs un écho particulier si l'on considère par exemple les délais de conservation avant destruction. Toutefois, les thèses attribuant la propriété des documents et dossiers médicaux aux établissements publics ou aux professionnels libéraux sont battues en brèche par les évolutions législatives intervenues dans le domaine de la santé depuis la loi du 4 mars 2002. Contrairement au dossier pénal, le malade a désormais un accès direct à son dossier médical partagé et à de nombreuses informations le concernant. Quant aux documents et dossiers sous format papier, les professionnels et les établissements de santé n'en ont que la garde. La loi informatique et libertés contribue notamment à affirmer la maîtrise des données personnelles, dont les données de santé sont une catégorie spécifique, mais cette maîtrise ne permet en rien d'affirmer la propriété des documents et du dossier médical, pas plus que la doctrine ne s'accorde d'ailleurs sur la propriété des données informatiques[352]. En somme, la question de la propriété des documents contenant des informations secrètes relatives au patient et, *a fortiori*, du dossier médical n'est pas tranchée. Il faut toutefois distinguer l'appropriation de la notion de propriété, cette distinction permettant de comprendre que les documents médicaux puissent être l'objet d'un vol alors même qu'ils ne font pas l'objet d'un droit de propriété.

65. L'appropriation, condition suffisante. Ni le malade, ni le professionnel, ni d'ailleurs l'établissement sanitaire ne semblent être titulaires d'un droit de propriété sur les documents comportant des informations relatives au malade, puisqu'ils ne sont titulaires d'aucune des

---

incompatible avec une appropriation privative par un particulier, et, par conséquent, avec toute aliénation ou constitution d'un droit réel. »

[350] L'affectation du dossier pénal au service public de la justice pénale est plus évidente à démontrer dans la mesure où « *Le dossier, ouvert par une enquête de police ou une véritable poursuite, appelle, dès sa création, une protection particulière parce qu'il va permettre au service public de la justice de découvrir la vérité matérielle. Il est affecté exclusivement à une finalité pénale, relevant du monopole de l'Etat* » (C. RIBEYRE, *La communication du dossier pénal*, *op. cit.*, n° 569). Le même auteur considère que le dossier médical est constitué dans le seul intérêt du patient (*Ibid.,* n° 564), il nous semble toutefois que cette assertion ne s'applique pas à tous les documents médicaux, dès lors qu'ils contribuent à favoriser la coordination des soins, la qualité et la continuité des soins (au même titre d'ailleurs que le dossier pharmaceutique : C. LE GAL, « *Le dossier pharmaceutique : un outil technique de santé publique* », *RDSS* 2009, p. 301). En outre, certains documents contenant des informations à caractère secret contribuent à la maîtrise des dépenses de santé, l'établissement public participe de cette maîtrise en ce qu'il permet d'éviter les actes de soins redondants. Bien qu'ils contiennent – comme le dossier pénal d'ailleurs – des informations relatives au patient, le fait qu'ils soient utiles à ce dernier ne suffit pas à exclure une possible affectation à l'intérêt général.

[351] C. RIBEYRE, *La communication du dossier pénal, op. cit.,* n° 582, reprenant le raisonnement de G. LOISEAU, « Typologie des choses hors commerce », *RTD civ.* 2000, p. 47.

[352] V. *infra,* n° 379.

prérogatives classiquement reconnues au propriétaire, à savoir l'*usus*, le *fructus* et l'*abusus*[353]. Le vol, tel que prévu à l'article 311-1 du Code pénal, sanctionne « *la soustraction frauduleuse de la chose d'autrui* », ce qui n'impose ni l'existence d'un droit de propriété sur cette chose, ni que l'identification du propriétaire[354]. Sanctionnant « *l'atteinte au fait d'être propre, devenu droit* »[355], le vol permet ainsi de « *préserver certains biens placés en dehors du commerce juridique, dont l'unique particularité réside alors dans leur attachement à une personne* »[356]. Il suffit donc que la chose soit appropriée et le juge pénal, pour entrer en voie de condamnation, se contente d'établir que celui qui a soustrait la chose n'en est pas le propriétaire[357]. En sanctionnant le vol de documents comportant des informations secrètes, comme un dossier médical, le juge pénal sanctionne parfois, de manière incidente, l'atteinte au secret des informations – *secret-état*.

66. Analyse de la jurisprudence. La faiblesse des poursuites pour vol de dossier médical ou de documents comportant des informations à caractère secret ne permet pas de systématiser notre raisonnement. Seules trois décisions, d'ailleurs contradictoires, concernent des vols de dossiers médicaux ou de documents. Dans deux de ces décisions, l'atteinte au secret des informations n'était pas en cause mais renvoyait aux hésitations relatives à la propriété du dossier médical. Il a par exemple été jugé que le médecin prévenu du chef de vol, en ce qu'il avait soustrait frauduleusement une feuille d'observation des urgences – pièce figurant au dossier médical – pour la remplacer par une autre, ne commettait pas le délit prévu à l'article 311-1 du Code pénal car « *le praticien hospitalier en charge du dossier, en est le seul légitime détenteur* »[358]. La Cour d'appel de Nîmes avait jugé que les faits commis par le praticien relevaient de la compétence de l'Ordre des médecins en ce qu'ils constituaient une faute déontologique. En déduisant que le médecin ne commet pas l'élément matériel de l'infraction, l'appropriation frauduleuse, puisqu'il est le détenteur – et non le propriétaire – de la chose, le

---

[353] O. DUPUY, *Le dossier médical*, 2ème éd., coll. Essentiel, LEH, 2005, pp. 12-13.
[354] Crim., 11 mars 1942, *Bull. crim.*, n° 23.
[355] G. BEAUSSONIE, *La prise en compte de la dématérialisation des biens par le droit pénal. Contribution à l'étude de la protection pénale de la propriété*, préf. B. DE LAMY, coll. Bibliothèque de droit privé, t. 532, LGDJ, 2012, n° 159.
[356] *Ibid.*
[357] Sur ce point v. par exemple : M. VERON, *Droit pénal spécial*, 17ème éd., coll. Université, Sirey, 2019, n° 480.
[358] Nîmes, ch. corr., 28 mai 2002, n° 612/02, JurisData n° 2002-197846.

juge pénal fait une application stricte du texte de l'article 311-1 du Code pénal. La détention matérielle de la chose exclut la soustraction frauduleuse constitutive du vol, puisqu'il s'agit d'une infraction de commission[359]. Un autre arrêt, plus ancien, concerne le vol du dossier médical d'un enfant décédé. A l'occasion de l'instance pénale, les parents de l'enfant ainsi que la clinique s'étaient portés partie civile[360]. La Cour de cassation a validé la décision de la Cour d'appel de Lyon d'avoir « *justifié l'indemnisation des parties civiles alléguant le préjudice directement subi par elle du fait de la soustraction au détriment de la clinique où il avait été établi, du dossier médical concernant le décès de leur enfant* ». La reconnaissance du préjudice des parents n'appelle pas de commentaire particulier, mais l'affirmation selon laquelle la clinique est le propriétaire du dossier médical est plus surprenante. Outre ces deux espèces, il en est une autre qui attire particulièrement l'attention : un médecin, praticien hospitalier, avait révélé, par lettre au Procureur de la République, des faits infractionnels commis par d'autres praticiens exerçant dans le même établissement et dont il avait eu connaissance. La violation du secret professionnel était justifiée par les dispositions de l'article 40 du Code de procédure pénale[361]. Pour attester ses allégations, le praticien avait remis des dossiers médicaux au capitaine de gendarmerie en charge de la procédure. Le praticien avait été poursuivi et condamné pour vol. La Cour de cassation a finalement rejeté le pourvoi formé contre l'arrêt d'appel : « *les documents qu'il a communiqués à l'officier de police judiciaire ont été prélevés par lui dans des dossiers concernant des patientes du Centre hospitalier d'Auxerre suivies par*

---

[359] La qualification d'abus de confiance (art. 314-1 du Code pénal) aurait, peut-être, été ici préférable. Le rapport de confiance entre le médecin et le patient est évident. Par ailleurs, le dossier médical (et l'information couverte par le secret elle-même, puisque l'infraction a pour objet un « *bien quelconque* » qui peut donc être incorporel contrairement à la chose v. G. BEAUSSONIE, « La dématérialisation de l'abus de confiance », *AJ pénal* 2017, p. 215 ; Concernant des données : Crim. 22 oct. 2014, n° 13-82630, *D.* 2015, p. 415, note A. MENDOZA-CAMINADE ; de clientèle : Crim., 22 mars 2017, n° 15-85929, publié au Bulletin ; *Rev. sociétés* 2018, p. 56, note H. MATSOPOULOU ; *D.* 2017, p. 1877, obs. C. MASCALA ; *AJ pénal* 2017, p. 232, obs. G. BEAUSSONIE ; *RTD com.* 2017, p. 447, obs. L. SAENKO) est remis (la question se pose du moins) en vue d'en faire un usage déterminé (la prise en charge du malade). Enfin, en substituant et en détruisant le document, le médecin se comporte comme s'il était le maître de la chose, et ce au préjudice du patient qui ne pourra plus en faire usage, comme moyen de preuve, devant les juridictions (la dissipation du bien pouvant en effet consister en une destruction : E. DREYER, *Droit pénal spécial*, 3ème éd., coll. Cours magistral, Ellipses, 2016, n° 1212).

[360] Crim., 12 janv. 1994, n° 93-81065, *Bull. crim.,* n° 176 ; *JCP G* 1994, 925 ; *D.* 1994, *IR* p. 106.

[361] CPP, art. 40 : « *Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs* » (V. Sur les faits justificatifs de violation du secret professionnel v. B. PY, *Rép. pén.*, *V°* « Secret professionnel », 2003 (mise à jour févr. 2017), n° 143 ; spéc. à propos du fait justificatif prévu à l'article 40 CPP : C. WILSON, *Enc. des collec. loc.*, Dalloz, août 2015, Chap. 4 (Folio n° 10340), « Personnel des collectivités territoriales : obligations relatives aux informations détenues par les agents », n° 110-126.

d'autres patriciens hospitaliers et même, pour deux d'entre elles, par d'autres hôpitaux, ; que, si le contrat de travail […] *stipulait que les dossiers et documents médicaux étaient conservés sous sa responsabilité, à* ***l'abri des indiscrétions****, cela ne l'autorisait pas à les* ***produire*** *en copie ou en original en dehors de l'exercice de ses fonctions* »[362]. Si la première branche du moyen confirme l'appropriation frauduleuse des documents dont le praticien n'est pas le détenteur, la seconde branche est plus surprenante. La Cour considère en effet que, s'agissant des documents placés sous la garde du médecin, le vol se déduit du fait qu'ils ne doivent pas être produits en dehors du cadre médical en raison de leur caractère secret. Au regard du principe de légalité criminelle, une telle interprétation est critiquable. Le vol ne sanctionne pas le fait de produire, c'est-à-dire de faire connaître ou d'utiliser à l'appui d'une cause, des documents confidentiels. La qualification paraît alors de pure opportunité, destinée à pallier l'impossibilité d'une poursuite pour violation du secret professionnel. Toutefois, dès lors que le vol sanctionne « *la mise en circulation involontaire du bien* »[363], l'infraction permet, en sanctionnant l'appropriation frauduleuse du support, de sanctionner l'atteinte au *secret-état*. Si les exemples qu'offre la jurisprudence ne concernent que des médecins, soumis au secret professionnel, le vol protège avant tout les documents de toute appropriation par un tiers, lequel pourrait alors prendre connaissance de l'information secrète par l'intermédiaire du support. Ainsi, l'infraction de vol participe également de la protection du secret des correspondances en sanctionnant la soustraction frauduleuse de la lettre de missive[364]. La répression du vol du support de l'information permet d'en protéger le secret. Le secret des informations relatives au malade est également protégé de la curiosité lorsque cette information est communiquée. L'infraction sanctionnant l'atteinte au secret des correspondances contribue à la protection du secret des informations issues de la prise en charge des personnes dans le système de santé – *état*.

---

[362] Crim., 3 mai 2001, n° 00-84301. Nous soulignons.
[363] G. BEAUSSONIE, *La prise en compte de la dématérialisation des biens par le droit pénal, contribution à l'étude de la protection pénale de propriété*, *op. cit*, n° 159.
[364] Sur ce point v. par exemple : V. PELTIER, *Le secret des correspondances*, préf. P. CONTE, PUAM, 1999, n° 472 à 479.

B - L'atteinte au support-véhicule de l'information

67. Le support de l'information secrète n'a pas pour seule fonction sa représentation, il peut également en être le véhicule **(1)**. L'atteinte au support-véhicule de l'information secrète peut alors être sanctionnée **(2)**.

1 - Contexte et définitions

68. Domaine de la communication. Le support de l'information n'a pas pour seule fonction de garder en mémoire l'information, il a aussi une fonction de communication[365]. Le domaine de la communication saisi par le droit couvre un champ très large. Le *droit de la communication*[366] a pour source une liberté fondamentale et un droit fondamental[367] et encadre l'information et la communication dites publiques[368], ce que la sociologie nomme *communication de masse*[369]. Le droit de la communication recouvre donc un champ large dans lequel la spécialisation est reine : le droit de la presse et des médias[370] définit la liberté de la presse et ses limites mais concerne également la communication au public par voie électronique, laquelle se subdivise en deux catégories que sont « *la communication audiovisuelle* »[371] et « *la communication au public en ligne* »[372]. Le premier concerne

---

[365] A. TRICOT, G. SAHUT et J. LEMARIE, *Le document : communication et mémoire*, De Boeck, 2016.
[366] E. DERIEUX, *Droit de la communication. Droit européen et international*, 3ème éd., coll. Legipresse, Victoires, 2011.
[367] La liberté de communication, issue de la Déclaration des droits de l'homme et du citoyen, art. 11 (« *Libre communication des pensées et des opinions* »). Il s'agit de la liberté « *pour chacun, d'utiliser librement le média de son choix pour exprimer sa pensée en la communiquant à autrui, ou pour accéder à l'expression de la pensée d'autrui quelle que soit, dans les deux cas, la forme ou la finalité de cette expression* » (F. BALLE (ss. la dir.), *Lexique d'information communication*, Dalloz, 2006) et le droit à l'information (DDHC, art. 10 et 11, CESDH, art. 10).
[368] « *Au-delà des principes généraux gouvernant l'expression des opinions, certains secteurs de la communication font l'objet de cadres réglementaires spécifiques : il en est ainsi de l'affichage, de la presse écrite, de la communication audiovisuelle ou du secteur cinématographique* » (P. KAMINA, *Jcl. com.*, Synth. 30 : « Régulation de la communication », mai 2018, spéc. introduction).
[369] Sur les enjeux sociologiques de la communication et l'évolution de l'information et de la communication publique : P. BRETON et S. PROULX, *L'explosion de la communication*, coll. Sciences humaines et sociales, La découverte, 1996.
[370] Pour un ouvrage complet : B. BEIGNIER, B. DE LAMY et E. DREYER (ss. la dir.), *Traité de droit de la presse et des médias*, coll. Traités, LexisNexis, 2009.
[371] Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (*JORF*, 1er oct. 1986, p. 11749).
[372] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (*JORF* n° 0143, 22 juin 2004, p. 11168). La communication en ligne entretient de nombreux liens avec le droit de l'internet dès lors que « *l'apparition de nouvelles activités économiques se traduit par une grande diversification des modes de communication sur l'internet : blogs, forums, de discussion, sites collaboratifs… De telle activités provoquent l'émergence de toutes sortes d'intermédiaires, techniques ou non, qui viennent s'immiscer dans la relation entre fournisseur et consommateur de contenus en ligne. Le régime de responsabilité est à définir : sont-ils de simples*

spécifiquement la télévision, la radio et les services qui ne relèvent pas de la communication publique en ligne. La seconde sous-branche concerne la communication assurée par « *le biais d'un réseau accessible à tous, qui relie entre eux les ordinateurs permettant les échanges de données et de messages. Dès lors que la communication a un caractère public, le droit de la communication à vocation à s'appliquer* »[373]. Ainsi, le droit de la presse et des médias et plus particulièrement – s'agissant des dispositifs modernes de communication que sont les réseaux informatiques et l'internet – le droit de la communication au public en ligne ne sont pas indifférents à la question du secret professionnel, ce dernier constituant une limite à la liberté d'information[374]. Le présent développement porte uniquement sur l'atteinte au *secret-état* par le biais du support qui véhicule les informations secrètes – *secret-fait* – dans le cadre de communications privées.

69. Correspondances, secret professionnel et atteinte au secret des informations relatives au malade par le secret des correspondances. La violation du secret des correspondances est sanctionnée par une incrimination spécifique, bien que la notion de secret des correspondances, comme celle de « secret médical », soit plus large[375]. La correspondance est parfois présentée comme le « *siège du secret professionnel* »[376] ou comme « *une*

---

intermédiaires techniques ou des éditeurs de contenus au sens du droit de la presse ? » (C. CASTETS-RENARD, *Le droit de l'internet*, coll. Cours, Montchrestien, 2010, n° 13).

[373] C. CASTETS-RENARD, « La spécificité des communications en ligne », *in* B. BEIGNIER, B. DE LAMY et E. DREYER (ss. la dir.), *Traité de droit de la presse et des médias*, coll. Traités, LexisNexis, 2009, n° 1898.

[374] Par exemple concernant consacrant un développemnt au *secret médical* : A. GUEDJ, « Liberté et responsabilité en droit européen et international », *in* B. BEIGNIER, B. DE LAMY et E. DREYER (ss. la dir.), *Traité de droit de la presse et des médias*, *op. cit.*, n° 218 et svt.

[375] Le secret des correspondances ne se résume pas à l'infraction de violation du secret des correspondances. Bien que l'on pense en premier lieu, lorsque l'on évoque la notion, au texte d'incrimination prévu à l'article 226-15 du Code pénal. Madame Peltier explique que « *le secret des correspondances se présente* […] *comme une notion juridique autonome qui tend à l'effectivité par la répression pénale de toutes formes d'atteintes imaginables, de quelques origines qu'elles proviennent.* […] *Le droit au secret des correspondances apparaît donc élevé au rang de droit digne d'une protection spéciale, notamment en France, grâce au jeu d'incriminations pénales autonomes* » (V. PELTIER, *Le secret des correspondances*, *op. cit.*, n° 19).

[376] L'assertion concerne principalement le secret professionnel des avocats, mais peut aussi s'appliquer au secret professionnel dans le domaine de la santé : « *Les correspondances entrent dans le champ du secret professionnel dès lors qu'elles renferment des informations remises à titre confidentiel par celui qui se confie. Mais l'évolution qu'a connue l'incrimination de l'article 226-13, marquant le passage entre le professionnel dépositaire à titre exprès d'un secret et le professionnel « confident nécessaire », prenant connaissance indirectement d'une information à caractère confidentiel, doit également être appliquée au secret des correspondances. Il en résulte que des correspondances sont couvertes par le secret professionnel quand bien même le maître du secret ne l'aurait pas confié expressément au professionnel. Il ne s'agit pas d'une information quelconque, mais d'une*

expression »[377] de celui-ci. En effet, les correspondances entre un professionnel soumis au secret et un usager, un client ou un patient ainsi que celles échangées entre deux professionnels dans le cadre du secret partagé[378] peuvent contenir des informations couvertes par le secret professionnel[379] – *secret-fait*. Ainsi, la révélation des informations contenues dans une correspondance peut constituer l'infraction de violation du secret professionnel. Or, si les correspondances peuvent contenir des informations que le professionnel ne peut révéler sous peine d'une sanction pénale, le secret des informations – *secret-état* – est également assuré à l'égard des tiers. Dès lors que l'information couverte par le secret – *secret-fait* – est l'objet d'une communication, les infractions sanctionnant l'atteinte au secret des correspondances contribuent à la protection du secret des informations relatives au malade – *secret-état*. En protégeant le support de la communication, l'infraction prévue à l'article 226-15 du Code pénal sanctionne l'atteinte au contenu des correspondances et donc l'atteinte au secret des informations issues de la prise en charge des personnes dans le domaine de la santé. De plus, l'infraction prévue à l'article 432-9 du Code pénal punit spécifiquement cette atteinte lorsqu'elle est le fait d'une personne dépositaire de l'autorité publique ou chargée d'une mission

---

information recueillie par l'état, la profession, la mission ou la fonction temporaire » (P. BONFILS et E. GALLARDO, *Rep. pén.*, *V°* « Secret des correspondances », (mise à jour juin 2018), n° 102).

[377] *Ibid.,* n° 150.

[378] A propos de l'échange et du partage d'information entre professionnels soumis au secret dans le domaine de la santé v. *infra* n° 236. Le secret partagé ne serait pas un fait justificatif propre au domaine de la santé. Bien qu'aucun texte ne fonde une telle exception dans d'autres domaines, la pratique est courante et admise : « *L'existence de secrets partagés ne se rencontre pas qu'en matière médicale. De nombreux professionnels font aujourd'hui une utilisation largement partagée de leur secret, comme lors de la défense d'un particulier par une équipe d'avocats comme cela arrive fréquemment en cour d'assises. C'est également le cas des fonctionnaires d'un même service, qui peuvent évidemment se communiquer des éléments relatifs aux dossiers qu'ils ont à traiter ensemble* » (M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, th. dact., ss la dir. d'A. PROTHAIS, Université de Lille II, soutenue en 2004, n° 174) *; Adde* B. PY, *Rép. pén.*, *V°* « Secret professionnel », févr. 2003 (mise à jour févr. 2017), n° 163 : « *Certaines décisions, certes isolées, laissent à penser qu'il pourrait exister d'autres hypothèses de secrets partagés. Il a été jugé que le délit n'est pas constitué par la circulation au sein d'un établissement bancaire de la photocopie d'un chèque qui n'avait pas pour conséquence directe ou indirecte de faire connaître à un tiers un fait confidentiel en dehors de la « sphère bancaire » (Cass. crim. 18 oct. 2000, n° 99-85.563, Legifrance) ou encore que la communication, entre agents d'un même cabinet ministériel, d'un secret acquis dans l'exercice des fonctions, pour les besoins du service, ne constitue pas une révélation susceptible de tomber sous le coup de la loi pénale (CA Paris, 8 févr. 2001, Bull. inf. C. cass., n°538, 2001, n°727). Inversement, a été refusée pour non-préservation du secret professionnel entre associés la demande d'ouverture d'un cabinet secondaire d'avocats (CA Basse-Terre, 19 janv. 2000, Bull. info. C. cass., no 519, 2000, n°994). La casuistique n'épargne donc pas la question du secret partagé* ».

[379] Par exemple : Crim., 27 juin 1967, *Bull. crim.* n° 194. Rappellons toutefois qu'il existe une différence importante entre les professions soumises au secret. Le secret des correspondances des avocats a fait l'objet de longues discussions doctrinales et d'une évolution législative importante.

de service public dans le cadre de l'exercice de ses fonctions ou missions, cette atteinte au secret des correspondances est incriminée comme un abus d'autorité[380].

70. Définition des correspondances. Toute communication n'est pas une correspondance au sens du droit positif[381], la correspondance suppose une relation entre deux ou plusieurs personnes[382], et, par ailleurs, un support. Ainsi, « *l'objet de la correspondance prend la forme d'une information véhiculée par un support. Le support intervient à raison de l'impossibilité de communiquer une information directement – souvent à raison de l'éloignement de son correspondant – ou de la volonté de la communiquer indirectement – préférer les petits mots aux grandes paroles. On peut alors entretenir une conception plus ou moins stricte de l'objet-correspondance : soit n'appréhender comme telle que les informations personnelles et certains supports ; soit faire accéder à cette qualification toute information, quelle qu'elle soit, et n'importe quel support* »[383]. Selon la seconde hypothèse évoquée par cet auteur, toute information, peu importe la nature de son support, peut consister en une correspondance. Dès lors, une information couverte par le secret professionnel, représentée et communiquée à des personnes déterminées peut être qualifiée de correspondance. Le support n'est pas uniquement ce qui permet de fixer l'information mais aussi le *véhicule* de l'information, c'est-à-dire le support de la communication[384]. Il faut, par ailleurs, noter que si le contenu de la correspondance fonde la protection de la correspondance, la répression de la violation du secret des correspondances est indépendante du contenu de celle-ci[385]. Le support de la

---

[380] L'infraction figure dans une section portant sur les abus d'autorité commis contre les particuliers au sein d'un chapitre relatif aux atteintes à l'administration publique commises par des personnes exerçant une fonction publique. L'ensemble des infractions relevant du livre IV du Code pénal relatif aux crimes et délits contre la Nation, l'Etat et la paix publique.

[381] N'est pas considéré comme une correspondance un simple message publicitaire ou un tract dès lors que ceux-ci sont envoyés à des personnes non identifiées. N'est pas non plus une correspondance un *spam* ou un message adressé à une liste de diffusion (en ce sens, v. V. PELTIER, *Jcl. Pénal Code*, art. 432-9, Fasc. 20 : « Atteinte au secret des correspondances commises par des personnes dépositaires de l'autorité publique », mars 2008 (mise à jour mars 2018), n° 9).

[382] La correspondance se définit au regard de son caractère *intuitu personae* : « *On retrouve l'idée d'une communication entre, au moins, deux personnes qui se répondent, de sorte que la correspondance englobe à la fois la relation entre les personnes qui ont choisi de communiquer et l'objet de cette communication* » (V. PELTIER, « Atteinte au secret des correspondances commises par des personnes dépositaires de l'autorité publique », *op. cit.,* n° 4).

[383] G. BEAUSSONIE, *Jcl. comm.*, Fasc. 3403 : « Secret des correspondances », mars 2014 (mise à jour août 2017), n° 7.

[384] La correspondance étant alors à la fois représentation (support) et instrument (véhicule) : *Ibid.*, n° 411.

[385] *Ibid.*, n° 20 et 21.

communication est alors l'élément essentiel de cette protection. Enfin pour qu'il y ait correspondance, il faut que le document soit « *entré dans un processus d'envoi* »[386] et qu'il n'ait pas encore été ouvert par son destinataire. La protection est donc temporaire ou, selon la formule de Monsieur Beaussonie, « *ontologiquement provisoire* »[387] en ce que ce le champ d'application *rationae temporis* s'apprécie au regard de son essence. Elle n'est plus protégée dès lors que le destinataire en a pris connaissance. D'autres infractions pénales pourront alors prendre le relais[388].

2 - L'atteinte au secret des correspondances

71. Eléments de l'atteinte au secret des correspondances. La particularité des délits sanctionnant l'atteinte au secret des correspondances tient au fait que les infractions prévues aux article 226-15 et 432-9 du Code pénal ont une double finalité. Elles sanctionnent la prise de connaissance du contenu de la correspondance puisqu'est sanctionnée aussi bien le fait, pour un tiers à la correspondance, d'en prendre connaissance que d'ouvrir celle-ci[389] ; elles permettent également de sanctionner le fait d'entraver son acheminement dès lors que son retard, sa destruction et son détournement sont sanctionnés par les textes d'incrimination[390]. C'est la première hypothèse qui intéresse notre étude, la seconde visant spécifiquement à assurer la liberté de communication, et de manière plus évidente, peut-être, le droit de propriété[391]. Pourtant, même s'agissant de la sanction de l'atteinte au secret des correspondances due à la prise de connaissance illicite de l'information, le support comme élément intrinsèque de la communication, en ce qu'il véhicule celle-ci, demeure la condition essentielle de cette prise de connaissance. En effet, le fait, pour un tiers, de prendre

[386] *Ibid*., n° 16. Le document qui ne serait pas expédié vers son destinataire peut toutefois être l'objet d'un vol. Ainsi peut-il en être des résultats d'un examen médical qui constitueraient à la fois une pièce du dossier médical et seraient destinés à être envoyés par le médecin à l'origine de l'examen vers un autre dans le cas d'une prise en charge commune.
[387] G. BEAUSSONIE, « Secret des correspondances », *op. cit.*, n° 15.
[388] La soustraction d'une lettre, en possession du destinataire qui l'aurait déjà ouverte, afin de prendre connaissance de son contenu pourra être sanctionnée sur le fondement de l'article 311-1 du Code pénal.
[389] CP, art. 226-15, al. 1 et art. 432-9 al. 1.
[390] *Ibid*.
[391] Plus évidente, s'agissant des correspondances véhiculées par un support matériel, bien qu'il soit possible d'affirmer que la propriété s'étend à l'information elle-même : En ce sens v. V. PELTIER, *Le secret des correspondances*, *op. cit.*

connaissance de la correspondance « *fait suite à une ouverture et entérine un retard ou un détournement* »[392].

72. Le secret des correspondances entre professionnels de santé, particularité. Comme toute autre correspondance, celles échangées entre professionnels soumis au secret peuvent être l'objet de l'infraction de violation du secret des correspondances, peu importe leur contenu. Le secret des informations relatives au malade – *secret-état* – est donc incidemment protégé par l'infraction. Si la sanction de l'infraction de violation du secret des correspondances n'est pas aggravée en raison de la soumission au secret de l'émetteur et du destinataire[393], une particularité propre au domaine de la santé existe à propos des lettres d'introduction : lorsqu'un médecin conseille à un malade de consulter un confrère en particulier, il peut lui remettre une lettre, le pli étant alors destiné au confrère en question. Or, la Cour de cassation a jugé que la prise de connaissance d'une telle lettre, par le patient lui-même, ne peut être qualifiée de violation du secret des correspondances en raison du principe d'ordre public du libre choix du médecin par le malade, la remise de la lettre étant alors optionnelle[394]. Le secret des informations – *secret-état* – n'est pas opposable au patient lui-même, ce qui se justifie aujourd'hui par le droit d'accès qui lui est reconnu. La prérogative attachée à ce droit, qui consiste en la possibilité pour le malade d'exiger la communication des informations qui le concernent, marque la filiation entre secret des correspondances et secret des informations relatives à la santé. Le premier ne s'applique pas plus au patient concerné par la correspondance que le second. Aussi, les correspondances échangées entre professionnels intervenant dans le

---

[392] V. PELTIER, « Atteinte au secret des correspondances commises par des personnes dépositaires de l'autorité publique », *op. cit.,* n° 34.

[393] Il n'est par ailleurs pas nécessaire d'y apposer une mention du type « *secret médical* » comme a pu le préconiser le Conseil de l'Ordre des médecins (CNOM, « Les courriers entre médecins », Rapport du 30 janv. 1998, disponible en ligne sur <https://www.conseil-national.medecin.fr/sites/default/files/courriers.pdf.> (dernière consultation le 15 juillet 2018). La caractérisation de l'infraction de violation du secret des correspondances dépend, non pas d'une quelconque mention, mais de la qualification de correspondance, laquelle suppose simplement qu'elle soit adressée à personne déterminée.

[394] Ch. réun., 16 mai 1967 ; *JCP* 1968, II, 15374, note A. CHAVANNE ; *D.* 1963, p. 437, note J. LARGUIER ; *Gaz. Pal.* 1963, p. 462 ; et sur la totalité de l'affaire : T. civ. Versailles, 10 juill. 1957, *D.* 1958, somm. 48 ; *JCP* 1958, II, 10436, note R. SAVATIER ; *Gaz. Pal.* 1958, p. 77 ; *RSC* 1958, p. 399, obs. L. HUGUENEY et p. 407, obs. P. BOUZAT ; Paris, 6 mai 1958, *JCP* 1958, II, 10833, concl. LECOURTIER ; *RSC* 1959, p. 122, obs. L. HUGUENEY; Crim., 24 mai 1960, *Bull. crim.*, n° 284 ; *D.* 1960, somm., p. 114 ; *JCP* 1960, II, 11858, note R. SAVATIER ; *RSC* 1960, p. 650, obs. L. HUGUENEY et 1961, p. 356, obs. P. BOUZAT ; Orléans, 20 janv. 1961 ; *D.* 1961, p. 485 ; *S.* 1961, p. 284 ; *JCP* 1961, II, 12132 ; *Gaz. Pal.* 1961, p. 419 ; *RSC* 1961, p. 590, obs. L. HUGUENEY.

système de santé sont des éléments contenus dans le dossier médical du patient[395]. Le secret des correspondances contribue à la protection du secret des informations relatives au patient tout en intégrant une donnée essentielle : le patient ne peut être regardé comme un tiers à la correspondance échangée à son sujet.

§ 2 - La désolidarisation du support et de l'information

73. Le phénomène désigné par le terme « dématérialisation » est caractéristique de l'utilisation des technologies de l'information et de la communication. Il est bien souvent présenté comme un processus impliquant la disparition des supports matériels. Il s'agit d'une représentation, qui participe des imaginaires développés à propos des dispositifs techniques de l'information et de la communication dont il faut se départir **(A)**. Plusieurs infractions sont susceptibles de sanctionner l'appropriation de l'information secrète, par un tiers, indépendamment de son support **(B)** ainsi que la maîtrise illicite de l'information ainsi obtenue **(C)**.

A - Prolégomènes sur les phénomènes de dématérialisation

74. La reception de l'immatériel par le droit pénal des biens. Alors que *l'immatériel* désigne la chose où l'être qui est objet de la pensée, la dématérialisation désigne un phénomène, elle est donc le résultat d'un processus, une « *Action ou fait de rendre immatériel, d'ôter la matière concrète, les éléments matériels de…* »[396]. La dématérialisation qui intéresse notre étude n'est pas tant celle du droit[397] que celle des biens en droit pénal. Nous avons expliqué que l'infraction sanctionnant le vol et la violation du secret des correspondances permettaient une protection incidente du secret des informations relatives aux personnes prises en charge par un professionnel intervenant dans le système de santé – *secret-état* –, par l'intermédiaire du support de l'information, identifié au *secret-fait* par le jeu de la représentation. Il nous importe désormais de constater que le secret des informations –

---

[395] CSP, art. R. 1112-2, issu du Décret n° 2002-637 du 29 avril 2002. Certaines jurisprudences n'ont donc plus lieu de s'appliquer (telle la solution de l'arrêt du 16 mai 1967 précité).
[396] TLFi, *V°* « Dématérialisation ».
[397] Comme le constate Monsieur Amselek, traitant de l'ontologie du droit, « *en tant qu'objets ou outils mentaux, les règles juridiques appartiennent à notre intérieur, à l'univers de notre pensées* » (P. AMSELEK, *Cheminements philosophiques dans le monde du droit et des règles en général*, coll. Le temps des idées, Armand Colin, 2012, p. 64).

secret-état – fait également l'objet d'une telle protection mais, cette fois, indépendamment de l'usurpation de son support.

Ce qui est immatériel est ce qui « *n'a pas de consistance matérielle, qui n'est pas formé de matière* »[398] ou, selon la définition philosophique, « *Qui est opposé à la matière et n'a de rapport ni avec les sens ni avec la chair* »[399]. Les informations sont immatérielles par nature et leur représentation sur un support physique leur offre une corporéité, si bien que l'information est alors identifiée à son support[400]. L'immatériel ou incorporel – que nous considérons comme synonymes[401] – est évidemment saisi par le droit. En droit des biens, la dichotomie héritée des Romains distinguait les biens concrets et les biens incorporels, ces derniers – *jura* – n'étant pas des choses mais des droits[402]. Aussi ne faut-il pas confondre choses incorporelles et biens incorporels[403], deux « *assimilations fallacieuses* »[404] en découlent : « *l'immatériel ne résiderait que dans les droits ; la propriété serait exclusivement corporelle* »[405]. L'immatériel peut également être confondu avec la *virtualité*[406], désignant alors l'anticipation par le droit du devenir d'une situation présente. Des questions que l'immatériel pose au droit, celle de la prise en compte des biens incorporels par le droit pénal des biens intéresse particulièrement notre étude. La doctrine se montre réticente à admettre l'existence d'un droit de propriété sur les informations personnelles[407] et refuserait donc celle d'un secret des informations fondé sur la propriété. Force est, toutefois, de constater qu'au sein du titre consacré aux appropriations frauduleuses dans le livre du Code pénal portant sur les crimes et délits contre les biens, *le*

---

[398] TLFi, *V°* « Immatériel ».
[399] *Ibid.*
[400] C'est l'objet de nos développements précédents.
[401] « *Qui n'a pas de corps, qui n'est pas constitué de matière. Synon. Immatériel* » (TLFi, *V°* « Incorporel »).
[402] Pour une restitution complète de la pensée romaine sur ce point v. F. ZENATI-CASTAING, T. REVET, *Les biens*, 3ème éd., coll. Droit fondamental, PUF, 2008, n° 83 et n° 166.
[403] « *La différence est claire : les choses incorporelles sont des choses certes artificielles, mais dont l'existence relève des relations économiques et non d'un quelconque système juridique préétabli ; en revanche, les droits sont des objets créés à l'intérieur même des relations juridiques, par des techniques adéquates*. » (R. LIBCHABER, *Rép. civ.*, *V°* « Biens », mai 2016 (mise à jour avr. 2018), n° 67).
[404] G. BEAUSSONIE, *La prise en compte de la dématérialisation des biens par le droit pénal. Contribution à l'étude de la protection pénale de la propriété*, *op. cit.*, n° 6.
[405] *Ibid.*
[406] M.-A. FRISON-ROCHE, « L'immatériel à travers la virtualité », *in Le droit et l'immatériel*, *Arch. phil. dr.*, t. 43, 1999, pp. 139-148.
[407] Pour un état des questions v. J. ROCHFELD, *Les grandes notions du droit privé*, 2ème éd., PUF, 2013, n° 4.35 d).

secret peut être l'objet de plusieurs délits, dont l'extorsion et le chantage. Le juge pénal semble, en outre, avoir admis que le vol puisse porter sur des informations. Cette prise en compte de l'information en tant que bien illustre le phénomène plus général de la prise en compte par le droit pénal de la dématérialisation des biens, brillamment approfondi par Monsieur Beaussonie[408]. L'auteur démontre la particularité de la notion de bien en droit pénal et sa place au sein des incriminations[409] au travers du phénomène de dématérialisation des biens. Partant, il explique que si l'information est protégée par l'intermédiaire de son support, les deux entretenant un lien de représentation[410], c'est toujours l'information qui est protégée à travers le bien corporel[411]. Il défend ainsi la thèse d'une protection pénale du bien informationnel, affirmant la prise en compte par le droit pénal de la valeur *per se*, à contre-courant de la vision matérialiste dominante. Si l'analyse des incriminations d'extorsion et de chantage permet de sanctionner l'usurpation d'un secret indépendamment de l'existence de tout support, la désolidarisation de l'information et du support met en exergue l'indépendance entre l'information et celui-ci s'agissant notamment de l'infraction de vol et de celle de recel. Bien que la doctrine s'oppose de longue date[412] à propos de la question de l'appropriation de l'information sous la forme d'un droit de propriété, l'utilisation des dispositifs techniques de l'information et de la communication, en ce qu'elle permet la dissociation du support, a revivifié le débat au sein de la doctrine pénaliste quant à la possibilité de consacrer le vol d'informations[413]. Cette dissociation constitue le processus essentiel de ce mouvement. Il est toutefois l'objet de représentations qui faussent l'approche du phénomène puisqu'il est également désigné sous le terme de « dématérialisation ».

75. Le discours et les représentations sur le phénomène de « dématérialisation ». La doctrine, prenant la suite du discours politique, s'est longuement intéressé au phénomène

---

[408] G. BEAUSSONIE, *La prise en compte de la dématérialisation des biens par le droit pénal. Contribution à l'étude de la protection pénale de la propriété*, préf. B. DE LAMY, coll. Bibliothèque de droit privé, t. 532, LGDJ, 2012.
[409] *Ibid.*, n° 13.
[410] *Ibid.*, n° 380.
[411] *Ibid.*, n° 34. A propos, par exemple, du vol d'information, v. *contra* E. DREYER, *Droit pénal spécial*, 3ème éd., coll. Cours magistral, Ellipses, 2016, n° 880.
[412] Pour un résumé des positions de la doctrine v. J. ROCHFELD, *Les grandes notion du droit privé*, 2e éd., coll. Thémis, PUF, 2013, n° 4.35 d).
[413] G. BEAUSSONIE, « A propos d'une controverse contemporaine et persistante : le vol d'informations », *Revue de droit d'Assas*, déc. 2018, n° 17, p. 99.

qu'elle a désigné sous le terme de « dématérialisation ». D'ordre technique et social, ce phénomène est parfois pris comme synonyme de « numérisation ». Il consiste, en effet, dans une première représentation, à se débarrasser des documents papiers ou des autres supports physiques en numérisant les documents. La numérisation est alors le fait d'utiliser un scanner pour reproduire un document papier sous forme électronique, l'océriser, ce qui n'implique pas nécessairement l'absence d'un document sur support physique[414]. La dématérialisation concernerait également des processus : dématérialisation des échanges[415], des procédures[416]. Ce phénomène serait au cœur de la société depuis l'apparition et la démocratisation conjointe de l'informatique et des réseaux de communication[417]. La « dématérialisation » ainsi décrite fait naître une opposition entre l'écrit représenté sur un support tel qu'il a été envisagé jusqu'à présent – caractérisé par sa matérialité – et l'écrit d'écran, caractérisé par son opposition au monde analogique. Appréhendée de la sorte, la « dématérialisation » concernerait aussi bien les supports de la mémoire que ceux de la communication. Elle permet même, contrairement à la téléphonie qui consiste dans le seul usage des réseaux de communication, à remplacer la rencontre physique des personnes[418].

Toujours selon cette représentation, la « dématérialisation » s'entendrait de deux processus. D'une part, la dématérialisation concernerait les documents et dossiers conservés sur

---

[414] M.-C. DAUBIGNEY, « La marche vers la dématérialisation de la procédure pénale », *AJ pénal*, 2007, p. 460.
[415] O. CACHARD, *La régulation internationale du marché électronique*, préf. P. FOUCHARD, coll. Bibliothèque de droit privé, t. 365, LGDJ, 2002.
[416] La procédure pénale ferait ainsi l'objet d'une dématérialisation constante. Sur le sujet, v. M. VELICOGNA, *Utilisation des technologies de l'information et de la communication (TIC) dans les systèmes judiciaires européens*, *Les études de la CEPEJ*, n° 7, 2007 ; S. SONTAG-KOENIG, *Les droits de la défense face aux technologies de l'information et de la communication*, th. dact. ss. la dir. de J.-P. JEAN, soutenue le 13 déc. 2013, Université de Poitiers ; A. TOURE, *L'influence des nouvelles technologies dans l'administration de la justice pénale*, th. dact. ss. la dir de S. CIMAMONTI, soutenue le 8 déc. 2015, Université Aix-Marseille ; J. BOSSAN, « La dématérialisation de la procédure pénale », *D.* 2012, p. 627 ; M.-C. DAUBIGNEY « La marche vers la dématérialisation de la procédure pénale », *op. cit.* ; S. SONTAG, « La dématérialisation des procédures », *AJ pénal* 2014, p.154. Sur des points précis de procédure pénale, les articles sont nombreux : S. SONTAG, « L'accès de l'avocat aux procédures dématérialisées » *AJ pénal* 2011, p. 455 ; « La signature électronique en procédure pénale : une évolution amorcée », *AJ pénal* 2014, p. 123.
[417] Le fameux rapport au Président de la République de Messieurs Minc et Nora est souvent présenté comme le point de départ du projet politique de l'informatisation. Son ambition était d'ailleurs de poser les bases permettant de « *déterminer une politique d'informatisation de la société* ».
[418] En matière judiciaire la visioconférence a fait l'objet d'une étude de sociologie du droit : L. DUMOULIN, C. LICOPPE (ss. la dir.), *Justice et visioconférence : les audiences à distance. Genèse et institutionnalisation d'une innovation*, contrat GIP Mission de recherche Droit et Justice / ISP / Télécoms Paris-Tech, Rapport final, janv. 2009 ; *Adde* A. TOURE, *L'influence des nouvelles technologies dans l'administration de la justice pénale*, *op. cit.*, n° 1 ; Sur la visioconférence et l'administration de la justice, v. *Ibid.*, n° 76 à 95.

support papier et d'autre part, les échanges et le partage d'informations jusqu'alors majoritairement effectués par le biais des correspondances sur support papier. Par exemple, Madame Touré, dans son étude relative à l'influence des technologies de l'information et de la communication sur l'administration de la justice pénale, considère que la dématérialisation n'est pas qu'un procédé de *numérisation* mais aussi un processus de *« non matérialisation »*[419]. L'information, directement traitée informatiquement n'aurait pas de support physique, elle serait néanmoins représentée quand bien même son support serait également immatériel[420]. La dématérialisation recouvrirait donc plusieurs procédés techniques : la numérisation des supports papier de l'information[421], l'absence de matérialisation et enfin la dématérialisation des moyens de la communiquer. Se retrouve parfois l'expression « *dématérialisation des informations* »[422] ou « *dématérialisation des données* »[423] dans le discours de la doctrine.

76. La dématérialisation dans le discours politiques et son emploi dans les politiques de santé publique. Le domaine de la santé n'a pas échappé à cette représentation de la « dématérialisation » qui fait l'objet de politiques publiques de maîtrise des dépenses de santé et d'amélioration de la qualité des soins. Les projets des gouvernements en la matière ne sont pas récents. A d'abord été évoquée la « dématérialisation » des feuilles de soins que les assurés sociaux transmettaient à la Caisse nationale d'assurance maladie afin de bénéficier du remboursement de leurs soins ou médicaments[424], puis celle de l'historique de

---

[419] A. TOURE, *op. cit.*, n° 34.

[420] En sciences de l'information et de la communication, un phénomène analogue est appelé « redocumentarisation ». Dans la définition qui en est donnée, la prétendue dématérialisation du support physique de l'information n'a pas d'intérêt, il s'agit plutôt du passage d'un document à un autre (R. PEDAUQUE (ss. la dir.), *La Redocumentarisation du Monde*, éd. Cépadues, 2007 ; R. PEDAUQUE, J.- M. SALAUN, *Le document à la lumière du numérique*, C&F éd., 2006). Selon cette théorie, les activités des individus sur internet constituent également une forme de redocumentation de soi (O. ERTZSCHEID, « L'homme est un document comme les autres : du World Wide Web au World Life Web », *Revue Hermès* 2009, p. 33).

[421] Utilisant l'expression dématérialisation des dossiers : M. DUPONT, *Feuillets mobiles, Litec Droit médical et hospitalier*, Fasc. 9-30 : « Dossier en établissement de santé. Dossier dématérialisé », nov. 2016.

[422] Pour ne donner qu'un seul exemple : C.-A. DUBREUIL, « La démocratie et la transparence », *RFDA* 2016, p. 655.

[423] Par exemple : A.- L. BENEAT, P. BALLET, « Dématérialisation des données de santé : quels référentiels ? », *Gaz. Pal.,* 22 janv. 2011, p. 22 ; F.- J. PANSIER et C. CHARBONNEAU, « La dématérialisation des données médicales et les enjeux de leur hébergement », *Gaz. Pal.,* 17 déc. 2002, p. 23 ; O. DE MAISON ROUGE, « Décryptage sur la protection juridique des informations sensibles », *Dalloz IP/IT* 2017, p. 273 ; F. EON, « Hôpital public et données personnelles des patients », *RDSS* 2015, p. 85).

[424] L'objectif politique de cette première étape de « dématérialisation » avait pour ambition de maîtriser les dépenses de santé, le plan dit « Juppé » a engagé sa mise en œuvre dès 1996 (ordonnance n° 96-345 du 24 avril 1996 relative à la maitrise médicalisée des dépenses de soins) grâce au système Sesam-Vitale. Il s'agit d'un système d'échanges électroniques sécurisé – grâce aux cartes nominatives du professionnel (CPS) et à la carte

remboursements[425] (*Web* médecin) de chaque assuré social, également informatisé et accessible grâce aux cartes précitées. Les projets dits de « dématérialisation » se sont ensuite accélérés au rythme des innovations et des évolutions des dispositifs techniques de l'information et de la communication. La télémédecine, dont l'usage est ancien[426], s'est imposée à partir des années 2000 comme une opportunité pour le marché européen, comme en témoignent les plans d'action sur la santé en ligne lancés au début du millénaire par la Commission européenne[427]. Les gouvernements successifs ont ensuite fait une large promotion en faveur de son

Vitale (dont le patient est porteur mais appartenant à la caisse d'assurance maladie) – entre les professionnels de santé et les organismes d'assurance maladie. Cet échange est rendu possible grâce à la non-matérialisation de la feuille de soin qui est directement saisie, par le professionnel de santé, sur le terminal de son ordinateur *via* un logiciel spécifique. Les informations saisies sont ensuite télétransmises à l'organisme d'assurance maladie. Utilisant à la fois l'informatique et les réseaux de communication, il s'agit donc d'une application particulière de la télématique, ou e-santé (v. P. LAFARGE, « Secret professionnel, confidentialité et nouvelles technologies d'informations », *Gaz. Pal.* 1998, p. 481 ; A. LOTH, « Systèmes d'information et cartes de santé », *Droit social* 1996, p. 829 ; E. PIDOUX, « La responsabilité médicale au regard de la télétransmission et de la télémédecine », *LPA* 27 juill. 2000, p. 5 ; N. REBOUL-MAUPIN, « Responsabilités des médecins et internet », *Gaz. Pal.*, 26 mars 2002, p. 28).

[425] Créé par la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie (*JORF,* 17 août 2004).

[426] Les premières applications de la télémédecine sont anciennes. Utilisant dans un premier temps les ondes radio, elles ont permis de soigner les personnes auxquelles aucun médecin ne pouvait venir en aide, notamment les marins et le personnel scientifique en expédition (N. FERRAUD- CIANDET, *Droit de la télésanté et de la télémédecine*, éd. Heures de France, 2011, p. 12). La réflexion est engagée en France à partir des années 1990 et les rapports et études sur la question se succèdent, quelques exemples : J.-P. THIERRY, *La télémédecine, enjeux médicaux et industriels*, Rapport, Ministère de l'industrie des postes et des télécommunications et du commerce extérieur, Ministère de l'enseignement supérieur et de la recherche, Ministère des affaires sociales de la santé et de la ville, 1993 ; J. GROS, *Santé et nouvelles technologies de l'information*, Conseil économique et social, 2002 ; V. HAZEBROUCQ Rapport sur l'état des lieux, en 2003, de la télémédecine française, Ministère de la jeunesse, de l'éducation nationale et de la recherche, 2003 (disponible sur : <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/034000522.pdf> (dernière consultation le 15 août 2019) ; J. DIONIS DU SEJOUR, J.-C. ETIENNE, *Les télécommunications à haut débit au service du système de santé*, Office parlementaire d'évaluation des choix scientifiques et technologiques, Assemblée nationale – Sénat, 2004.

[427] Communication de la Commission au Conseil, au Parlement européen, Comité Économique et Social Européen et au Comité des régions, « *e*-Europe 2005 : une société de l'information pour tous », COM (2002) 263, mai 2002 ; Communication de la Commission au Conseil, au Parlement européen, Comité Économique et Social Européen et au Comité des régions, « Santé en ligne - améliorer les soins de santé pour les citoyens européens : plan d'action pour un espace européen de la santé en ligne », COM (2004) 356, avr. 2004 (Plus largement sur la télésanté en Europe v. N. FERRAUD-CIANDET, *RTD eur.* 2010, p. 537 ; F. SAUER, « Europe et télésanté », *RDSS* 2011, p. 1029).

développement[428], jusqu'à sa consécration[429] et son encadrement par décret[430]. Suivant la représentation du phénomène sous le terme de « dématérialisation », la télémédecine ne procède pas d'une « dématérialisation » des documents mais d'une « dématérialisation » des actes de soins engendrant une pratique de ceux-ci à distance. La télémédecine pose principalement des questions relatives aux responsabilités des divers acteurs[431], car il ne s'agit que d'une application particulière des réseaux de communication. Aussi, l'acte de télémédecine peut-il se réaliser par téléphone[432] ou grâce à l'utilisation d'un dispositif dédié permettant la pratique à distance des actes de soins. Il s'agit néanmoins de véhiculer des informations entre deux personnes, ce qui fait de l'acte de télémédecine une forme de correspondance « dématérialisée ». Enfin, le discours sur la « dématérialisation » concerne aussi les documents médicaux et les dossiers qui les contiennent – dossiers médicaux ou médico-sociaux[433], dossier

---

[428] La promotion de la télémédecine est principalement menée au travers d'une stratégie de gouvernance conduite par la Direction générale de l'offre de soin (DGOS) et la Haute autorité de santé et dont les Agences Régionales de Santé. La place de ces acteurs s'explique par le fait que la télémédecine est surtout représentée comme une « dématérialisation » de la relation de soin pouvant résoudre les problèmes d'accès au soin sur les territoires à faible démographie médicale (C. BOURDAIRE-MIGNOT, « Téléconsultation : quelles exigences ? Quelles pratiques ? », *RDSS* 2011, p. 100).

[429] La loi n° 2004- 810 relative à l'assurance maladie propose une première définition de la télémédecine (art. 32).

[430] La définition de la télémédecine sera précisée par l'article 78, I (CSP, art. L. 6316- 1) de la Loi n° 2009- 879 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires (HPST), sa mise en œuvre précisée par le Décret n° 2010- 1229 relatif à la télémédecine et par plusieurs circulaires.

[431] Les questions qui ont occupé les juristes concernent davantage les responsabilités en cas de dommage. Sur le sujet, v. S. LANGARD, *Approche juridique de la télémédecine : entre droit commun et règles spécifiques*, th. dact. ss. la dir. de B. PY et J.-B. THIERRY, soutenue le 15 déc. 2012, Université de Lorraine ; et parmi les nombreux articles de doctrine sur la question du développement de la télémédecine et ses enjeux v. O. RENAUDIE, « Télémédecine et téléservice public », *RFAP* 2013, n° 146, p. 262 ; M. CONTIS, « La télémédecine : nouveaux enjeux, nouvelles perspectives juridiques", *RDSS* 2010, p. 235 ; Concernant les aspects ayant trait à la responsabilité et particulièrement celle des tiers technologiques v. J.- F. FORGERON, « Les application de télémédecine : des responsabilités médicales traditionnelles aux responsabilités techniques nouvelles », *Gaz. Pal.* 16 oct. 2001, n° 289, p. 20 ; S'agissant de la responsabilité civile des médecins v. E. PIDOUX, « La responsabilité médicale au regard de la télétransmission et de la télémédecine », *op. cit.* ; C. CORGAS-BERNARD, « Responsabilité civile médicale et nouvelles pratiques numériques : l'exemple de la télémédecine », *LPA* 18 août 2014, n° 164, p. 27 ; Sur les responsabilités civile, pénale et disciplinaire des acteurs, v. L. GRYNBAUM, « La responsabilité des acteurs de la télémédecine », *RDSS* 2011, p. 996.

[432] La régulation médicale est un acte de télémédecine : CSP, art. R. 6316-1.

[433] Ainsi qu'il a déjà été mentionné (v. *supra* n°51), les informations recueillies par les personnes soumises au secret professionnel dans le cadre d'une prise en charge médicale ou médico-sociale sont nombreuses et les dossiers ont longtemps été disséminés. Il existait autant de dossiers que de types de soins (dossier psychiatrique, dossier infirmier, dossier d'anesthésie …). D'abord conçus comme une extension de la mémoire des professionnels, les dossiers sont ensuite apparus d'une utilité certaine pour assurer la qualité de la prise en charge des patients à condition qu'ils soient accessibles et partagés (V. *infra* n° 236). Depuis la loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, un effort de rapprochement de ces dossiers est amorcé, tous les documents font désormais partie d'un dossier médical unique, que les établissements publics ou privés ont l'obligation de renseigner et dont le contenu est fixé par décret (CSP, art. R. 1112-2). Les professionnels de santé en exercice libéral tiennent également un dossier médical, la seule disposition qui en traite étant déontologique (Code de déontologie médicale, art. 45, et CSP, art. R. 4127-45). Il existe un dossier médical

médical partagé[434], dossier pharmaceutique[435] –, la dématérialisation étant présentée comme l'un des objectifs centraux des politiques de santé, ensuite intégrée dans une vaste stratégie

en santé au travail (DMST) mentionné à l'article D. 4624-46 du Code du travail. Tous ces dossiers, contenant des informations relatives au malade et pour le dernier, au salarié, sont désormais informatisés et font donc l'objet, dans le discours, d'une « dématérialisation ». Il faut enfin signaler le dossier résident informatisé ouvert pour les personnes résidant en EHPAD.

[434] Le dossier médical partagé (DMP) est pensé, dès l'origine, comme un dossier informatique aux nombreuses vertus pour la prise en charge des malades aussi bien en ville qu'à l'hôpital : plus qu'un outil de maîtrise de dépenses de santé il permet d'assurer un suivi efficace des patients (M. FIESCHI, *Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins*, Rapport au ministre de la Santé, de la Famille et des Personnes handicapées, janv. 2003). Créé par la loi du 13 août 2004 (Loi n° 2004-810), il devait être effectif au 1er juillet 2007 mais sa généralisation s'est faite attendre (En 2008 une mission de relance du DMP a été nommée, le groupe de travail a rédigé un ensemble de recommandations destiné à dégager une stratégie de mise en œuvre de ce dossier informatisé : M. GAGNEUX, *Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information en santé*, Rapport à la ministre de la Santé, de la Jeunesse, des Sports et de la Vie associative, disponible en ligne : <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000279.pdf> (dernière consultation le 15 août 2019) ; A. MONNIER, « Le Dossier médical Personnel : historique, encadrement juridique et perspectives », *RDSS* 2009, p. 625). Le dispositif législatif et règlementaire encadrant le DMP a ensuite été plusieurs fois modifié jusqu'à la loi n° 2016-41 du 21 janvier 2016. Sur les vicissitudes du DMP, v. M. DUPONT, *Feuillets mobiles, Litec Droit médical et hospitalier*, Fasc. 9-30 : « Dossier médical. Dossier en établissement de santé. Dossier dématérialisé », n° 52 à 64. Pour une monographie complète, bien que déjà datée, sur les questions relatives au DMP, v. C. ZORN, *Donnes de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, coll. « Santé, qualité de vie et handicap », PUN, 2010. Il faut enfin noter que la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, *JORF* n°0172 du 26 juillet 2019).

[435] Le dossier pharmaceutique (DP) est une initiative de l'Ordre national des pharmaciens. L'outil trouve une base légale dans la loi de financement de la sécurité sociale pour 2007 (Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions, *JORF*, 1er févr. 2007). Défini à l'article L. 4211-1 CSP, ce dossier est conçu pour « *favoriser la coordination, la qualité, la continuité des soins et la sécurité de la dispensation des médicaments, produits et objets définis à l'article L. 4211-1* » (CSP, art. L. 1111-23). C'est le Conseil national de l'ordre des pharmaciens qui met en œuvre le DP, celui-ci étant organisé par un décret pris en Conseil d'Etat après avis de la CNIL (Décret n° 2008-1326, 15 déc. 2008 *: JORF,* 17 déc. 2008, p. 19237 ; CSS, art. R. 161-58-1 à R. 161-58-11). Par ailleurs, depuis la loi n° 2009-879 du 21 juillet 2009 (HPST), les informations contenues dans le dossier pharmaceutique et utiles à la prise en charge sont reportées dans le dossier médical partagé (CSP, art. L. 1111-23). Celui-ci doit donc permettre d'alimenter le dossier médical partagé. Pour une description complète de l'outil et de sa mise en œuvre v. C. LE GAL, « Le dossier pharmaceutique : un outil technique de santé publique », *RDSS* 2009, p. 301. Sur l'alimentation du DMP par le DP, laquelle prend la forme d'une interopérabilité (selon le dictionnaire Larousse, ce terme technique désigne, en matière informatique la « *capacité de matériels, de logiciels ou de protocoles différents à fonctionner ensemble et à partager des informations* ») prévue à l'article R. 1111-20-10 CSP, v. J.-B. DUFOUR, « Le dossier pharmaceutique : du DP patient au DP rupture, un formidable outil de santé publique créé par les pharmaciens », *RGDM*, n° 67, 2018, pp. 19-28.

nationale[436]. C'est également un objectif central de la stratégie nationale de santé 2018-2022[437], des plans « e-santé 2020 »[438] et « ma santé 2022 »[439]. Le terme est, enfin, visé pour qualifier l'utilisation des dispositifs techniques de l'information et de la communication par les différents acteurs au sein des structures hospitalières et entre médecins libéraux pour l'envoi et la réception des communications[440]. Ainsi, c'est tout le système de santé qui ferait l'objet d'une transformation qualifiée de « dématérialisation ». Il nous semble nécessaire de revenir sur le phénomène ainsi identifié.

77. Un phénomène mal nommé. Si la dématérialisation consiste à retirer de la matière, à rendre immatériel, il nous semble que ce terme ne peut servir à désigner le phénomène de suppression des supports papier. Comme l'indique un auteur spécialiste des sciences de l'information et de la communication, « *l'écrit ne se dématérialise pas* »[441] mais « *l'écriture redéfinit radicalement la relation qui la lie à la matière de son support. En quelque sorte, la trace se désolidarise du support. Plus profondément, l'écrit, qui n'était déjà plus graphie (trace du geste) avec l'imprimé, cesse d'être trace avec l'informatique* »[442]. Il précise encore, à propos

---

[436] La direction de la Caisse nationale d'assurance a publié un rapport visant à généraliser l'e-prescription, c'est-à-dire la prescription dématérialisée, dès 2019 : v. *Améliorer la qualité du système de santé et maîtriser les dépenses*, juin 2018, Propositions de l'Assurance Maladie pour 2019, Rapport au ministre chargé de la Sécurité sociale et au Parlement sur l'évolution des charges et produits de l'Assurance Maladie au titre de 2019 (loi du 13 août 2004), proposition n° 25). Le gouvernement a mis en place, à partir de 2011, un plan national favorisant le passage au numérique. Ce plan de gouvernance piloté par la DGOS et au niveau local par les ARS, comprend un certain nombre d'objectifs centrés sur l'effectivité des dossiers patients informatisés, la compatibilité des systèmes d'information avec le DMP, l'informatisation des résultats d'imagerie, de biologie et d'anatomo-pathologie. En somme, c'est l'informatisation et la dématérialisation ou la non-matérialisation de l'ensemble des systèmes d'informations des établissements publics de santé qui est recherchée (v. Hôpital Numérique. Guide des indicateurs des prérequis et des domaines prioritaires du socle commun, DGOS, avr. 2012, disponible sur <http://solidarites-sante.gouv.fr/IMG/pdf/DGOS_Guide_d_indicateurs_Programme_Hopital_Numerique_-_avril_2012-2.pdf> (dernière consultation le 19 août 2019)).

[437] Stratégie nationale de santé 2018-2022 du ministère des solidarités et de la santé (disponible en ligne : <http://solidarites-sante.gouv.fr/IMG/pdf/dossier_sns_2017_vdef.pdf> (dernière consultation le 15 août 2019)).

[438] Stratégie nationale e-santé 2020, *Le numérique au service de la modernisation et de l'efficience du système de santé*, 4 juill. 2016 (disponible en ligne : <https://solidarites-sante.gouv.fr/IMG/pdf/strategie_e-sante_2020.pdf> (dernière consultation le 6 sept. 2019)).

[439] Stratégie nationale « Ma santé 2022 » (disponible en ligne : <https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/ma-sante-2022-un-engagement-collectif/> (dernière consultation le 6 sept. 2019)).

[440] Par le biais des messageries électroniques sécurisées qui permettent notamment l'envoi et la réception des lettres de liaison prévues à l'article L. 1112-1 du Code de la santé publique. Ces dernières pouvaient, selon les termes de la loi, être « dématérialisées ». Le décret n° 2016-995 du 20 juillet 2016 relatif aux lettres de liaison prévoit désormais la seule transmission dématérialisée.

[441] Y. JEANNERET, *Y-a-t-il vraiment des technologies de l'information et de la communication,* coll. Savoirs mieux, Presses universitaire Septentrion, 2011, « Chapitre 4. L'écrit d'écran : lire, écrire et un peu davantage », n° 31.

[442] *Ibid.*, n° 27.

de la *dématérialisation* qu'il qualifie d'idéologie : « *Le technicien sait bien que la miniaturisation des dispositifs est une condition de la « révolution numérique » et que l'équipement informatique demande beaucoup de quincaillerie (en anglais : « hardware »). Quant au sémioticien, il sait que tout processus de signification comporte un plan de l'expression, c'est-à-dire une face matérielle* »[443]. Nous ne pouvons qu'abonder dans le sens de cet auteur. L'information non représentée est toujours immatérielle. Aussi, parler de « dématérialisation de l'information » ou de « dématérialisation des données » n'a pas grand sens. Ensuite, la télémédecine n'est pas une dématérialisation de l'acte de soin, comme d'ailleurs l'utilisation de la visioconférence n'est pas une dématérialisation de l'audience mais signale l'existence d'une interface entre les personnes[444]. Enfin, la numérisation des documents ou le traitement informatique des informations consiste bien en une redéfinition du rapport entre l'écrit et son support. Les supports continuent d'exister, ce sont tous les dispositifs informatiques. Le rapport entre le support papier et l'écrit n'est pas le même qu'avec le support informatique : dans le premier cas, l'écrit est indissociable de son support, dans le second, l'information peut être appréhendée indépendamment de son support.

78. Protection incidente du secret des informations par les infractions sanctionnant une atteinte aux biens. L'immatérialité intrinsèque de l'information a été évoquée, de même que sa représentation et, partant, l'évidente protection de son secret par la protection du support qui l'incorpore. Nous souhaitons évoquer le rôle des infractions sanctionnant l'atteinte aux biens dans la protection du secret des informations, qu'il s'agisse de constater que le *secret* peut être l'objet de certaines infractions contre les biens ou que l'usurpation de l'information est sanctionnée indépendamment de son support. Ce qui relèverait d'un double mouvement : une prise en compte de la dématérialisation des biens par le droit pénal, nous invitant à concevoir l'existence de biens informationnels d'une part, et la dématérialisation de certaines infractions contre les biens liée à la possibilité de dissocier l'information de son support d'autre part. Notre développement a donc pour objet de démontrer que le « secret médical » peut s'entendre de la protection du *secret-état* par d'autres mécanismes que le secret professionnel. Il s'agit

---

[443] *Ibid.* n° 27.

[444] L'interface, en informatique et au sens figuré peut se définir comme une « *zone de contacts et d'échanges* » (TLFi, *V°* « Interface »). La rencontre entre deux personnes dans un espace donné s'effectue sans intermédiaire, chacun est accessible par la totalité des sens, tandis que la rencontre qui s'opère par une interface rend inactifs certains sens, le rapport sera alors, souvent, auditif et/ou visuel.

également de démontrer que certaines infractions contre les biens sanctionnent l'atteinte au secret des informations lorsqu'elle est usurpuées indépendamment de son support.

B - Les appropriations indues

79. Les ressources du droit pénal spécial permettent de sanctionner l'obtention illicite de l'information secrète indépendamment de son support **(1)** mais également l'atteinte au secret des correspondances échangées par voie électronique **(2)**.

1 - L'obtention illicite de l'information secrète

80. Il apparaît que que plusieurs infractions contre les biens sont susceptibles de protéger, de manière incidente, les informations secrètes appréhendé indépendamment de leur support tandis qu'une infraction sanctionne spécifiquement l'obtention irrégulière d'information couvertes par le secret professionnel dans le domaine de la santé (a). Un développement particulier doit être réservé à celle sanctionnant l'atteinte aux systèmes de traitement automatisé de données du fait de la particularité des modifications dont elle a fait l'objet (b).

a - La concurrence entre les infractions contre les biens et l'infraction spéciale d'obtention d'informations couvertes par le secret professionnel dans le domaine de la santé

81. Le Code pénal connaît une infraction contre les biens susceptibles de sanctionner l'obtention frauduleuse de l'information secrète tandis que l'article L. 1110-4-IV du Code de la santé publique sanctionne l'obtention irrégulière de l'information secrète issues de la prise en charge des personnes par des professionnels intervenant dans le système de santé (i). Par ailleurs, le juge pénal est à l'origine de la dématérialisation des éléments de l'infraction sanctionnant les appropriations frauduleuses, l'infraction est donc également susceptible de s'appliquer à l'appropriation d'informations secrètes (ii).

i - L'obtention frauduleuse et l'obtention irrégulière d'informations couvertes par le secret

82. L'extorsion de secret. L'emploi de certains moyens peut être destiné à contraindre un professionnel soumis au secret à révéler des informations ou à transmettre un document contenu dans le dossier médical d'un patient. Les personnes ayant intérêt à prendre connaissance de telles informations sont nombreuses. Un employeur, par exemple, a tout intérêt à connaître les

raisons de l'arrêt maladie de l'un de ses salariés afin de pouvoir anticiper certaines de ses décisions ; une compagnie d'assurance peut souhaiter infirmer ou confirmer l'état de santé d'un assuré ; lors d'un procès, l'une des parties, à l'appui de sa demande, peut souhaiter apporter des éléments médicaux concernant la partie adverse. L'infraction d'extorsion ne protège toutefois qu'incidemment le secret des informations et, a *fortiori,* le secret des informations relatives à la santé. En tant qu'infraction voisine du vol[445], elle permet en effet de sanctionner l'agent qui contraindrait une personne soumise au secret à lui révéler un fait secret (objet de l'infraction), ayant pour conséquence une *atteinte au secret*. En effet, les articles 312-1 et suivants du Code pénal, inscrits au sein du titre consacré aux appropriations frauduleuses, sont relatifs à l'extorsion. L'infraction, définie à l'article 312-1, sanctionne « *le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque* »[446]. Les moyens employés par l'agent afin d'obtenir la révélation des informations n'appellent pas de remarques particulières. La liste de ces moyens est exhaustive et permet de distinguer l'extorsion des autres infractions contre les biens[447], notamment de l'escroquerie, cette dernière étant caractérisée par la mise en œuvre de manœuvres frauduleuses[448] tandis que l'extorsion est caractérisée par l'emploi de la violence, de menace de violence ou de la contrainte. L'élément moral réside dans la conscience que la remise – ou, dans notre hypothèse, la révélation – est « *la conséquence des pressions exercées sur la victime* »[449]. Quant à l'objet de l'infraction, il peut s'agir d'une information secrète de toute nature[450]. La tentative du délit est également punissable[451]. Cette infraction apporte une protection tout à fait subsidiaire au secret des

---

[445] V. par ex. E. DREYER, *Droit pénal spécial*, 3ème éd., coll. Cours Magistral, Ellipses, 2016, n° 921 ; M. VERON, *Droit pénal spécial*, 17ème éd., coll. Université, Sirey, 2019, p. 327 ; M.-L. RASSAT, *Droit pénal spécial*, 8ème éd., coll. Précis, Dalloz, 2018, n° 204.
[446] CP, art. 312-1.
[447] E. CLEMENT, « Concours et cumul des infractions contre les biens », *AJ pénal* 2017, p. 219.
[448] M. REDON*, Rép. pén., V°* « Extorsion », nov. 2016, n° 9.
[449] E. DREYER, *Droit pénal spécial*, *op. cit.*, n° 922.
[450] *Contra* M.- L. RASSAT, *Droit pénal spécial*, *op. cit.*, n° 205 : Madame Rassat distingue les « secrets » ayant une incidence matérielle, comme par exemple la révélation d'un lieu où se trouve un objet de valeur, et les « secrets » ayant une incidence personnelle. Cet auteur considère que l'infraction punissant l'extorsion ne devrait s'appliquer que pour les premiers secrets. Selon elle, si le juge entrait en voie de condamnation pour des faits d'extorsion de secrets ayant une incidence personnelle, il faudrait en déduire que l'infraction est « *mal classée* » puisqu'elle n'aurait pas sa place dans les infractions contre les biens.
[451] CP, art. 312-9.

informations relatives à la santé en raison de l'existence d'une infraction spéciale prévue à l'article L. 1110-4, V du Code de la santé publique.

83. Le concours entre l'extorsion et l'obtention irrégulière d'informations couvertes par le secret professionnel dans le domaine de la santé. La jurisprudence portant sur des infractions d'extorsion de secret est faible[452]. S'agissant particulièrement de l'extorsion, à un professionnel tenu au secret, d'une information relative à la santé d'un malade, une seule affaire a été portée à notre connaissance. A l'occasion d'un conflit de voisinage, une des parties avait intenté à sa propre vie, tentative de suicide dont elle tenait son voisin pour responsable. A la suite de la révélation de ces informations par l'époux, certificat médical à l'appui, le voisin auquel les reproches étaient adressés avait contacté le médecin à l'origine du certificat médical. Il était poursuivi pour avoir, selon le témoignage du médecin « […] « essayé de la relever du « secret médical » *et* [avoir] *proféré des propos calomnieux à l'égard de sa patiente* »[453]. L'acte de poursuite prévoyait le chef de prévention d'extorsion et celui d'obtention irrégulière d'informations médicales à caractère secret prévu à l'article L. 1110-4, V du Code de la santé publique. La décision de la cour d'appel prononçant la relaxe encourt la cassation dès lors que les juges du fond n'ont pas examiné la prévention de tentative d'obtention irrégulière d'informations médicales à caractère secret, également visée par l'acte de poursuite. Cet unique arrêt est parfois cité au sein des manuels et encyclopédies de droit pénal[454] comme une illustration de l'extorsion de secret. Pourtant, les juges ne se prononcent qu'au regard du seul chef de prévention issu de l'article L. 1110-4, V du Code de la santé publique. Si le concours entre ces infractions peut paraître idéal, l'infraction prévue au texte précité couvre un champ plus large. En effet, l'obtention ou la tentative d'obtention d'information est punie sans que soit exigé un quelconque moyen de l'appropriation frauduleuse. Aussi, une simple demande d'information, sans recours à une quelconque manœuvre, à des violences ou menaces, paraît suffire à qualifier l'infraction. L'élément moral ne ressort pas expressément de la définition, sans doute peut-il être déduit de la conscience de l'agent d'obtenir des informations couvertes par le secret. Pourtant, la preuve de l'intention – dol général –, ne semble pas pouvoir aisément découler de l'élément matériel en l'absence de toute précision, ce qui, par ailleurs, interroge au

[452] Nous n'avons connaissance que de la seule décision relatée.
[453] Crim., 26 mars 2008, n° 07-87072.
[454] Par exemple : M. REDON, *Rép. pén.*, *V°* « Extorsion », nov. 2016, n° 6.

regard du principe de légalité criminelle[455]. Outre le caractère spécial du texte, la faiblesse de la légalité du texte dont découle un champ d'application extrêmement large facilite le choix de la qualification idoine.

84. Un constat identique concernant l'infraction de chantage. Le chantage est, comme l'extorsion, une infraction sanctionnant les atteintes aux biens et, comme pour l'infraction d'extorsion, sa rédaction fut modifiée lors de la réforme du Code pénal[456] pour étendre son domaine. Le secret peut faire l'objet d'un chantage ou d'une tentative de chantage. L'infraction définie à l'article 312-10 du Code pénal est voisine de l'extorsion et ne s'en distingue que par les moyens employés en vue d'amener la victime à la révélation d'un secret. L'élément matériel du chantage exige, pour être constitué, l'emploi par l'agent de menaces de révélation ou d'imputations de propos diffamatoires, consistant en une révélation publique ou non de faits de nature à porter atteinte à la réputation et à l'honneur de l'individu dont il sollicite la révélation du secret. Ici encore les qualifications de chantage et d'obtention irrégulière d'informations médicales à caractère secret peuvent paraître donner lieu à un concours idéal. Celui-ci n'est toutefois qu'apparent puisque le domaine de l'infraction prévu à l'article L. 1110-4, V du Code de la santé publique permet de sanctionner l'obtention ou la tentative d'obtention indépendamment des moyens employés.

85. Infractions contre les biens, étendues à des biens sans valeur patrimoniale. Bien que rangées dans le titre consacré aux infractions contre les biens, l'extorsion et le chantage ne constituent pas une démonstration de la reconnaissance, par le droit pénal, de la propriété des

---

[455] Notons, sur ce point, qu'il a pu être reproché le manque de clarté et de qualité de ce droit pénal dit « technique » au profit de l'efficacité. Le droit pénal médical, entendu comme l'ensemble des normes pénales qui s'appliquent à l'activité médicale, a été qualifié de « *droit pénal au rabais* » par Monsieur Mistretta (P. MISTRETTA, *Droit pénal médical*, Cujas, 2013, n° 52). L'auteur constate et critique la prolifération des renvois formant de véritables « *renvois à la chaîne* » (*ibid.,* n° 53). Cette « *légalité mal maîtrisée* » (*ibid.,* n° 56) nuit à l'accessibilité de la norme et participe à son incohérence. Par ailleurs, le texte d'incrimination, de type *ouvert*, porte une autre lacune ; l'individu se trouve dans l'impossibilité de savoir quel est le comportement punissable (E. DREYER, *Droit pénal spécial*, 3e éd., coll. Cours magistral, ellipses, 2016, n° 28). L'arrêt évoqué (Crim., 26 mars 2008, n° 07-87072) illustre, en outre, le fait que la matière est jalonnée d'incriminations presque identiques à celles, plus générales, inscrites dans le Code pénal. Pour une réflexion plus générale sur le dol général et le constat selon lequel « *aucune recherche psychologique, d'ordre subjectif, n'est menée pour vérifier l'intensité avec laquelle l'agent à réellement voulu son acte* », v. E. DREYER, *Droit pénal général*, LexisNexis, 5ème éd., 2019, n° 895 et svt..

[456] Loi n° 92-684 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes (*JORF* n°169, 23 juill. 1992 p. 9857).

informations secrètes. Comme l'ont remarqué les auteurs du *Code pénal commenté*[457], le caractère plus compréhensif de la rédaction du texte d'incrimination de l'infraction d'extorsion se situe dans le prolongement d'une loi plus ancienne[458] qui avait admis que le délit pouvait porter sur la seule signature et incluait, ainsi, l'extorsion d'écrits n'intéressant pas le patrimoine. Pouvait alors faire l'objet d'une extorsion l'aveu écrit de la commission d'une infraction[459]. Si l'extorsion ou le chantage visant la révélation d'un secret consiste sans doute en une réception de l'immatériel par le droit pénal des biens au sein de l'élément matériel, cette seule démonstration ne peut suffire à affirmer la propriété comme fondement du secret des informations relatives aux personnes et, *a fortiori*, à la santé des malades. Il nous semble plutôt que les incriminations d'extorsion et de chantage sont mobilisées indépendamment de l'intérêt protégé. L'étude de l'infraction de vol, en ce que son texte d'incrimination est moins compréhensif[460] et a pour objet la « chose d'autrui », permet d'interroger de manière plus convaincante l'admission, par le droit de pénal des biens, de l'information indépendamment de toute appropriation de son support.

ii - La dissociation du support et de l'écrit : l'appropriation frauduleuse de l'information secrète

86. L'indépendance de l'information représentée et de son support. Le passage au support informatique a généré des craintes quant à la possibilité, pour un tiers, d'appréhender plus aisément les informations couvertes par le secret que lorsqu'elles sont représentées sur un support physique[461]. La question du vol d'informations s'est toutefois posée bien avant la

---

[457] G. ROUJOU DE BOUBEE, J. FRANCILLON, B. BOULOC, Y. MAYAUD, *Code pénal commenté*, Dalloz, 1992, p. 541.
[458] Loi n° 81-82 du 2 février 1981 renforçant la sécurité et protégeant la liberté des personnes (*JORF* n° 0028, 3 févr. 1981 p. 415).
[459] R. MERLE et A. VITU, *Traité de droit criminel. Droit pénal spécial* (par A. VITU), t. 1, Cujas, 1982, n° 2293.
[460] Tandis que le vol suppose une soustraction matérielle, certaines infractions ne nécessitent qu'une soustraction juridique, ce qui favorise du même coup l'extension du « *nombre de choses à même d'être volées* » (P. CONTE, *Droit pénal spécial*, 4ème éd., LexisNexis, 2013, n° 530). Autrement dit, « *ce qui est sanctionné, c'est un comportement qui a pour conséquence de priver une personne de sa chose, à la différence de l'escroquerie ou de l'abus de confiance, qui supposent seulement la remise d'une chose, sans nécessairement que la remise prive le remettant de sa propriété* » (P. BERLIOZ, « Consécration du vol de données informatiques. Peut-on encore douter de la propriété de l'information ? », *RDC* 2015, p. 951).
[461] « *L'utilisation du support informatique est intrinsèquement porteuse d'insécurités pour le dossier médical (vols, copies de fichiers ...) que multiplient les possibilités récentes de connexion à distance (internet, intranet ...)* » (P. MISTRETTA, « La loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé. Réflexions critiques sur un droit en pleine mutation », *JCP G* 2002, doctr. 141).

généralisation de l'informatique et du numérique. Jusqu'alors, le caractère indissociable de l'information et de son support matériel avait permis à la Cour de cassation de maintenir un doute quant à l'application de l'incrimination de vol pour les informations seules[462], l'existence du support facilitant la caractérisation de l'infraction, laquelle doit porter sur une chose. Une autre difficulté, tenant à l'élément matériel de l'infraction, a alors surgi : « […] *la particularité de l'information consiste dans le fait que sa transmission n'implique pas nécessairement, et même généralement pas, la rupture du lien qui l'unit à celui qui la détient* »[463]. Plus précisément encore : « *Si une personne recopie sur son ordinateur le contenu d'une disquette appartenant à une autre personne, ce contenu informationnel présente la particularité d'exister identiquement en deux endroits à la fois, sans avoir fait l'objet d'une véritable soustraction* »[464]. Plus adapaté aux progrès techniques actuels, l'exemple du téléchargement de données à distance répond au même schéma. Cette ubiquité de l'information invite à ne pas admettre la possibilité de sa soustraction. Si le problème semble ne plus se poser pour l'infraction d'abus de confiance, laquelle a connu une dématérialisation de l'ensemble de ses éléments et n'exige, de plus, qu'une remise ne nécessitant une dépossession préalable[465], le doute quant au vol subsiste.

---

[462] La Cour a parfois usé d'un raisonnement ambigü en admettant le vol par reproduction dès lors qu'il y avait déplacement, même momentané, du support physique de l'information : Crim., 8 janv. 1979, *Logabax*, *Bull. crim.*, n° 73 ; Crim., 3 mars 1992, *D.* 1994, somm. p. 157, obs. G. ROUJOU DE BOUBEE ; *Dr. pén.* 1992, comm. 254. Bien que reconnaissant le vol du contenu informationnel, l'acte matériel consistait dans l'appréhension du support, interdisant toute généralisation quant au vol des seules informations : Crim., 1er mars 1989, *Bull. crim.* n° 100 ; *D.* 1990, somm. p.330, obs. J. HUET ; *RSC* 1990, p. 346, obs. P. BOUZAT, et p. 507, obs. M.- P. LUCAS DE LEYSSAC ; *RTD com.* 1990, p. 142, obs. P. BOUZAT.

[463] P. BERLIOZ, « Consécration du vol de données informatiques. Peut-on encore douter de la propriété de l'information », *op. cit.*.

[464] D. GUTMANN, « Du matériel à l'immatériel dans le domaine des biens », *Arch. phil. dr.*, *Le droit et l'immatériel*, t. 43, 1999, p. 73.

[465] Concernant précisément l'objet de l'infraction, la Cour de cassation a affirmé que « *les dispositions de l'article 314-1 du Code pénal s'appliquent à un bien quelconque et non seulement à un bien corporel* » (A propos du détournement d'un numéro de carte bancaire : Crim., 14 nov. 2000, n° 99-84522, *Bull. crim.*, n° 338 ; *Dr. pén.* 2001, comm. 28 (2e arrêt), obs. M. VERON, et chron. 16, obs. S. JACOPIN ; *D.* 2001, p. 1423, note B. DE LAMY ; *RTD civ.* 2001, p. 912, obs. T. REVET ; *Gaz. Pal.* 2001, 2, somm., p. 1219, note Y. MONNET ; *RSC.* 2001, p. 305, obs. R. OTTENHOF. Au sujet d'un projet de borne numérique de gestion de station d'épuration : Crim., 22 sept. 2004, n° 04-80225, *Bull. crim.*, n° 218 ; *JCP G* 2005, I, 106, n° 1, obs. M. VERON ; *JCP G* 2002, II, 10034, note A. MENDOZA-CAMINADE ; *D.* 2005, p. 411, note B. DE LAMY. Quant au détournement d'un fichier d'entreprise : Crim. 16 nov. 2011, n° 10-87866, *Bull. crim.*, n° 233 ; *D.* 2011, p. 2935, obs. M. LENA ; *D.* 2012, p. 137, note G. BEAUSSONIE ; *AJ pénal* 2012, p. 163, obs. J. LASSERRE-CAPDEVILLE ; *Dr. pénal* 2012, comm. 1, obs. M. VERON ; *JCP G* 2012, 322, note S. DETRAZ ; *Gaz. Pal.* 2012, 1, p. 300, note E. DREYER ; *RSC* 2012, p. 139, obs. J. FRANCILLON.

87. Le vol de la chose incorporelle. S'agissant d'abord de l'objet du vol, la Cour de cassation a admis à plusieurs reprises la possibilité de qualifier de vol la soustraction de l'information indépendamment de son support sous l'expression désormais consacrée de « *contenu informationnel* »[466]. Il demeurait que, dans de nombreuses affaires, le support physique de l'information était manié ou déplacé[467]. L'évolution des dispositifs informatiques permet désormais d'accéder à distance à un système d'informations, de prendre connaissance des informations qui y figurent et d'en faire une copie numérique directement sur son propre espace de stockage. Dans une telle hypothèse, il n'y a aucune mainmise sur le support. C'est pourtant le raisonnement validé par la Cour de cassation dans un arrêt du 20 mai 2015[468], à l'occasion duquel elle admet que le fait d'extraire des données du système d'information extranet de l'Agence nationale de sécurité sanitaire et de l'alimentation constitue un vol. Le vol avait également été retenu à l'occasion d'une affaire dans laquelle un avocat avait accédé puis téléchargé les courriers de l'un de ses associés[469]. L'on pourrait dès lors affirmer qu'une qualification similaire trouverait à s'appliquer dans le cas d'une usurpation d'informations relatives au patient et couvertes par le secret. Néanmoins, comme l'ont remarqué certains

---

[466] V. notamment: Crim., 12 janv. 1989, n° 87-82265, *Bull. crim*. n° 14; *RSC* 1990. 346, obs. P. BOUZAT; *ibid.* 507, obs. M.-P. LUCAS DE LEYSSAC; *RTD com.* 1990. 143, obs. P. BOUZAT; Crim. 1er mars 1989, n° 88-82.815, *Bull. crim.* n° 100; *D.* 1990. 330, obs. J. HUET; *RSC* 1990. 346, obs. P. BOUZAT; *ibid.* 507, obs. M.-P. LUCAS DE LEYSSAC; *RTD com.* 1990. 142, obs. P. BOUZAT; Crim. 4 mars 2008, n° 07-84.002, *D.* 2008, p. 2213, comm. S. DETRAZ, « Vol du contenu informationnel de fichiers informatiques »; *Rev. pénit.*2008, p. 880, obs. V. MALABAT; *Rev. sc. crim.* 2009, p. 131, obs. J. FRANCILLON.

[467] Par exemple : Crim. 3 avr. 1995, n° 93-81.569, *Bull. crim*. n° 142 ; *D.* 1995, p. 320, obs. J. PRADEL ; *RSC* 1995, p. 599, obs. J. FRANCILLON, p. 821, obs. R. OTTENHOF, 1996, p. 645, obs. B. BOULOC, et p. 660, obs. R. OTTENHOF ; Crim. 19 juin 2001, n° 99-85.188, *Bull. crim.* n° 149 ; *D*. 2001, p. 2538, note B. BEIGNIER et B. DE LAMY, et 2002 (somm.), p. 1463, obs. J. PRADEL ; *GAPP*, 7e éd., 2011, n° 30 ; *RSC* 2002, p. 96, obs. B. BOULOC, p.119, obs. J. FRANCILLON, et p. 592, obs. J.-P. DELMAS SAINT-HILAIRE ; *RTD com.* 2002, p.178, obs. B. BOULOC ; JCP 2002, II, p. 10064, concl. D. COMMARET, note A. LEPAGE ; Crim. 12 juin 2007, n° 06-87.361, *Bull. crim.* n° 157 ; *JCP G*, 2007, II, p. 10159, note F. FOURMENT, C. MICHALSKI et P. PIOT ; *Dr. pénal*, 2007, comm. 143, obs. M. VERON ; *D.* 2009. 123, obs. T. GARE ; *AJ pénal* 2007, p. 439, obs. G. ROYER ; *RSC* 2008, p. 95, obs. J. FRANCILLON ; *RTD com.* 2008, p. 197, obs. B. BOULOC.

[468] Crim., 20 mai 2015, n° 14-81336, *Bull. crim.*, n° 119 ; *D.* 2015, p. 1466, note L. SAENKO ; *ibid.* p. 2465, obs. G. ROUJOU DE BOUBEE, T. GARE, C. GINEST, M.-H. GOZZI et S. MIRABAIL ; *AJ pénal* 2015, p. 413, note E. DREYER ; *JCP G* 2015, 887, note G. BEAUSSONIE ; *Dr. pén.* 2015, comm. 107, note M. VERON ; *ibid.* comm. 123, note P. CONTE ; *ibid.* chron. 10, obs. A. LEPAGE ; *Gaz. Pal*. 18 juin 2015, p. 8, note S. DETRAZ ; *RSC* 2015, p. 860, obs. H. MATSOPOULOU ; *ibid.* p. 887, obs. J. FRANCILLON ; *RTD com.* 2015, p. 600, obs. B. BOULOC ; *RTD eur.* 2016, p. 374, obs. E. MATRINGE ; *RDC* 2015, p. 951, note P. BERLIOZ ; *LPA*, 29 juill. 2015, n° 150, p. 15, obs. E. CHAUVIN ; *PI* janv. 2016, p. 97, obs. M. VIVANT.

[469] Crim., 28 juin 2017, n° 16-81113, publié au Bulletin ; *D.* 2017, p. 1885, note G. BEAUSSONIE ; *AJ pénal* 2017, p. 448, obs. J. LASSERRE-CAPDEVILLE ; *RSC* 2017, p. 752, obs. H. MATSOPOULOU ; *RTD com*. 2017, p. 713, obs. L. SAENKO.

auteurs, cette décision n'a pas posé clairement de solution[470] mais, surtout, le législateur est intervenu pour modifier et élargir le champ d'application de l'article 323-3 du Code pénal[471]. Sanctionnant le fait de s'introduire, de se maintenir, de supprimer ou modifier frauduleusement des données dans un système de traitement automatisé de données, le texte d'incrimination sanctionne désormais le fait d'extraire, de détenir, de reproduire ou de transmettre des données à l'insu du responsable du traitement de données. Ainsi, de tels faits trouvent désormais un fondement répressif correspondant et ne devraient plus, selon certains auteurs, être sanctionnés sur le fondement de l'article 311-1 du Code pénal[472]. Il demeure que l'infraction prévue à l'article 323-3 du Code pénal sanctionne également les atteintes à la propriété et semble donc admettre une forme de « *vol de données* »[473]. La controverse relative au vol d'information devrait pouvoir trouver une issue si l'on admet que la qualification idoine se trouve être l'incrimination définie à l'article 323-3 du Code pénal. Si l'argument téléologique en faveur d'une telle hypothèse est considéré par Monsieur Beaussonie comme un argument sérieux[474], la question de savoir si la sanction de l'appropriation frauduleuse d'informations personnelles, couvertes par le secret, peut s'opérer par le truchement de cette incrimination et participer de la protection du secret des informations relatives au malade, se pose.

b - La sanction de la prise de connaissance et de l'extraction de données

88. L'infraction relative à l'atteinte portée au STAD est née de la nécessité de protéger les systèmes d'informations conçues comme des biens. Aussi, la protection du secret des informations relatives à la santé, que celles-ci soient ou non détenues par un professionnel soumis au secret si elle peut être admise **(i)** est également incidente **(ii)**.

---

[470] J. LASSERRE CAPDEVILLE, « Les développements récents du droit sanctionnant le vol », *AJ pénal* 2017, p. 208 ; E. DREYER, « Consécration – provisoire – du vol de données informatiques », *AJ pénal* 2015, p. 413.
[471] Loi n° 2014-1353 du 13 novembre 2014 (*JORF* n° 0263).
[472] En ce sens : M.-L. RASSAT, *Droit pénal spécial*, coll. Précis, Dalloz, 8ème éd., 2018, n° 107.
[473] E. DREYER, « Consécration – provisoire – du vol de données informatiques », *op. cit.*
[474] G. BEAUSSONIE, « A propos d'une controverse contemporaine et persistante : le vol d'informations », *Revue de droit d'Assas*, déc. 2018, n° 17, p. 104.

i - Les atteintes aux systèmes automatisés de traitement de données

89. A propos du glissement sémantique, de l'information aux données. A ce stade de notre démonstration, il faut noter que la transformation des supports de l'écrit s'est accompagnée d'un changement de vocabulaire. Le terme de *données* est utilisé, dès 1988, dans la loi Godfrain[475], tandis que la loi informatique et libertés traite des « *informations nominatives* »[476], devenues ensuite « *données à caractère personnel* »[477]. Le glissement sémantique est consécutif de l'utilisation des dispositifs informatiques de l'information et de la communication. Le traitement[478], dans le vocabulaire informatique, s'entend en effet comme « *Traitement (automatique) des données* ; *plus usuel traitement de l'information* » ou « *Ensemble des opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction, l'édition de données et d'une façon générale leur exploitation* »[479]. D'abord, le traitement automatisé des informations impose de différencier la donnée – au singulier –, des données – au pluriel –, une donnée étant « *la représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement* »[480]. Cette définition rejoint celle proposée par Madame de Lamberterie : « *la transformation que cette dernière* [l'information] *subit pour être utilisée en vue d'un traitement informatique* […]*, la donnée possède donc une valeur ajoutée d'ordre technologique* »[481]. Cette dernière définition doit toutefois être relativisée dans la mesure où

---

[475] Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique.
[476] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (*JORF*, 7 janv. 1978).
[477] C'est à l'occasion de la transposition d'une directive européenne (Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (*JOUE* L 281, 23 nov. 1995)) qu'intervient le changement sémantique (Loi nº 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (*JORF*, 7 août 2004)). L'utilisation de l'expression *informations nominatives* dans la loi informatique et libertés tient sans doute au fait que celle-ci ne s'applique pas uniquement aux traitements automatisés, le terme était donc plus générique que celui de *données* qui ne désigne que les informations traitées automatiquement, c'est-à-dire à l'aide d'un ordinateur.
[478] Le terme de traitement est ici entendu dans un sens large, qui est celui des sciences de l'information et de la communication. Nous envisagerons ultérieurement le sens qui lui est donné en droit de la protection des données à caractère personnel.
[479] TLFi*, V°* « Traitement ».
[480] Arrêté du 22 décembre 1981 relatif à l'enrichissement du vocabulaire de l'informatique (*JONC,* 17 janv. 1982, p. 624).
[481] I. DE LAMBERTERIE, « Qu'est-ce qu'une donnée de santé? », *RGDM* 2004, numéro spécial *Le droit des données de santé*, LEH, pp. 11-34, spéc. p.13 – *Adde* C. ZORN, *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, coll. « Santé, qualité de vie et handicap », PUN, 2010, n° 6.

l'information qui subit un traitement automatisé constitue un ensemble de données et non pas une seule donnée. Chaque donnée peut ensuite faire l'objet d'un traitement particulier et constituer, mise en lien avec d'autres données, une nouvelle information. Le terme de *données* (*data* en anglais) désigne donc toutes les informations traitées informatiquement et dont le support est également informatique. Ce glissement sémantique, d'ordre purement technique dans un premier temps, explique que l'on trouve dans la doctrine, dans la jurisprudence et parfois dans les textes de loi, l'expression « *données couvertes par le secret* »[482] pour qualifier les informations couvertes par le secret – *secret-fait* –, tout en marquant le passage d'un support à un autre. Quant à la *valeur ajoutée*, d'ordre technologique, elle a pu participer à raviver le débat sur la valeur de l'information, à présent déplacé vers la propriété des données. Un auteur souligne à ce titre que « *Le glissement sémantique de l'«* information *» à la «* donnée *» n'est pas neutre car la donnée est une information valorisée. Elle est dotée d'une valeur ajoutée technologique qui procède d'un formatage numérique de nature à permettre son exploitation, de sorte que la patrimonialisation progresse plus vite à travers la notion de données. Sans doute progressera-t-elle plus vite encore à travers celle de* Data*, qui évoque les données massives qui, sous le poids du nombre, apparaissent comme une ressource à valoriser, indépendamment de leur ancrage avec les personnes* »[483]. Au regard de ces développements, et puisqu'aucun régime spécifique ne se déduit du choix du vocabulaire, nous prendrons pour synonymes informations et données pour ce qui concerne la fraude informatique telle qu'elle est sanctionnée par l'incrimination prévue à l'article 323-3 du Code pénal.

90. Présentation générale de l'infraction. C'est par une loi du 5 janvier 1988 relative à la fraude informatique[484] que le législateur a, pour la première fois, réprimé des agissements

---

[482] L'emploi de l'expression est d'ailleurs souvent fort peu à propos car sans lien avec un traitement informatisé, par exemple : Code du travail, art. L. 4451-3, à propos des personnes désignées en matière de radioprotection des travaillleurs qui sont soumises au secret, selon les termes de l'article « *au titre des données couvertes par le secret qui lui ont été communiquées par le médecin du travail* ». Du reste, l'emploi de l'expression vise en général des informations traitées informatiquement. Pour ne donner que quelques exemples : CSP, art. R. 1341-7, qui vise les « *données couvertes par le secret médical* » ; C. ROQUET, « Le secret médical à l'épreuve du contentieux social des relations collectives, *RDSS* 2018, p. 658 ; A. DENIZOT, « Droit de la santé : les avalanches de l'hiver 2017 », *RTD civ.* 2017, p. 500 ; Civ. 2ème, 28 nov. 2013, n° 12-27209.

[483] F. LESAULNIER, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p. 573.

[484] Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique (*JORF*, 6 janv. 1988, p. 231).

perpétrés par le moyen de l'outil informatique et ayant pour objet les biens informatiques[485]. Cette loi préfigure ce que l'on nomme aujourd'hui la *cybercriminalité*[486]. Or, ces incriminations ont très rapidement montré leurs limites, comme en témoigne la jurisprudence en matière d'abus de confiance et de vol dont le juge pénal s'est employé à élargir le champ d'application afin de prendre en compte l'émergence de cette nouvelle forme de criminalité. Les infractions, d'abord définies par la loi du 5 janvier 1988[487], ont ensuite été modifiées afin d'augmenter le *quantum* des peines et d'ajouter une incrimination réprimant le trafic de moyens destinés à

---

[485] Les dispositions pénales de la loi informatique et libertés (Loi n° 78-17 du 6 janvier 1978) ne peuvent servir de fondement pour réprimer de tels comportements puisque leur champ d'application est restreint aux atteintes aux droits de la personne résultant de fichiers ou de traitements informatiques, c'est-à-dire au non-respect des conditions autorisant le traitement des données à caractère personnel (F. CHOPIN, *Rép. pén.*, *V°* « Cybercriminalité », juill. 2013 (mise à jour avr. 2018), n° 3). C'est cette inadaptation qui avait conduit le législateur à incriminer spécifiquement certains agissements : R. GASSIN, « Le droit pénal de l'informatique », *D.* 1986. chron. p. 35 ; W. JEANDIDIER, *Droit pénal des affaires*, 6ème éd., coll. Précis, Dalloz, 2005, n° 398 et svt. ; J. PRADEL et M. DANTI-JUAN, *Droit pénal spécial*, 7ème éd., coll. Référence, Cujas, 2017, n° 1015 ; M. VERON, *Droit pénal spécial*, 17ème éd., coll. Université, Sirey, 2019, n° 617 et svt ; J. DEVEZE, *Jcl. Pénal Code*, Art. 323-1 à 323-7, Fasc. 20 : « Atteinte aux systèmes de traitement automatisé de données », févr. 2010 (mise à jour juin 2018), n° 3 et svt. Aussi, les concours de qualifications qui sembleraient apparaître entre les infractions évoquées et celles de la loi informatique et libertés ne sont qu'apparents (v. O. DE MAISON ROUGE, « La donnée, enjeu cardinal de la cybersécurité », *Dalloz IP/IT* 2018. 170) V. *infra* Section I Chapitre II Titre II Partie I.

[486] La cybercriminalité « *est constituée par les délinquants qui utilisent les systèmes et les réseaux informatiques, soit pour commettre des infractions spécifiques à ces systèmes et réseaux informatiques, soit pour développer ou faciliter des infractions qui existaient avant l'arrivée d'internet* » (F. CHOPIN, « Cybercriminalité », *op. cit.,* n° 7). Elle est définie en fonction de son domaine par la Commission européenne et regroupe trois catégories d'activités : les infractions visant les systèmes d'information et les systèmes de traitement automatisé de données (STAD) ; les formes traditionnelles de criminalité, telles que la fraude en ligne, les escroqueries ; les infractions dites de contenu comme la pédophilie *via* internet, le racisme et la xénophobie (Communication de la Commission au Parlement européen, au Conseil et au Comité des régions intitulée «Vers une politique générale en matière de lutte contre la cybercriminalité », COM (2007) 267 final du 22 mai 2007). L'organisation pour la coopération et le développement économique (OCDE) considère qu'il s'agit de « *tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique de données et, ou de transmissions de données* ». L'ONU en donne également une définition : « *tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent* » (M. QUEMENER et Y. CHARPENEL, *Cybercriminalité. Droit pénal appliqué*, coll. Pratique du droit, Economica, 2010). Ces deux dernières définitions sont toutefois trop larges pour être opérantes (F. CHOPIN, « Cybercriminalité », *op. cit.*). Sans doute peut-on préférer la définition suivante, qui différencie cybercriminalité et cyberdélinquance : « *La cyberdélinquance correspond à l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunications en général et plus particulièrement sur internet. La cybercriminalité est une notion polymorphe qui peut concerner les infractions classiques commises par le biais des technologies numériques, comme de nouvelles infractions, nées de l'essence même de l'informatique. Les technologies numériques permettent la réalisation d'activités délinquantes et notamment Internet apparaît comme un vecteur privilégié pour le passage à l'acte des délinquants. On parle aussi de délinquance, d'infractions commises dans l'environnement numérique* » (M. QUEMENER et Y. CHARPENEL, *Cybercriminalité. Droit pénal appliqué*, *op. cit.*, n° 32).

[487] Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique.

commettre ces infractions[488]. Codifiées aux articles 323-1 à 323-7 du Code pénal, ces infractions punissent exclusivement les atteintes portées aux systèmes de traitement automatisé de données (STAD), nouvelle universalité de fait[489]. Partant, la frontière entre atteintes aux droits des personnes sanctionnées par la loi informatique et libertés et atteintes aux biens – les ordinateurs et leurs périphériques, les réseaux et logiciels – semblait conserver une certaine étanchéité. Le délit prévu à l'article 323-1 sanctionne l'introduction et le maintien dans un STAD, donc le fait de prendre connaissance des données y figure. Quant à l'article 323-3 du Code pénal tel que modifié par loi du 13 novembre 2014[490], il sanctionne désormais l'extraction, la détention et la transmission de données, ces comportements correspondant à une usurpation dans la mesure où il s'agit de s'approprier des données réservées[491]. Il convient toutefois d'analyser les éléments des textes d'incrimination afin de savoir si elles permettent, même subsidiairement, d'assurer le secret des informations relatives au malade.

---

[488] Qualifiées d' « *armes numériques* » par un auteur : D. BENICHOU, « Cybercriminalité : Jouer d'un nouvel espace sans frontière » *AJ pénal* 2005, p. 224 ; *Adde* C. ROBACZEWSKI, *Jcl. Pénal Code*, Art. 323-1 à 323-7, Fasc. 20 : « Atteinte aux systèmes de traitement automatisé de données ».

[489] « […] *protéger* le système en lui-même *ne soulève pas de difficulté majeure relative au droit de propriété, à la condition d'accéder à l'idée que le système et une totalité qui se présente comme une nouvelle « universalité de fait » en droit français. Ses éléments essentiels, qui sont les moyens du traitement des informations, sont déjà des biens en droit positif : l'ordinateur et ses périphériques comme biens matériels susceptibles, comme tous les autres meubles corporels, de propriété ; les logiciels comme œuvres de l'esprit protégées par le droit d'auteur depuis la loi du 3 juill. 1985. Il suffit de considérer le regroupement de ces divers éléments comme un ensemble, le système de traitement automatisé de données, lui-même susceptibles de faire l'objet d'une appropriation comme «* universalité de fait *», à l'exemple du fonds de commerce* » (R. GASSIN, « La protection pénale d'une nouvelle « universalité de fait » en droit français : les systèmes de traitement automatisé de données (Commentaire de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique) », *ALD* 1989, 2ème cahier, p. 5). L'universalité de fait, par opposition à l'universalité de droit (ensemble de biens et de dettes qui forme un tout comme par ex. le patrimoine) est « *un ensemble de biens formant* (…) *une entité complexe prise globalement comme un bien unique (...) et soumis à un régime juridique particulier* » *(V°* « Universalité », *in* G. CORNU (ss. la dir.), *Vocabulaire juridique*, 9ème éd., Quadrige-PUF, 2011. Pour une étude de la notion, v. A. DENIZOT, *L'universalité de fait*, préf. R. LIBCHABER, coll. Thèses, Fondation Varenne-LGDJ, 2008.

[490] Loi n° 2014-1353 du 13 novembre 2014 (*JORF* n° 0263, 14 nov. 2014, p. 19162).

[491] Etendre la définition du STAD aux données qu'il contient revient à affirmer une protection tant du contenu que du contenant, constat qui s'impose en raison de l'indépendance du support par rapport aux données. L'argument selon lequel il s'agirait de protéger le fonctionnement du système au travers des données qu'il contient est un argument à prendre en compte de notre point de vue (Monsieur Dreyer considère que *« ce qui est en cause ce n'est pas tant le contenu que le contenant et, plus particulièrement, ce qui le fait fonctionner* » (E. DREYER, *Droit pénal spécial*, 3ème éd., coll. Cours magistral, Ellipses, 2016, n° 858 ; dans le même sens, v. G. BEAUSSONIE, « A propos d'une controverse contemporaine et persistante : le vol d'informations », *op. cit.*, p. 104, affirmant que « *les données généralement prises en comptes sont celles qui permettent le fonctionnement des systèmes, pas celles que les systèmes renferment indépendamment de cela* »).

ii - Une protection subsidiaire du secret des informations

91. La condition commune à toutes les infractions sanctionnant une atteinte aux STAD. L'existence d'un système automatisé de données est une condition préalable commune à l'ensemble des infractions prévues au chapitre des atteintes aux systèmes de traitement automatisé de données[492]. La notion n'a pas été définie par le législateur au moment de la rédaction de la loi du 5 janvier 1988. Lors des travaux préparatoires, la proposition formulée par le Sénat était la suivante : « *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs déterminés* »[493]. Cette définition, bien qu'ayant finalement été écartée, devait guider le juge pénal dans son office d'interprétation[494]. De cette définition, deux éléments ressortent : *« d'une part, il s'agissait d'un ensemble composé d'éléments de nature diverse (unités de traitement, mémoires, logiciels, données, organes d'entrées et sorties, liaisons) dont les relations entre eux pouvaient résulter de la recherche d'un résultat déterminé (le traitement de données) ; d'autre part, il s'agissait d'un ensemble protégé par des dispositifs de sécurité* »[495]. Cette définition n'étant qu'une indication pour les juges[496], la jurisprudence est parfois plus souple et n'exige pas toujours une relation entre des éléments divers[497], ce qui constitue pourtant l'essence d'un *système*[498]. L'absence de définition des STAD dans le texte d'incrimination des infractions sanctionnant les atteintes qui y sont portées permet de couvrir un large champ d'application.

92. STAD et traitement de données couvertes par le secret. L'atteinte à un STAD pourrait ainsi être caractérisée dès lors qu'elle concerne une messagerie sécurisée de santé, un logiciel de gestion de patient, et ce quel que soit le mode d'exercice du ou des professionnels soumis au secret qui traitent les données. Par ailleurs, dès lors que les bases de données sont

---

[492] C. ROBACZEWSKI, « Atteinte aux systèmes de traitement automatisé de données », *op. cit.*, n° 5.
[493] *Doc. AN* n° 1009, 1987-1988.
[494] En ce sens v. J. PRADEL et M. DANTI-JUAN, *Droit pénal spécial*, 7ème éd., coll. Référence, Cujas, 2017, n° 1016.
[495] C. ROBACZEWSKI, « Atteinte aux systèmes de traitement automatisé de données », *op. cit.*, n° 6.
[496] H. CROZE, « L'apport du droit pénal à la théorie générale du droit de l'informatique (à propos de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique) », *JCP G* 1988, I, 3333, spéc. n° 7.
[497] C. ROBACZEWSKI, « Atteinte aux systèmes de traitement automatisé de données », *op. cit.*, n° 11.
[498] Toutes les définitions du terme, peu importe le domaine, désignent le système comme ce qui se compose d'éléments matériels ou immatériels (de la pensée) formant un ensemble ou concourant à un but, une fonction commune (TLFi, *V°* « Système »).

une part d'un système de traitement de données[499], les infractions sanctionnant l'atteinte au STAD pourraient concerner la Plateforme des données de santé[500]. Il est inutile et fastidieux de tenter de dresser une liste de tous les éléments qui composent ou peuvent composer un système de traitement automatisé de données puisque l'absence de définition constitue une garantie d'adaptabilité des infractions aux évolutions technologiques[501]. Un obstacle semble toutefois s'ériger quant à une telle interprétation. De prime abord, pour le seul fait d'extraire des données couvertes par le secret, qui sont également des données à caractère personnel ou des données de santé au sens des dispositions relatives à la protection des données à caractère personnel, deux qualifications seraient en concours. Pourraient trouver à s'appliquer l'infraction prévue à l'article 323-3 du Code pénal et celle sanctionnant la collecte déloyale de données telle que punie par l'article 226-16 du Code pénal[502].

93. Cumul de qualifications et concours d'infractions. Si tout traitement automatisé de données à caractère personnel et de données de santé , tel que prévu par les dispositions relatives à la protection des données à caractère personnel, suppose l'existence d'un STAD, le volet pénal de la loi informatique et libertés – dont les infractions figurent dans le Code pénal au sein d'un chapitre portant sur les atteintes aux droits de la personne[503] – permet de sanctionner spécifiquement l'extraction de données couvertes par le secret. Ces dernières sont effectivement des données personnelles ou des données de santé[504] au sens de ces dispositions spécifiques.

---

[499] « *Cette notion ne doit pas être confondue avec celle de « traitement automatisé de données » qui désigne l'activité accomplie au moyen d'un système, mais non le système lui-même qui permet d'y procéder* » (F. CHOPIN, « Cybercriminalité », *op. cit.*, n° 12. Toutefois, la Cour de cassation, pour qualifier l'infraction prévue à l'article 323-1 du Code pénal, sanctionnant l'accès et le maintien frauduleux dans un STAD, juge qu'« *est frauduleuse l'utilisation pendant plus de deux ans d'un code permettant l'accès à une base de données accessibles aux seules personnes autorisées, alors que ce code a été remis à un salarié pour sa période d'essai* » (Crim., 3 oct. 2007, n° 07-81045, *AJ pénal* 2007, p. 535).

[500] Créée par la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé.

[501] A propos de la proposition de définition faites par le Sénat un auteur remarque : « *Il convient cependant de préciser deux points : tout d'abord, l'énumération des éléments de l'ensemble ne doit pas être considérée comme exhaustive afin de s'adapter à l'évolution du progrès technique. En outre, les éléments qui composent un système de traitement automatisé de données sont de nature différente (par ex. : ordinateur, support de logiciels, informations codées sous forme de données, etc.)* » (F. CHOPIN, « Cybercriminalité », *op. cit.*, n° 11).

[502] CP, art. 226-16.

[503] CP, art. 226-16 à 226-24, Section V « Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques », Chap. IV « Des atteintes à la personnalité », Titre II « Des atteintes à la personne humaine », Livre II « Des crimes et délits contre les personnes », Partie législative.

[504] V. *infra* n° 146 et svt.

Ainsi, le fait d'extraire d'un système de traitement automatisé des données couvertes par le secret, sans autorisation pour le faire, constitue l'infraction prévue à l'article 226-18 du Code pénal qui sanctionne « *Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite* »[505]. La collecte, au sens des dispositions relatives à la protection des données à caractère personnel, correspond à un traitement de données. En effet, « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* »[506]. Il apparaît donc que l'extraction de données couvertes par le secret, dans la mesure où les informations qui en sont l'origine ont été préalablement recueillies par une personne soumise au secret, correspond à un traitement frauduleux de données. Tandis que l'alinéa 1er du texte d'incrimination de l'article 323-3 du Code pénal, modifié par la loi du 13 novembre 2014[507], punit « *Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient* »[508]. Les deux qualifications pourraient donc s'appliquer à un même fait. Apparaît alors un cumul de qualifications dès lors que les faits ne sont pas divisibles et que les qualifications ne portent pas atteinte aux mêmes intérêts protégés[509]. En effet, l'infraction prévue à l'article 226-18 du Code pénal participe à la protection de la personnalité, tandis que l'infraction prévue à l'article 323-3 du même code sanctionne une atteinte aux biens et protège les données comme éléments de l'universalité de fait qu'est le système de traitement automatisé de données. Le juge pénal utilise les ressources de manière complémentaire et retient les deux qualifications[510] ;

---

[505] CP, art. 226-18.
[506] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE), art. 4.
[507] Loi n° 2014-1353 du 13 novembre 2014.
[508] CP, art. 323-3.
[509] E. DREYER, *Droit pénal général*, 5ème éd., LexisNexis, 2019, n° 644 et svt.
[510] C'est la solution traditionnelle lorsqu'une seule activité matérielle tombe sous le coup de plusieurs qualifications et porte atteinte à des valeurs sociales protégées différentes (Crim., 3 mars 1960, *Bull. crim.*, n° 138 ; *RSC* 1961, p. 105, obs. P. LEGAL ; comm. *in* J. PRADEL et A. VARINARD, *Les grands arrêts du droit pénal général*, coll. Grands arrêts, Dalloz, 2016, n° 19 ; Crim., 8 nov. 1977, *Bull. crim.*, n° 339 ; Crim., 21 sept. 1999,

« *ces deux catégorie d'incriminations permettent le cas échéant d'assurer, en cas de fraude informatique, la protection de l'être et de l'avoir* »[511]. Serait ainsi confirmé le raisonnement de Monsieur Beaussonie selon lequel l'infraction inscrite à l'article 323-3 n'a pas été créée pour protéger le contenu des STAD[512]. Le même constat ne s'impose pas s'agissant du second alinéa du texte d'incrimination de l'article 323-3 du Code pénal.

94. L'extraction de données des STAD à caractère personnel mis en œuvre par l'Etat. Le second alinéa de l'article 323-3 prévoit une circonstance aggravante lorsque l'introduction, l'extraction, la détention, la reproduction, la transmission, la suppression ou la modification frauduleuse des données est commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat[513]. La peine est alors portée à sept ans d'emprisonnement et à 300 000 € d'amende. Cette circonstance aggravante est également commune aux infractions sanctionnant l'introduction ou le maintien frauduleux dans un STAD[514] et le fait d'entraver ou de fausser le fonctionnement d'un STAD[515]. Elle a été ajoutée aux textes d'incrimination à l'occasion de la loi du 27 mars 2012 relative à la protection de l'identité[516]. Cette loi devait, à l'origine, créer un fichier national des documents d'identité. La disposition, ainsi que de nombreuses autres ont finalement été invalidées par le Conseil constitutionnel[517]. Les circonstances aggravantes ici présentées devaient permettre d'accroître

---

n° 97-85551, *Bull. crim*. n° 191 ; *D.* 2000, somm. p. 383, obs. M.-C. AMAUGER-LATTES ; *RSC* 2000, p. 200, obs. Y. MAYAUD). On trouve une illustration dans un domaine qui n'est pas celui de la santé : dans cette affaire jugée par la Cour d'appel de Paris (Paris, 15 sept. 2017, pôle 4, ch. 11 disponible sur <www.legalis.net>), un individu a extrait les données personnelles des clients d'une billetterie en ligne, à partir de la base de données du site de vente en ligne afin d'alimenter sa propre billetterie en ligne et de mieux la concurrencer : 8000 fichiers clients provenant du site avaient été dérobés. Mais une telle solution s'appliquerait sans doute de la même manière dans l'hypothèse où un individu s'introduirait dans un STAD (par exemple l'ordinateur et le logiciel de gestion des patients d'un professionnel de santé).

[511] A. LEPAGE, « Un an de droit pénal du numérique (Octobre 2016- Septembre 2017) », *Dr. pén.* 2017, chron.11.

[512] G. BEAUSSONIE, « A propos d'une controverse contemporaine et persistante : le vol d'informations », *Revue de droit d'Assas*, déc. 2018, n° 17, p. 104.

[513] CP, art. 323-3, al. 2.

[514] CP, art. 323-1.

[515] CP, art. 323-2.

[516] Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité (*JORF* n° 0075, 28 mars 2012, p. 5604).

[517] Sur les vicissitudes de l'élaboration de cette loi et les difficultés de respecter l'équilibre constitutionnel en matière de fichage public v. Cons. const., déc. 22 mars 2012, n° 2012-652 DC ; *RLDI* juin 2012, obs. L. COSTES ; *AJDA* 2012, p. 623, note R. GRAND. ; *Dr. famille* 2012, alerte 29, obs. M. BRUGGEMAN. Pour une analyse de loi, v. V. TCHEN, « L'informatisation des documents d'identité numérisés », *Dr. adm*. 2012, comm. 48 ;. F. MATTATIA, « La loi sur la protection de l'identité est-elle conforme à la Constitution ? », *LPA* 24 avr. 2012, n° 82, p. 6. ; C. GUERRIER, « La CNI biométrique française : entre préservation de l'identité et protection des

la protection des personnes fichées en renforçant la répression pénale du piratage des fichiers mis en œuvre par l'État. Si, dans le contexte de la loi, ces aggravations des sanctions pénales visaient particulièrement certains fichiers très sensibles[518], elles s'appliquent à tous les traitements de données à caractère personnel mis en œuvre par l'Etat et concernent donc également ceux comprenant des données de santé et des données à caractère personnel issues de la prise en charge des patients et donc couvertes par le secret. Toutefois, il ne s'agit en aucun cas de sanctionner une atteinte aux biens mais de punir les atteintes à la personnalité. Qu'une telle aggravation trouve sa place au sein d'incriminations protégeant les biens ne pose aucune difficulté. Il s'agit en effet de délits, comme il en existe quantité au sein de notre droit criminel et qu'André VITU qualifiait de « *délit pluri-offensant* »[519], désignant une incrimination qui vise à réprimer l'atteinte portée à plusieurs valeurs sociales pénalement protégées[520]. La fonction expressive[521] du droit pénal montre ici ses limites. Le législateur raisonne, en réalité, davantage sur les moyens employés que sur les valeurs, ce qui illustre, sur ce point au moins, les critiques formulées à l'égard d'une conception normative du droit au regard de la variabilité des intérêts protégés[522]. Les circonstances aggravantes sont une illustration évidente de cette variabilité, le vol qui sanctionne une atteinte aux biens est aggravé par la circonstance de violences commises à l'encontre de la victime et constituent une atteinte à l'intégrité physique[523]. Une dernière

---

libertés individuelles » ; *RLDI* 2012, n° 82 ; D. BOTTHEGI et A. LALLET, « Les vicissitudes du fichage », *AJDA* 2010, p. 1930.

[518] « *Cette aggravation paraît pleinement justifiée par la gravité des faits : Entraver ou fausser volontairement un fichier géré par l'État, comme par exemple le casier judiciaire, le fichier des empreintes génétiques, ou la nouvelle base centrale de délivrance de titres d'identité et de voyage, peut en effet avoir des conséquences extrêmement graves sur les libertés individuelles ou la lutte contre la criminalité* » (P. GOUJON, Rapport n° 3599 du 29 juin 2011 fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur la proposition de loi (n° 3471), adoptée par le sénat, relative à la protection de l'identité, p. 34).

[519] A. VITU, « De l'illicéité en droit criminel français », rapport présenté à l'occasion des 2èmes journées franco-helléniques de droit comparé à Nancy, *Bull. de la société de législation comparé* 1984, p. 127 et svt. ; *Droit pénal spécial,* Cujas, 1981, p. 30, n° 22.

[520] La question des valeurs sociales pénalement protégées est aux fondements du droit pénal et donne lieu à de nombreuses controverses fondamentales en matière pénale. V. par exemple le rejet de l'expression par Monsieur Dreyer, l'auteur lui préférant celle « *d'intérêts protégés par le droit pénal* » puisqu'il dénie toute filiation entre morale et droit pénal (E. DREYER, *Droit pénal général*, 5ème éd., LexisNexis, 2019, n° 160 et svt). L'intérêt pour le concept, ses enjeux et l'évolution de ces valeurs ne faiblit pas puisqu'elles témoignent de l'évolution conjointe de la société et du droit pénal. V. P. MISTRETTA, C. KUREK et S. PAPILLON (ss. la dir.), *L'empreinte des valeurs sociales protégées en droit pénal*, colloque organisé le 6 juin 2019, Université Jean Moulin Lyon III, actes à paraître.

[521]« […] *la lecture des incriminations permet de reconstituer les valeurs sociales éminentes, celles qui importent le plus pour la société ; c'est la fonction expressive du droit pénal* » (G. BEAUSSONIE, *Rep. pén., V°* « Infraction », mai 2018, n° 45).

[522] E. DREYER, *Droit pénal général*, *op. cit.*, n° 160 et svt.

[523] CP, art. 311-1 et 311-4.

hypothèse reste à envisager, il s'agit de l'incrimination qui vise le fait de s'introduire où de se maintenir dans un STAD.

95. L'incrimination de l'accès ou du maintien frauduleux dans un STAD, vie privée et propriété. L'infraction prévue à l'article 323-1 du Code pénal incrimine « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* ». Il s'agit d'une infraction matérielle, aussi l'accès comme le maintien sont-ils sanctionnés sans qu'un résultat ne soit exigé. L'élément matériel est double et suppose soit l'accès, soit le maintien frauduleux dans un STAD. Le législateur sanctionne ici une forme d'« *espionnage informatique* »[524]. Monsieur Dreyer fait un parallèle entre celle-ci et l'incrimination de la violation de domicile prévue à l'article 226-4 du Code pénal[525]. Cette comparaison est intéressante en ce qu'elle démontre encore la porosité de la frontière entre l'être et l'avoir. Le fait de s'introduire frauduleusement dans un STAD n'entraîne pas systématiquement une perturbation du système. Il s'agit simplement de sanctionner une introduction et un maintien « *sans droit* »[526] dans le système. Par ailleurs, le parallèle entre l'incrimination de la violation de domicile et celle de l'introduction ou du maintien frauduleux dans un STAD permet de pousser encore la réflexion sur ce que le législateur a entendu protéger. Madame Matsopoulou souligne ainsi, à propos de la violation de domicile : « *Si le principe même de la protection du domicile ne peut être mis en cause, encore faut-il savoir ce que recherche le législateur en édictant des sanctions pénales. S'agit-il de protéger le domicile pour lui-même ou bien d'assurer une sphère de tranquillité pour l'individu ? Ce serait certainement la première conception que consacrerait le droit, si la protection concernait l'intégrité du local à la manière de ce qui est admis en matière de destruction ou de dégradation de biens. Mais, outre que l'incrimination n'est pas insérée dans le livre III visant la protection des biens, la loi – ancienne ou nouvelle – punit la simple violation ou profanation du local, peu*

---

[524] E. DREYER, *Droit pénal spécial*, *op. cit.*, n° 860I.

[525] « *La formule* « accéder ou se maintenir frauduleusement » *évoque l'incrimination de la violation de domicile (art. 226-4). Elle répond à la même logique. Le STAD peut jouer, en quelque sorte, le rôle de domicile virtuel pour celui qui en est le maître et veut s'y sentir* « chez lui » […] » (E. DREYER, *op. cit.*, n° 860).

[526] C'est-à-dire de ne pas respecter les règles d'accès qui procèdent de la loi (sur la notion de tiers autorisé, v. *infra* n° 208 et svt.), du contrat ou de la volonté du « maître du système » (Paris, 5 avr. 1994*, JCP E* 1995, I, 461, obs. F. VIVANT et C. LE STANC ; *LPA* 1995, n° 80, p. 13, chron. Droit de la communication, note V. ALVAREZ *; Adde* C. ROBACZEWSKI, « Atteinte aux systèmes de traitement automatisé de données »*, op. cit.,* n° 31 *)*.

important qu'il n'y ait pas eu de dommages. C'est dire que ce que l'on veut protéger, c'est la vie privée qui, évidemment, se déroule pour l'essentiel dans un lieu privé »[527]. Les atteintes aux STAD qui sont incriminées touchent autant au fonctionnement du système – destruction, perturbation – qu'à la violation *du lieu* virtuel et troublent, en ce qu'il contient des données que l'on a souhaité réserver, la tranquillité. Cette lecture contribuerait à admettre que la protection accordée ne concerne pas des données précisément identifiées mais toutes les données qu'une loi, un contrat ou simplement le *maître du système* a entendu réserver, ce qui concerne aussi des informations relatives à l'intimité de la vie privée[528].

96. Une protection incidente du secret des informations relatives au malade. Quelques exemples jurisprudentiels récents invitent à penser que l'infraction offre une protection incidente aux secrets et, *a fortiori*, au secret des informations relatives aux personnes prises en charge par un professionnel intervenant dans le système de santé. Par exemple, concernant l'installation d'un *keylogger*[529] par un individu sur l'ordinateur de son épouse à l'insu de celle-ci, les juges du fond ont prononcé une condamnation du chef de maintien frauduleux dans un système de traitement de données[530] et de violation du secret des correspondances[531]. Plus récemment encore[532], les juges ont eu à connaître d'une affaire dans laquelle un médecin avait installé un logiciel espion similaire à celui évoqué dans l'affaire précédente afin de prendre connaissance des codes d'accès des messageries électroniques de deux de ses confrères de manière à pouvoir ensuite consulter celles-ci. Ces deux affaires portaient donc sur des formes d'espionnage et étaient toutes deux accompagnées d'une atteinte au secret des correspondances, par ailleurs sanctionnée sur le fondement de l'article 226-15 du Code pénal. Aussi est-il possible de ne voir dans l'atteinte aux STAD qu'un moyen de parvenir à la violation du secret des

---

[527] H. MATSOPOULOU, *Jcl. Pénal Code*, Art. 226-4, Fasc. 20 : « Violation de domicile », sept. 2009, n° 8.
[528] En ce sens, concernant l'infraction prévue à l'article 323-1 du Code pénal sanctionnant l'accès dans un STAD, v. F. CHOPIN, « Cybercriminalité », *op. cit.*, n° 15 : « *Il s'agit ici de sanctionner ceux qui cherchent à prendre connaissance d'informations, confidentielles ou non, contenues dans des systèmes de traitement automatisé de données, dont l'accès leur est interdit* »).
[529] Logiciel enregistreur de frappe qui renvoie les messages formés par la saisie des lettres du clavier sur un serveur extérieur.
[530] « […] *se rend coupable de l'infraction prévue à l'article 323-1 du Code pénal la personne qui, sachant qu'elle n'y est pas autorisée, pénètre dans un système de traitement de données* » (Crim., 10 mai 2017, n° 16-81822 ; *Dr. pén.* 2017, chron. 11, n° 8, obs. A. LEPAGE).
[531] CP, art. 226-15.
[532] Crim., 16 janv. 2018, n° 16-87168, publié au Bulletin ; *D.* 2018, p. 172 ; *AJ pénal* 2018, p. 205, obs. J.-B. THIERRY ; *RSC* 2018, p. 480, obs. P. MISTRETTA ; *Dalloz act.*, 12 févr. 2018, obs. M. RECOTILLET ; *RDS* n° 83, 2018, p. 389, obs. M. MAZZUCOTELLI.

correspondances, cette dernière pouvant, lorsqu'elle est commise à l'encontre d'une personne soumise au secret, porter indirectement atteinte au secret des informations relatives au malade. De même, l'agent qui accèderait sans droit[533], quel que soit le moyen utilisé[534], à des dossiers patients informatisés pourrait être poursuivi sur le fondement de l'article 323-1 du Code pénal et de l'article L. 1110-4, V du Code de la santé publique ou sur le fondement d'une infraction spéciale issue de la loi informatique et libertés.

2 - La violation du secret des correspondances électroniques

97. Absence de spécificité des communications « dématérialisées ». Les correspondances définies précédemment peuvent être échangées par voie électronique. Bien que les lettres missives – dont la particularité tient à la matérialité de leur support – ne disparaîtront sans doute jamais, les correspondances entre les acteurs du parcours de santé, mais également entre ces derniers et les patients, se font aujourd'hui essentiellement par voie électronique. Comme le remarque un auteur : « *À l'heure de la télémédecine et de l'intelligence artificielle, la médecine s'exerce quasi exclusivement à l'aide du numérique et des moyens de télécommunication modernes notamment internet, et il n'est plus exceptionnel de recevoir une prescription ou un certificat médical de son médecin directement sur sa boîte mail* »[535]. Mais l'utilisation des dispositifs techniques de la communication à des fins de correspondance est plus ancienne. Avant l'utilisation moderne des ondes électromagnétiques, le téléphone a constitué le premier moyen généralisé de communication à distance. C'est, d'ailleurs, à ce titre

---

[533] Le tiers peut tout à fait être un médecin qui accèderait, par exemple, aux dossiers de malades suivis par un confrère par le biais de la carte de professionnel de santé de ce dernier et à son insu. Le caractère frauduleux peut ainsi s'appliquer à un professionnel soumis au secret mais qui n'aurait pas la possibilité d'accéder à certaines informations dès lors que les conditions relatives au secret partagé ne seraient pas réunies. A l'inverse, l'accès n'est pas frauduleux dès lors que l'agent est habilité par ses fonctions à accéder à la partie du système informatique contenant les données sensibles (Grenoble, 4 mai 2000, *JCP G* 2001, IV, 1473). Aussi, dès lors que le responsable d'un système de traitement automatisé de données ne sécurise pas suffisamment les accès et permet à tout membre du personnel d'y accéder, indépendamment des conditions relatives au partage de l'information secrète tel que prévue à l'article L. 1110-4 du Code de la santé publique, l'élément moral de l'infraction ne peut être caractérisé.
[534] Il n'est pas possible et d'ailleurs bien inutile de lister les techniques permettant de *hacker* un système de traitement automatisé de données. Ces moyens évoluent avec la technique et se renouvellent de même. Pour quelques réflexions déjà anciennes sur l'évolution de la cybercriminalité dans une approche criminologique, v. B. DUPONT, « L'évolution du piratage informatique : de la curiosité technique au crime par sous-traitance », *in* AAPI (Association sur l'Accès et la Protection de l'Information) (ss. la dir.), *Le respons@ble 2.0 : Acteur clé en AIPRP*, Cowansville, Yvon Blais, 2010, pp. 63-81.
[535] P. MISTRETTA, « Le secret des correspondances, Molière et les tartufferies médicales... », *RSC* 2018, p. 480.

que la régulation médicale est définie comme un acte de télémédecine[536], la racine grecque du mot – τῆλε (de loin) – étant propre aux transmissions à distance. Si le Code de la santé publique encadre spécifiquement la mise en œuvre des actes de régulation médicale comme participant à l'aide médicale d'urgence[537], ce type de correspondance est protégé par les mécanismes du droit commun au même titre que les autres correspondances entre professionnels ou entre professionnels et patients qui ne répondent pas à la définition d'un acte de télémédecine.

98. Protection du secret des communications à distance et protection du secret des informations relatives au malade. La loi relative à la vie privée avait, dans un premier temps, créé certaines infractions protégeant les télécommunications[538] avant que ne soit incriminés les comportements d'espionnage audio-visuel, dont la captation des télécommunications[539]. Le droit au respect de la vie privée a donc été le premier fondement sur lequel ont été sanctionnées les atteintes aux correspondances à distance. Depuis, l'ajout d'un second alinéa à l'article 226-15 du Code pénal[540] sanctionne spécifiquement l'atteinte au secret des correspondances. Le texte d'incrimination prévoit ainsi que « *le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions* » est puni des mêmes peines que lorsque l'atteinte au secret porte sur des correspondances écrites « *matérialisées par un support qui les véhicule autant qu'il les fixe* »[541]. Aussi, lorsque les correspondances sont électroniques, le fait pour un tiers à la communication d'en prendre connaissance peut être qualifié de violation du secret des correspondances. Cette violation porte atteinte au secret des informations relatives au malade lorsque le contenu de la communication concerne des informations couvertes par le secret professionnel. Que l'information soient dissociable de son véhicule n'empêche pas une telle qualification, il en ressort simplement que l'ouverture de la communication, élément matériel de l'infraction, se

---

[536] CSP, art. L. 6316-1.
[537] CSP, art. L. 6311-2, défini aux articles L. 6316-1 et R. 6326-1 du même code.
[538] Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens, art. 23.
[539] Les textes d'incrimination, plusieurs fois modifiés, sont désormais inscrits aux article 226-1 et suivants du Code pénal.
[540] Par la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications (J. PRADEL, *D.* 1992, chron., p. 49). Cette loi faisait suite à la condamnation de la France par le Cour européenne des droits de l'homme dans un arrêt du 24 avril 1990 (CEDH, 24 avr. 1990, n° 11801/85 et 11105/84, *Kruslin c/ France et Huvig c/ France*).
[541] G. BEAUSSONIE, *Jcl. comm.*, Fasc. 3403 : « Secret des correspondances », mars 2014 (mise à jour août 2017), n° 22.

trouve dématérialisé[542]. La lecture des courriels suppose l'introduction dans la messagerie électronique. Cet acte constitue l'infraction prévue au premier alinéa de l'article 323-1 du Code pénal qui sanctionne l'accès et le maintien frauduleux dans un système de traitement automatisé de données[543].

C - La protection contre la maîtrise illicite de l'information secrète

99. Le recel est défini à l'article 321-1 du Code pénal[544]. Il s'agit d'une infraction de conséquence[545] qui nécessite la commission d'une infraction primaire, comme le prévoit le texte d'incrimination. En effet, la structure de l'incrimination suppose l'existence d'une condition préalable ainsi que la réunion d'un élément matériel et d'un élément moral. La condition préalable consiste dans l'existence de l'infraction d'origine, délit ou crime, ayant procuré la chose recelée. Le recel punit le fait de bénéficier ou de détenir une chose qui provient d'un crime ou d'un délit, aussi le vol est-il le « *support privilégié* »[546] de l'infraction mais « *l'élargissement concentrique des infractions servant de support au recel démontre que la nature de l'infraction d'origine est indifférente* »[547]. Ensuite, les deux alinéas du texte d'incrimination sanctionnent respectivement le recel-maîtrise[548] et le recel-profit[549]. Du fait de l'incrimination du bénéfice tiré du produit de l'infraction[550], le recel a également fait l'objet

---

[542] L'emploi du terme est ici exact. Il s'agit bien d'une dématérialisation de l'élément matériel de l'infraction.
[543] Crim., 16 janv. 2018, n° 16-87168, publié au Bulletin ; *D*. 2018, p. 172 ; *AJ pénal* 2018, p. 205, obs. J.-B. THIERRY ; *RSC* 2018, p. 480, obs. P. MISTRETTA ; *Dalloz act*., 12 févr. 2018, obs. M. RECOTILLET ; *RDS,* n° 83, 2018, p. 389, obs. M. MAZZUCOTELLI.
[544] Sur les incriminations spécifiques de recel v. P. MAISTRE DU CHAMBON, *Rép. pén.*, *V°* « Recel », 2009 (mise à jour mars 2018), n° 2 à 5.
[545] Sur lesquelles, v. E. DREYER, *Droit pénal général*, *op. cit.*, n° 702 et svt.
[546] P. MAISTRE DU CHAMBON, « Recel », *op. cit.*, n° 8.
[547] *Ibid.*, n° 13.
[548] Selon la formule utilisée par Monsieur Dreyer, car au regard du premier aliéna de l'article 321-1 du Code pénal, est incriminé le fait de dissimuler, de détenir, de transmettre et de faire office d'intermédiaire dans la transmission de la chose. Ainsi, ce que l'on nomme d'ordinaire recel-détention couvre un champ plus large que la simple détention. Il s'agit bien de maîtriser la chose, maîtrise pouvant se caractériser notamment par une détention (E. DREYER, *Droit pénal spécial*, *op. cit.*, n° 1239).
[549] Le recel-profit permet notamment de punir celui qui profite de la chose soustraite. L'exemple jurisprudentiel le plus connu concernait la condamnation pour recel du passager d'un véhicule dont il savait qu'il avait été dérobé : Crim., 9 juill. 1970, *RSC* 1973, p. 81, obs. M. CULIOLI.
[550]« […] *l'acte de recel peut consister dans le profit tiré de l'infraction d'origine, un profit qui n'implique pas forcément une quelconque détention, ce qui suffit à justifier que le recel puisse avoir pour objet un bien incorporel* » (P. MAISTRE DU CHAMBON, « Recel », *op. cit.*, n° 40). Ainsi le profit peut être simplement moral : M. DAURY-FAUVEAU, *Jcl. Pénal Code*, Fasc. 20 : « Recel », mars 2012 (mise à jour juin 2018), n° 25.

d'une dématérialisation[551]. Le produit étant le résultat d'une activité humaine[552], il n'est pas nécessairement tiré d'une chose, « *il est* […] *le produit d'une infraction, c'est-à-dire tout ce qu'il apparaît possible d'en obtenir, au-delà même de la chose qui n'en représente qu'une espèce* »[553]. Il ne fait donc nul doute que l'information secrète puisse faire l'objet d'un recel sur le fondement de l'alinéa 2 de l'article 321-1 du Code pénal. Sont ainsi punis le recel d'escroquerie[554], le recel de délit d'initié[555] et le recel de secret professionnel. Rien n'interdit par ailleurs de sanctionner le recel-profit d'une information obtenue irrégulièrement, c'est-à-dire indépendamment d'une violation du secret professionnel mais ayant pour conséquence de porter atteinte au *secret des informations*[556]. Mais la question se pose avec plus de difficulté s'agissant du recel-maîtrise étant donné qu'il nécessite la maîtrise d'une chose. Monsieur Beaussonie souligne à ce propos que la dématérialisation du recel « *ne doit être étudiée qu'en ce qu'elle constitue la conséquence de l'immatérialité de la chose, soit que l'infraction d'origine puisse également protéger un objet incorporel, soit que l'infraction d'origine ne protège, dès sa détermination, que de tels objets* »[557]. C'est pourquoi il nous semble utile de distinguer d'une part le recel de violation de secret professionnel **(2)** et d'autre part le recel d'usurpation d'informations couvertes par le secret **(1)**.

1 - Le recel de l'information secrète usurpée et des données extraites

100. Les errements de la jurisprudence ont été évoqués s'agissant de l'admission du vol des seules informations ou du « contenu informationnel ». Les hésitations jurisprudentielles rejaillissent nécessairement sur la qualification de recel **(a)**. La question se pose aussi à propos du recel d'extraction de données, mais la nature de l'infraction d'origine n'ayant pas d'importance, il semblerait qu'il faille admettre la possibilité d'un recel de données **(b)**.

---

[551] Pour un développement complet sur ce point, v. G. BEAUSSONIE, *La prise en compte de la dématérialisation des biens par le droit pénal. Contribution à l'étude de la protection pénale de la propriété*, préf. B. DE LAMY, coll. Bibliothèque de droit privé, t. 532, LGDJ, 2012, n° 260 à 283.
[552] C. ANDRÉ, « La cohérence de la notion de produit », *RRJ*, 2003-2, p. 751.
[553] *Ibid.*
[554] Une illustration : Crim., 11 févr. 2009, n° 07-86705, *AJ pénal* 2009, p. 183 ; *D.* 2009, p. 2403, obs. B. SARCY.
[555] Une illustration : Crim., 26 oct. 1995, *Bull. crim.* n° 324, *RSC* 1996, p. 648, obs. B. BOULOC, *Dr. pén.* 1996, comm. 189, obs. J.-H. ROBERT.
[556] CSP, art. L. 1110-4, V.
[557] G. BEAUSSONIE, *La prise en compte de la dématérialisation des biens par le droit pénal. Contribution à l'étude de la protection pénale de la propriété*, *op. cit.*, n° 259.

a - L'objet du recel

101. De l'usurpation au recel d'informations secrètes, la question de l'objet. L'admission par la jurisprudence du recel d'informations sur le fondement de l'article 321-1, alinéa 1 du Code pénal donne lieu à des débats doctrinaux qui font écho à ceux relatifs au vol d'informations[558]. En effet, si l'on admet que l'infraction protège l'information représentée et que c'est pour ne pas « *choquer les esprits* »[559] que le juge s'est astreint à employer des « *subterfuges* »[560] en reconnaissant par exemple le vol par reproduction[561] ou d'une utilisation[562], alors il devrait être admis que le recel puisse avoir pour objet les seules informations. En effet, dans une telle hypothèse le recel du vol du contenu informationnel par reproduction portera nécessairement sur les seules informations, la photocopie n'étant pas la chose soustraite. Le problème tient donc principalement à la notion de *chose* et la controverse tenant au vol d'information rejaillit nécessairement sur la détermination de la nature de la chose recelée.

102. La chose objet du recel. La *chose* objet du vol ne pourrait selon certains être incorporelle[563], toutefois cet argument est balayé par Monsieur Beaussonie dont nous

---

[558] A. MIHMAN, *Rep. pén.*, *V°* « Vol », avr. 2016 (mise à jour août 2017), n° 44.
[559] V. PELTIER, *Le secret des correspondances*, préf. P. CONTE, PUAM, 1999, n° 524.
[560] *Ibid.*
[561] Crim., 8 janv. 1979, *Logabax* ; *D.* 1979, p. 509, note P. CORLAY *; ibid.* IR p. 182, obs. G. ROUJOU DE BOUBEE ; M.-L. RASSAT, *in* Rapport de la Cour de cassation [année judiciaire 1979] ; *JCP G* 1981, I, 3041, nº 25 ; solution ensuite reprise : Crim., 29 avr. 1986, *Bull. crim.*, n° 148 ; *JCP* 1987, II, 20788, note H. CROZE ; *D.* 1987, p. 131, note M.-P. LUCAS DE LEYSSAC ; Crim., 6 janv. 1989, *Dr. pén.* 1990, n° 86. ; Crim., 24 oct. 1990, n° 89-84.485, *Bull. crim.*, n° 355 ; Crim., 9 juin 2009, n° 08-86843, *Bull. crim.*, n° 118 ; *Rev. pén.* 2009, p. 858, obs. S. FOURNIER ; *Gaz. Pal.* 25 août 2009, n° 237, p. 10, note S. DETRAZ ; *D.* 2010, p. 306, note H. KOBINA GABA ; Crim., 8 nov. 2011, n° 10-82021. Pour des analyses plus générales, v. J. DEVÈZE, « Les vols de « biens informatiques » », *JCP G* 1985, I, 3210, n° 20 s. ; M.-P. LUCAS DE LEYSSAC, « Une information seule est-elle susceptible de vol ou d'une autre atteinte juridique aux biens ? », *D.* 1985, chron. p. 443, n° 22 et svt. ; R. GASSIN, « Le droit pénal de l'informatique », *D.* 1986. chron. p. 35 *; Le droit criminel face aux technologies nouvelles de la communication*, 1986, Economica ; F. ALT-MAES, « Une évolution vers l'abstraction : de nouvelles applications de la détention », *RTD civ.* 1987, p. 21.
[562] Crim., 20 mai 2015, n° 14-81336, *Bull. crim.*, n° 119 ; *D.* 2015, p. 1466, note L. SAENKO ; *ibid.* p. 2465, obs. G. ROUJOU DE BOUBEE, T. GARE, C. GINEST, M.-H. GOZZI et S. MIRABAIL ; *AJ pénal* 2015, p. 413, note E. DREYER ; *JCP G* 2015, 887, note G. BEAUSSONIE ; *Dr. pén.* 2015, comm. 107, note M. VERON ; *ibid.* comm. 123, note P. CONTE ; *ibid.* chron. 10, obs. A. LEPAGE ; *Gaz. Pal.* 18 juin 2015, p. 8, note S. DETRAZ ; *RSC* 2015, p. 860, obs. H. MATSOPOULOU ; *ibid.* p. 887, obs. J. FRANCILLON ; *RTD com.* 2015, p. 600, obs. B. BOULOC ; *RTD eur.* 2016, p. 374, obs. E. MATRINGE ; *RDC* 2015, p. 951, note P. BERLIOZ ; *LPA*, 29 juill. 2015, n° 150, p. 15, obs. E. CHAUVIN ; *PI* janv. 2016, p. 97, obs. M. VIVANT.
[563] En ce sens, notamment, v. E. DREYER, *Droit pénal spécial*, *op. cit.*, n° 881 ; M.-L. RASSAT, *Droit pénal spécial. Infractions du Code pénal*, 8ème éd., coll. Précis, Dalloz, 2018, n° 105 à 107.

partageons le point de vue[564]. Il en va de même du recel : d'abord, la condition préalable consiste dans l'existence d'une infraction d'origine qui peut être un crime ou délit, la nature de celle-ci étant indifférente, ensuite l'objet du recel est également une « chose » et l'on trouve dans la jurisprudence les mêmes hésitations qu'en matière de vol. L'on pourrait toutefois admettre une telle possibilité, indépendamment de toute remise matérielle, par le jeu de la notion de recel-profit comme le soulignent Mesdames Matsopoulou et Lepage[565].

b - Le recel de données extraites d'un système de traitement automatisé de données

103. Existence d'un recel spécial. Dès lors qu'est incriminé le fait d'extraire des données d'un système automatisé, que la peine est aggravée lorsqu'il s'agit de données à caractère personnel issues d'un système automatisé mis en œuvre par l'Etat, l'infraction peut contribuer à la protection du secret des informations relatives au malade. Prévu à l'article 323-3 alinéa 2 du Code pénal, le délit aggravé est puni de sept ans d'emprisonnement et de 300 000 euros d'amende. L'incrimination générale de recel de chose ne trouve pourtant pas à s'appliquer dans le cas d'une détention ou d'une transmission d'extraction de données d'un système de traitement automatisé. Comme pour d'autres hypothèses[566], le législateur a spécifiquement incriminé la détention et la transmission frauduleuse de données contenues dans un système de traitement automatisé, ces actes étant également incriminés à l'article 323-3 du Code pénal. L'agent qui extrait les données et celui qui les détient seront donc poursuivis sur le même fondement. Cette incrimination spécifique constitue une réponse adéquate aux difficultés relatives au recel de données issues d'une fraude informatique. Un parallèle peut être fait avec l'incrimination du recel d'images pédopornographiques sur le fondement de l'article 227-3 du

---

[564] « […] *Est donc une chose, en droit en général, et en droit pénal en particulier, tout ce qui n'est pas une personne (juridique : car certaines personnes humaines ont été des choses, et ce qui compose chaque personne humaine l'est encore), tout objet, quel qu'il soit qui existe indépendamment du sujet de droit*. […] *A cet égard, il faut distinguer les informations nommées, généralement par métonymie, des informations qualifiées, la plupart du temps simplement dites « confidentielles » ou « personnelles ». Pour être plus difficilement identifiables, les secondes n'en existent pas moins, mais nécessitent que le juge les dévoile avant d'en sanctionner l'éventuelle appropriation frauduleuse*. » (G. BEAUSSONIE, « A propos d'une controverse contemporaine et persistante : le vol d'informations », *Revue de droit d'Assas*, déc. 2018, n° 17, p. 102).

[565] H. MATSOPOULOU et A. LEPAGE, *Droit pénal spécial*, coll. Thémis droit, PUF, 2015, n° 878.

[566] Est ainsi spécifiquement sanctionné le recel de criminel (CP, art. 434-6), le recel de cadavre (CP, art. 434-7) ou encore le recel d'images pédopornographiques (CP, art. 227-3, al. 4). Pour une liste des recels spéciaux v. P. MAISTRE DE CHAMBON, « Recel », *op. cit.*, n° 2 à 5.

Code pénal qui avait permis d'éviter les obstacles relatifs au recel de diffusion d'image ou de représentation de mineur à caractère pédopornographique[567]. Les images ou représentations de mineur à caractère pornographique pouvant également être indépendantes de tout support matériel lorsqu'elles circulent sur internet, le législateur avait choisi d'incriminer leur détention par une infraction autonome[568] en réaction à la pratique de certains juges ayant eu recours à des artifices en considérant notamment que le disque dur contenant les images constituait un support matériel qui était l'objet du recel[569].

2 - Le recel de violation de secret professionnel

104. L'étude du recel avant l'étude de l'infraction principale. Bien que la violation du secret professionnel ne soit envisagée qu'ulterieurement, le recel de la violation de secret professionnel peut être étudié dès à présent. Les raisons qui justifient ce choix s'explique par le fait que si la nature de l'objet du recel tient à l'objet de l'infraction principale, et que le recel suppose une infraction préalable, elles sanctionnent des comportements différents. Elles présentent donc, s'agissant de l'agent qui commet un recel de secret professionnel, une protection supplémentaire du secret des informations mais cette fois à l'égard du tiers qui détient ou transmet à son tour l'information objet du délit de violation du secret professionnel. L'indifférence quant à l'utilisation de la chose détenue permet de sanctionner l'agent qui rendrait publique des informations obtenues suite à une violation du secret professionnel. Aussi, il n'est nul besoin d'étudier la violation du secret professionnel pour analyser celle punissant le recel de ce délit. Il suffit de garder à l'esprit que pour que l'infraction de conséquence soit constituée il faut nécessairement que soit démontrer l'existence du premier délit, condition préalable.

105. L'information secrète, objet du recel de secret professionnel. La chose recelée doit provenir d'un crime ou d'un délit, aussi le recel n'est-il pas limité à la seule protection du

---

[567] CP, art. 227-3, al. 1.
[568] Pour une étude complète, v. J. LEONHARD, *Etude sur la pornographie pénalement prohibée*, th. dact. ss. la dir. de B. PY, soutenue le 5 nov. 2011, Université Nancy II, n° 334.
[569] Crim., 9 juin 1999, n° 98-80.052 ; *JCP G* 1999, IV, 2867 ; *Dr. pén.* 1999, comm. 138, M. VERON ; *Adde* J. LEONHARD, *Etude sur la pornographie pénalement prohibée*, *op. cit.*, n° 334.

patrimoine et peut protéger la personnalité[570]. Il est ainsi admis que la violation des secrets protégés par la loi peut faire l'objet d'un recel[571], ce qui implique la violation du secret professionnel des personnes intervenant dans le système de santé ainsi que la violation des correspondances qui seraient échangées entre des professionnels soumis au secret ou entre un professionnel et un patient. Néanmoins, l'objet du recel-maîtrise incriminé à l'alinéa premier de l'article 321-1 du Code pénal demeure une *chose*. Contrairement au vol, le secret professionnel, infraction d'origine, ne suppose que la révélation d'une information secrète, le moyen de la révélation est par ailleurs indifférent, celle-ci peut être écrite ou orale, quel qu'en soit le véhicule. Les termes du texte d'incrimination du recel semblent donc interdire de qualifier ainsi la détention ou la transmission d'une information secrète sans remise matérielle, ce que retient par ailleurs le juge répressif lorsqu'il affirme que « *si une information échappe aux prévisions de l'article 321-1, C. pén. qui réprime le seule recel d'une chose, et ne relève, le cas échéant, que des dispositions légales spécifiques à la liberté de la presse, tel n'est pas le cas du recel de documents provenant d'une violation du secret de l'instruction ou du secret professionnel* »[572]. Cette solution est dominante s'agissant du recel de violation de secrets[573], et l'on peut en trouver une illustration s'agissant du recel de violation du secret professionnel médical[574]. Ainsi, l'infraction de recel n'apporterait le support de sa sanction à la protection du secret des informations relatives au malade que lorsque l'information est attachée à un support, c'est-à-dire représentée sur un support matériel[575]. De même, l'admission d'un recel de violation du secret des correspondances posera une difficulté lorsque les communications sont

---

[570] P. MAISTRE DE CHAMBON, « Recel », *op. cit.*, n° 11.

[571] A propos du recel d'un secret de fabrique : Crim., 7 nov. 1974, *Bull. crim.* n° 323, *D.* 1974, somm. p. 144. S'agissant du recel de violation du secret professionnel par un fonctionnaire de police : Crim., 26 oct. 1995, *Bull. crim.*, n° 328 ; *RSC* 1996, p. 660, obs. R. OTTENHOF. Sur un recel de violation du secret de l'instruction : Crim., 12 juin 2007, n° 06-87361, *Bull. crim.*, n° 157 ; *JCP* 2007, II, 10159, note F. FOURMENT ; *Rev. pén.* 2008, p. 113, obs. J.-C. SAINT-PAU.

[572] Crim., 12 juin 2007, n° 06-87361, préc.

[573] Crim., 26 oct. 1995, *Bull. crim.*, n° 328; *RSC* 1996, p. 660, obs. R. OTTENHOF; Crim., 19 juin 2001, *Bull. crim.*, n° 149 ; *D.* 2001, p. 2538, note B. BEIGNIER et B. DE LAMY ; *D.* 2002, somm. p. 1463, obs. J. PRADEL ; *RSC* 2002, p. 96, obs. B. BOULOC *; ibid.* p. 119, obs. J. FRANCILLON ; *ibid.* p. 592, obs. J.-P. DELMAS SAINT-HILAIRE ; *JCP* 2002, II, 10064, concl. D. COMMARET, note A. LEPAGE. Il apparaît toutefois qu'un courant jurisprudentiel minoritaire semble favorable à la reconnaissance du recel d'information issue de la violation d'un secret professionnel sans remise materielle, ainsi que le souligne Mesdames Matsopoulou et Lepage (H. MATSOPOULOU et A. LEPAGE, *Droit pénal spécial*, coll. Thémis droit, PUF, 2015, n° 878). A titre d'exemple : le prévenu condamné pour avoir « *accueilli, en connaissance de cause, des renseignements, frauduleusement communiqués, sur un secret de fabrication et qui les a mis en œuvre* » : Crim., 7 nov. 1974, *Bull. crim.*, n° 323 ; Crim., 20 juin 2006, n° 05-86491.

[574] Crim., 19 oct. 2005, n° 04-85098.

[575] En ce sens P. MAISTRE DE CHAMBON, « Recel », *op. cit.*, n° 41.

effectuées à distance. Il a pu être défendu l'idée selon laquelle la matérialité de l'acte de recel devrait suffire à qualifier l'acte[576]. Par ailleurs, Madame Rassat réfute l'interprétation selon laquelle le recel de l'information seule échappe aux prévisions de l'article 321-1 du Code pénal, considérant que « *tout ce qui a été appréhendé par un crime ou un délit peut être recelé sans qu'il soit utile ni, d'ailleurs juridiquement possible, de faire une distinction selon la nature de ces objets* »[577].

106. Conclusion du premier chapitre. En mobilisant le concept de représentation, propre aux techniques de l'information, comme lien unissant l'information et son support, nous avons pu envisager les mécanismes juridiques protégeant le secret « objet » au travers de son support. En tenant compte de la polysémie du mot « secret », mais aussi de l'usage du syntagme « secret médical » dans les textes et la jurisprudence, ainsi que du contexte dans lequel la doctrine le mentionne lorsqu'elle reproduit les formules employées par le législateur, il a été possible de différencier les hypothèses dans lesquelles le secret est visé comme une situation protégée – *secret-état*.

107. Le maintien de cette situation, du fait de l'existence du support, est en partie indépendant de l'attitude de silence du professionnel. Des règles juridiques et déontologiques imposent alors la mise en œuvre concrète de moyens visant la protection du support au travers duquel l'information secrète – *secret-fait* – est protégée. Partant, il a été entrepris une étude des mécanismes sanctionnant une atteinte au *secret-état*, qu'il s'agisse d'en soustraire le support, de prendre connaissance de l'information à travers celui-ci ou lorsque le support et l'information peuvent être désolidarisés. L'approche consistant à envisager le « secret médical » comme objet de protection nous apprend qu'il ne s'entend pas uniquement

---

[576] A propos du recel par transmission d'une violation du secret des correspondances V. PELTIER, *Le secret des correspondances*, *op. cit.*, n° 557 : « […] *la condition de la matérialité de l'acte de transmission semble pouvoir être tenue sans réelle difficulté même s'il s'agit de livrer des informations seules. Qu'il s'agisse de correspondances corporelles ou dématérialisées demeure ici indifférent. Effectivement, il faut imaginer que le receleur a reçu les informations sans l'aide d'un support, par conversation réalisée sans le biais d'une correspondance matérielle quelconque, sinon l'acte de réception serait matériel, et l'incrimination de la transmission ne servirait qu'à faire double emploi avec celle de la réception, ce qui se produit dans toutes les autres hypothèses de transmission. En clair, on suppose qu'une personne a frauduleusement soustrait des données appartenant à une entreprise. Si elle les livre à un tiers en discutant avec lui (sans passer par une correspondance qui conférerait à la réception une nature matérielle), ce dernier ne peut pas encore être qualifié de receleur. En revanche, s'il transmet ensuite les informations acquises illicitement, soit par téléphone, soit par lettre ou par fax, ne peut-on alors logiquement considérer qu'il tombe sous le coup de l'article 321-1 du Code pénal puisque l'acte de transmission* […] *est matériel ?* ».

[577] M.- L. RASSAT, *Droit pénal spécial*. *Infractions du Code pénal*, 8ème éd., coll. Précis, Dalloz, n° 234.

du secret professionnel mais vise également la protection spécifique de l'information représentée et la sanction des atteintes à son support. Au regard de l'utilisation des dispositifs techniques de l'information et de la communication, il a été mis en évidence que le « secret médical », ainsi compris, bénéficiait d'une protection multipolaire.

Chapitre 2 - La violation du secret professionnel et l'atteinte au secret

108. Indépendamment de la relation entre l'information secrète et son support, les dispositifs techniques de l'information et de la communication peuvent également permettre de capter ou fixer les informations. Il est souvent oublié que les techniques d'espionnage audiovisuel sont des technologies de la communication[578], elles permettent donc de porter atteinte au secret de la vie privée et partant au « secret médical » **(section 1)**. Les dispositifs techniques de la communication sont par ailleurs des moyens de violation du secret professionnel **(section 2)**.

Section 1 - La protection contre la fixation illicite d'informations relatives à la vie privée

109. Il importe désormais de constater que les dispositifs techniques peuvent également être un moyen d'atteinte au « secret médical » objet juridiquement protégé. Ils peuvent en effet permettre de capter ou fixer des informations issues de la prise en charge d'une personne par un professionnel intervenant dans le système de santé **(§2)**, l'information secrète étant en effet une information protégée par le droit au respect de la vie privée **(§1)**.

§ 1 - La protection des informations secrètes par le droit au respect de la vie privée

110. Les informations relatives à la santé sont classiquement admises comme faisant partie de la vie privée telle qu'elle est définie par la doctrine. Une brève analyse au regard de la définition substantielle qui en est donnée suffit à s'en convaincre **(A)**. Ainsi, le secret de ces informations peut être assuré par les instruments juridiques protégeant le secret de la vie privée **(B)**.

---

[578] V. par exemple : Direction générale des entreprises, *Etudes sur les technologies clés 2016*, « Technologies de l'information et de la communication », p. 58 et svt.
Disponible en ligne : <https://www.entreprises.gouv.fr/files/files/directions_services/politique-et-enjeux/innovation/tc2015/technologies-cles-2015-tic.pdf> (dernière consultation le 14 oct. 2019).

A - Le secret de la vie privée et les informations concernant le patient : approche substantielle

111. Selon la conception classique du droit au respect du secret de la vie privée, il nous faut traiter successivement de la santé des personnes comme élément de la vie privée **(1)** et de l'identité de la personne comme condition de l'atteinte au secret des informations relatives aux patients **(2)**.

1 - Le droit au secret de l'intimité de la vie privée et la santé des personnes

112. Du *droit au* « secret médical » dans la jurisprudence et de l'interprétation qui en est faite par la doctrine. A se référer à la définition traditionnellement admise du « secret médical », il s'agirait, outre d'une obligation du professionnel, d'un « *droit du patient* ». De cette annonce faite par le législateur lors de la loi du 4 mars 2002, il a été déduit, hâtivement selon nous, une *mutation* du secret professionnel médical[579]. Il s'agit d'affirmer que, tandis que l'expression a longtemps désigné le seul secret professionnel des professionnels de santé, elle viserait désormais un droit dont il a pu être affirmé qu'il consacrait la maîtrise de ses informations par le patient[580]. Depuis le début des années 2000, une jurisprudence abondante en matière civile paraît aller dans ce sens, notamment en matière d'assurance. Il nous semble que, sur ce point encore, l'emploi de l'expression « secret médical », dans la jurisprudence, a donné lieu à des confusions. Dans un arrêt, souvent pris en exemple comme confirmant cette évolution, la deuxième chambre civile de la Cour de cassation affirme : « *L'assureur ne peut produire un document couvert par le secret médical intéressant le litige qu'à la condition que l'assuré ait renoncé au bénéfice de ce secret* »[581]. Cette formulation a laissé penser que le

---

[579] « *Le secret médical apparaît être une notion en mutation. Il était envisagé à l'origine comme un devoir du médecin dont bénéficiait indirectement le malade, mais sa modernisation conduit aujourd'hui à l'envisager davantage comme un droit appartenant directement au patient* » (M. CAUCHY, A. DIONISI-PEYRUSSE, « Le droit au secret médical et son application en matière d'assurances », *D.* 2005, p. 1313) ; Dans le même sens v. D. THOUVENIN, « Secret médical et loi du 4 mars 2002 : quels changements », *Laennec* n° 2007/1, p. 64 ; S. ABRAVANEL-JOLLY, « Le secret médical en assurance de personne » *RGDA* 2005, n° 4, p. 887 ; M. COTTET, « Le secret de la personne protégé par le médecin : le secret médical », *LPA* 2016, n° 226-227, p. 36.

[580] « *Le médecin n'est plus maitre aujourd'hui du secret* » selon les mots de certains auteurs (A. LAUDE, B. MATHIEU et D. TABUTEAU, *Droit de la santé*, 3ème éd., coll. Thémis droit, PUF, 2012, n° 305).

[581] Cass. civ. 2ème, 2 juin 2005, n° 04-13.509, *D.* 2006, p. 1784, obs. H. GROUTEL ; *D.* 2006, p. 689, pan. J. PENNEAU.

consentement du déposant justifiait définitivement la violation du secret professionnel[582]. La possibilité, pour l'assuré, de donner son consentement à la divulgation d'informations relatives à sa santé s'explique pourtant par le fait que l'assureur n'est pas un professionnel soumis au secret[583]. Il peut donc être simplement entendu que la nécessité du consentement se déduit de l'article 9 du Code civil : *«la personne doit consentir au principe même d'une révélation ou d'une immixtion dans la vie privée* »[584]. Le professionnel qui n'est pas soumis au secret, comme c'est le cas de l'assureur, ne pourra révéler une information relative à la vie privée que lorsque la personne a consenti à la divulgation[585]. La lecture qui a été faite de certains arrêts, pour en

---

[582] Il a ainsi pu être affirmé que l'objectif du « secret médical » consistait uniquement dans « la protection de la vie privée » (M. CAUCHY, A. DIONISI-PEYRUSSE, « Le droit au secret médical et son application en matière d'assurance », *op. cit.*).

[583] Dans ce sens et sur les raisons du refus de soumettre les assurances au secret professionnel, v. C. JAY, *Le risque santé et la souscription d'assurance du crédit*, th. dact. ss. la dir. de B. PY, soutenue le 11 déc. 2017, Université de Lorraine, n° 97 à 99.

[584] A. LEPAGE, *Rép. civ.*, *V°* « Personnalité (Droits de la) », 2009 (mise à jour nov. 2017), n° 186.

[585] C'est ainsi qu'il faut entendre, à notre sens, la « renonciation au *secret médical* » mentionnée dans plusieurs arrêts (Civ. 1er, 3 janv. 1991, n° 89-13808, cité par J.-D. SARCELET, « La confidentialité des informations de santé peut-elle tenir face à la protection d'autres intérêts légitimes ? », *D.* 2008, p. 1921 ; civ. 1re, 9 juin 1993, *Bull. civ.* I, n° 214 ; *RTD civ.* 1996, p. 166, obs. J. MESTRE ; Civ. 1re, 29 oct. 2002, *Bull. civ.* I, n° 244 ; *D.* 2002, IR p. 3186 ; civ. 1re, 26 sept. 2006, n° 05-11906, *Bull. civ.* I, n° 417). Dans l'arrêt précité du 29 octobre 2002, il ne s'agissait pas de savoir si le médecin pouvait ou non révéler une information à caractère secret mais de constater « *que l'assureur avait subordonné sa garantie à la production d'un certificat médical indiquant « si possible » la nature de la maladie ayant entraîné le décès et que l'assuré avait, en acceptant la divulgation de certains éléments le concernant, renoncé lui-même et par avance au secret médical, une cour d'appel en a exactement déduit que ses ayants droit faisaient échec à l'exécution du contrat en refusant de communiquer les éléments nécessaires à l'exercice des droits qu'ils revendiquaient et notamment pour établir leur allégation d'un décès en dehors d'une maladie par l'avis du seul professionnel qualifié qu'est le médecin. La Cour de cassation admet clairement la renonciation de l'assuré à se prévaloir du secret médical, soit à l'occasion du sinistre, soit même à l'avance dès la prise d'assurance. Dans cette hypothèse, l'information n'est pas détenue par le médecin et l'assuré a renoncé lui-même à opposer le secret médical* » (A.-E. CREDEVILLE, « Le secret médical et la preuve judiciaire ou le secret médical mis en perspective », *D.* 2009, p. 2645) ; tandis que dans l'arrêt précité du 26 septembre 2006, « *La Cour de cassation admet que le médecin révèle les informations qu'il détient lorsque l'assuré ou ses ayants droit le sollicitent. C'est l'hypothèse où le patient ou ses ayants droit délient le médecin du secret. Ils pourront donc eux-mêmes, dès lors que ce sera dans l'intérêt de leurs prétentions, remettre copie des documents auxquels ils peuvent accéder depuis la loi du 4 mars 2002 à l'expert éventuellement désigné par le tribunal. Le médecin n'aura donc plus dans cette hypothèse à se demander s'il est ou non en droit de passer outre le secret médical* » (A.- E. CREDEVILLE, « Le secret médical et la preuve judiciaire ou le secret médical mis en perspective », *op. cit.*). L'on constate au regard de cette dernière remarque de l'auteur que ce qui est entendu par « renonciation au *secret médical* » consiste en réalité en un consentement à une révélation tel qu'entendu par l'article 9 du Code civil, ce qui se comprend dès lors que le malade est libre de faire ce qui lui plaît avec les informations le concernant. Le secret professionnel, le concernant, ne peut lui être opposé par le professionnel. Il n'est donc pas question de délier le médecin du secret mais simplement d'admettre que le patient est libre de divulguer les informations que lui fournit son médecin. Il s'agit simplement d'affirmer que le cocontractant qui révèle de lui-même certaines informations ne peut se prévaloir d'une violation de sa vie privée. L'emploi du terme « secret médical » pour signifier la nature des informations est source de confusion puisqu'il ne s'agit pas de s'interroger quant à la possibilité, pour le médecin, d'opposer le secret professionnel. En d'autres termes, la remise volontaire, par

déduire que « *le médecin est en droit de transmettre de telles informations dès lors que le patient à renoncé au bénéfice du* ***secret médical*** »[586] nous paraît être une interprétation défendable dès lors qu'elle ne conduit pas à affirmer que le consentement est, à lui seul, un fait justificatif de la violation du secret professionnel[587] . Nous souscrivons, sur ce point, à l'analyse de Madame Duval-Arnould selon laquelle lorsque le juge ordonne une expertise judiciaire, le professionnel soumis au secret *peut* communiquer les informations nécessaires si le patient y consent[588], mais *peut* également les communiquer malgré l'opposition de l'assuré « *dès lors que son opposition à la levée du secret médical tendait, non pas à faire respecter un intérêt moral légitime, mais à faire écarter un élément de preuve contraire à ses prétentions et à faire échec à l'exécution de bonne foi du contrat auquel il était partie, en mettant l'assureur dans l'impossibilité de prouver les réticences et omissions volontaires qu'il lui imputait* »[589]. Dès lors, il s'agit d'affirmer que l'article 11 du Code civil qui donne le pouvoir au juge civil, à la requête de l'une des parties, de demander ou ordonner la production de tous documents détenus par des tiers, s'il n'existe pas d'empêchement légitime, consiste en une autorisation de révéler. Il n'est toutefois pas possible d'y contraindre le professionnel en l'absence de texte prévoyant une telle obligation, lorsque son patient s'y oppose[590]. L'on en revient donc à la solution précédente : le médecin peut communiquer l'information malgré l'opposition de l'assuré. Il s'agit d'une autorisation de la loi et non d'une obligation. L'autorisation du patient est l'un des éléments de justification et, lorsqu'il n'est pas donné, c'est au juge de déterminer de la légitimité du refus et d'en tirer les conséquences quant à la nullité du contrat. Madame Duval-Arnauld,

---

l'assuré, des documents médicaux à l'assureur constitue une *renonciation implicite de se prévaloir du secret médical* selon les termes de ces arrêts, et consiste donc en une révélation volontaire d'élément relatif à sa vie privée par le patient lui-même. Il n'est pas possible d'en déduire que le malade peut *délier*, par sa seule volonté, le professionnel de son obligation.

[586] M. COUTURIER, « Que reste-t-il du secret médical ? », *in Mélanges en l'honneur de Gérard Mémeteau. Droit médical et éthique médicale : regards contemporains*, coll. Mélanges, LEH, 2015, p. 356.

[587] Sur cette question, v. *infra* n° 343 et svt.

[588] A propos de civ. 1re, 22 mai 2002, *Bull. civ.* I, n° 144 ; *D.* 2002, IR p. 2029 ; *Defrénois* 2002, p. 1477, note J. MASSIP ; D. DUVAL-ARNOULD, « Le juge civil face au secret médical », *D.* 2004, p. 2682. Dans cet arrêt il a été jugé que l'article 901 du Code civil exigeant la sanité d'esprit pour effectuer une donation vaut autorisation au sens de l'art. 226-14 du Code pénal. Il s'agit bien d'une autorisation et non d'une obligation, ainsi le professionnel peut révéler des informations dans l'intérêt de la personne ou de ses ayants droits, mais il n'y est pas obligé.

[589] A propos de civ. 1re, 3 janv. 1991, *Bull. civ.* I, n° 18 : D. DUVAL-ARNOULD, « Le juge civil face au secret médical *», op. cit.*

[590] Civ. 1re, 15 juin 2004, n° 01-02338, *Bull. civ.* I, n° 171 ; *D.* 2004, p. 2682, note D. DUVAL-ARNOULD ; *D.* 2005, pan. p. 1323, obs. H. GROUTEL ; *RTD civ*. 2005, p. 99, obs. J. HAUSER ; *ibid.*, p. 384, obs. J. MESTRE et B. FAGES.

concluant son propos, explique que « *depuis la loi du 4 mars 2002 ayant donné à l'assuré la possibilité d'accéder aux informations médicales le concernant et aux ayants droit celle d'accéder aux informations leur permettant de faire valoir leurs droits, l'expert judiciaire ne devrait plus avoir besoin de solliciter le médecin pour obtenir la communication des informations médicales nécessaires à l'exercice de sa mission ; l'assuré ou les ayants droit étant en mesure de lui remettre les copies des pièces médicales détenues par le médecin. Le juge, confronté à une opposition des ayants droit ou de l'assuré à leur remise à l'expert, devrait pouvoir plus aisément apprécier si celle-ci est fondée et en tirer les conséquences* »[591].

Partant, le patient ne *« renonce pas au secret médical »* lorsqu'il communique lui-même certaines informations mais consent à ce que les documents ou informations qu'il a lui-même transmis soient produites par l'assureur, non soumis au secret. Ensuite, son consentement à la révélation par un professionnel soumis au secret n'est jamais suffisant à justifier cette révélation. Il faut nécessairement qu'un texte l'autorise comme c'est le cas de l'article 11 du Code civil ou de l'article 109 du même code. Aussi est-il encore nécessaire de préciser, au regard de la polysémie du mot *secret*, que les informations couvertes par le secret professionnel sont à la fois objet de l'obligation de secret dont sont débiteurs les professionnels soumis au secret, autant qu'elles sont des informations relatives à l'intimité de la vie privée – intérêt juridiquement protégé – à l'égard des tiers. C'est en ce sens qu'il faut entendre le « *droit au respect de sa vie privée et du secret des informations la concernant* »[592]. L'article L. 1110-4 du Code de la santé publique, à notre sens, ne fait que réaffirmer le droit au respect de la vie privée tel qu'il est prévu à l'article 9 du Code civil.

113. Droit au respect de la vie privée, secret de la vie privée. Le droit au respect de la vie privée est traditionnellement défini comme un pouvoir et un intérêt[593]. Il est, pour une majorité de la doctrine, un droit de la personnalité fondé sur la notion de droit subjectif[594] et, selon un

---

[591] D. DUVAL-ARNOULD, « Le juge civil face au secret médical », *op. cit*.
[592] CSP, art. L. 1110-4.
[593] « *Avoir un droit, signifie qu'il existe quelque chose* pour nous*, que le pouvoir de l'Etat reconnaît, pour laquelle il nous accorde sa protection* » (R. von JHERING, *L'évolution du droit (Zweck im Recht)*, trad. O. de Meulenaere, Chevalier-Marescq, 1901).
[594] L'existence des droits de la personnalité est sujette à controverse et la pertinence de la catégorie juridique est discutée mais a fait l'objet d'une longue construction (R. NERSON, *Les droits extrapatrimoniaux*, th. Lyon, 1939 ; A. DECOCQ, *Essai d'une théorie générale des droits sur la personne,* préf. G. LEVASSEUR, LGDJ, 1960 ;

auteur, la « *matrice des droits de la personnalité* »[595]. L'objet de ce droit est le respect de la vie privée. Le droit au respect[596] se constitue, juridiquement, d'une « *prérogative défensive* »[597] et d'un « *pouvoir d'action* »[598] qui s'exprime dans la liberté de la vie privée. Ainsi, le droit subjectif garanti à l'article 9 du Code civil se compose de deux « *sous-prérogatives* »[599]. Cette dualité est affirmée par la jurisprudence qui considère, sur le fondement de l'article 9 du Code civil, comme illicite « *toute immixtion arbitraire dans la vie privée* »[600] mais juge également illicite toute révélation d'informations relatives à la vie privée d'un individu, que cette divulgation soit publique[601] ou privée. Le pouvoir de la personne réside donc dans la possibilité

P. KAYSER, « Les droits de la personnalité, aspects théoriques et pratiques », *RTD civ.*, 1971, p. 445 ; P. ANCEL, *L'indisponibilité des droits de la personnalité. Une approche critique de la théorie des droits de la personnalité*, th. dact., ss. la dir. de G. COUTURIER, Université de Lyon, 1978 ; J. ANTIPPAS, *Les droits de la personnalité – De l'extension au droit administratif d'une théorie fondamentale de droit privé,* préf. J. HUET, PUAM, 2012) et son autonomie a ensuite été affirmée, par opposition aux droits patrimoniaux, par Perreau (E.- H. PERREAU, « Des droits de la personnalité », *RTD civ.* 1909, p. 501) puis par Nerson (R. NERSON, *Les droits extrapatrimoniaux*, *op. cit.*). Enfin, Pierre Kayser proposa une classification de ces droits (P. KAYSER, « Les droits de la personnalité, aspects théoriques et pratiques », *op. cit.*). Pourtant les principaux caractères des droits de la personnalité – incessibles, personnels et intransmissibles – sont toujours discutés. A leur propos Messieurs Zenati-Castaing et Revet objectent : « *Le concept des droits de la personnalité a été créé pour traduire l'appropriation là où la catégorie du droit de propriété était rendue inutilisable par son inclusion dans les droits patrimoniaux. Il a semblé plus économe de créer une notion nouvelle que de redéfinir les notions de base du droit commun et réviser les classifications dans lesquelles l'évolution de la pensée juridique les avait rangées* » (F. ZENATI-CASTAING et T. REVET, *Manuel de droit des personnes*, 1re éd., coll. Droit fondamental, PUF, 2006, n° 262). En partant de l'idée selon laquelle « *le droit de propriété n'est pas un bien mais l'instrument par lequel une chose devient un bien* », les auteurs considèrent que « *La prérogative ayant pour objet la personnalité est un droit de propriété* » (*ibid.*), expliquant que « *Ces droits ne sont rien d'autres qu'une spécialisation parmi d'autres du régime de la propriété à raison du particularisme de son objet* » (*ibid.)*. Pour un état des questions sur ce point v. J. ROCHFELD, *Les grandes notions du droit privé*, 2ème éd., coll. Thémis, PUF, 2013, Notion n° 2, § 28.b.

[595] C'est ainsi que Monsieur Saint-Pau désigne la protection attachée à l'article 9 du Code civil, idée qu'il développe en réaction à une décision relative à l'image des personnes et dans laquelle la protection de l'image a été rattachée à l'article 9 du Code civil (J.-C. SAINT-PAU, note sous civ. 1re, 16 juill. 1998, *D.* 1999, p. 541). C'est par ailleurs ce que l'auteur développe dans sa thèse de doctorat et qu'il exprime ensuite ainsi « […] *le concept de vie privée ne s'entend plus seulement de l'intimité, mais également de l'identité ; chacun dispose ainsi d'un pouvoir de contrôle des éléments de son identification, c'est-à-dire d'un droit à l'anonymat* » (J.-C. SAINT-PAU, *Jcl. Comm.*, fasc. 34 : « Droit au respect de la vie privée – Définition conceptuelle du droit subjectif », n° 24).

[596] Ce droit au respect permet à la personne d'exercer un droit de contrôle légitime

[597] C'est-à-dire le « *droit à l'inviolabilité de la vie privée* » : J.-C. SAINT-PAU, « Le droit au respect de la vie privée », *in* J.-C. SAINT PAU (ss. la dir.), *Droits de la personnalité*, coll. Traités, LexisNexis, 2013, n° 1130.

[598] *Ibid.*

[599] V. PELTIER, *Le secret des correspondances*, préf. P. CONTE, PUAM, 1999, n° 60.

[600] Civ. 1re , 6 mars 1996, n° 94-11273, *Bull. civ.* I, n° 124 ; *D.* 1997, p. 7, note J. RAVANAS ; civ. 2ème, 3 juin 2004, n° 02-19886, *Bull. civ.* II, n° 273 ; *D.* 2004, p. 2069, note J. RAVANAS ; *D.* 2005, p. 2651, obs. L. MARINO ; *Dr. fam.* 2004, comm. 172, note V. LARRIBAU-TERNEYRE ; *RTD civ.* 2004, p. 489, obs. J. HAUSER. Par ailleurs, l'infraction prévue à l'article 226-1 du Code pénal punit les formes modernes d'espionnage.

[601] Cette publicité peut être médiatique ou non, par ailleurs, sur la distinction entre atteinte à la vie privée (C. civ., art. 9) et diffamation (loi du 29 juillet 1881 sur la liberté de la presse) v. P. KAYSER, « Diffamation et atteinte au respect de la vie privée », *in Etudes offertes à A. Jauffret*, PUAM, 1974, p. 409.

d'agir en réparation de l'atteinte au respect du secret de la vie privée ou du respect de la liberté de la vie privée. Spécifiquement, le droit au respect du secret de la vie privée comprend le pouvoir de s'opposer aux investigations de la vie privée ainsi que celui de s'opposer aux divulgations de la vie privée. Cette dichotomie des prérogatives a été principalement développée par Pierre Kayser[602]. Si leur objet – la vie privée – paraît difficile, voire impossible à définir dans son contenu[603], la doctrine s'est efforcée d'en déterminer le cœur.

114. Vie privée et intimité de la vie privée. Soucieuse de simplifier et de systématiser le contenu de la vie privée, la doctrine a souvent eu recours à des images, notamment pour définir l'intimité de la vie privée. Celle-ci serait une « *zone privilégiée de paix, de secret et de tranquillité* »[604], son *noyau*[605]. La métaphore des *cercles concentriques* a parfois été évoquée pour tenter de catégoriser les éléments entrant dans la vie privée. Dans une telle conception[606], l'intimité de la personne serait le cercle le plus proche du centre de la vie privée[607]. Dès lors,

---

[602] « *Il résulte de la finalité de ce droit qu'il comporte le pouvoir de s'opposer à la divulgation de la vie privée et celui de s'opposer à une investigation de celle-ci* » (P. KAYSER, « Les droit de la personnalité. Aspects théoriques et pratiques », *RTD civ.* 1970, p. 445).

[603] Sur l'ensemble des propositions doctrinales, leurs lacunes et leurs apports, v. A. LEPAGE, *Rép. civ. V°* « Personnalité (Droits de la) », 2009, (mise à jour nov. 2017), n° 61 et svt. L'impossible définition abstraite du contenu de la vie privée explique l'importance de la construction jurisprudentielle en la matière, d'ailleurs exprimée par un auteur : « *Il paraît impossible, d'un mot, d'une formule, de dire à l'avance où finit la vie privée, où commence la vie publique. Il semble bien que cette question sera toujours dans la dépendance de l'appréciation souveraine des tribunaux* » (L. MARTIN, « Le secret de la vie privée », *RTD civ.* 1959, p. 227, spéc. p. 230) ; *Adde* J.-L. HALPÉRIN, « L'essor de la "privacy" et l'usage des concepts juridiques », *Droit et Société* 2005, n° 61, p. 765 et svt., spéc. p. 778 : « *Nous sommes ainsi ramenés à l'impossibilité de définir la* privacy *autrement que par une collection, une combinaison de droits ou d'intérêts protégés, comme l'ont fait beaucoup d'auteurs et l'Assemblée du Conseil de l'Europe dans sa résolution 428 en 1970. Selon cette résolution, le droit à la* privacy *est «* le droit de mener sa vie comme on l'entend avec un minimum d'ingérences. Il concerne la vie privée, familiale, et le domicile, l'intégrité physique et morale, l'honneur et la réputation, la protection contre la diffusion d'une image fausse, l'interdiction de révéler des faits non pertinents ou embarrassants, la publication non autorisée de photographies privées, la protection contre la divulgation des renseignements donnés ou reçus par un individu de manière confidentielle *». Cette méthode, consistant à cataloguer des domaines concernés par la privacy, prouve l'impossibilité de réduire ce concept à un ou plusieurs critères cohérents et d'en donner une définition en termes de contenu* ».

[604] J. RAVANAS, *JCl. Civil Code,* art. 9, Fasc. 20 : « Jouissance des droits civils. – Protection de la vie privée – Délimitation de la protection », n° 19 (ancienne version du fascicule).

[605] Par exemple, v. G. LEVASSEUR, « La protection pénale de la vie privée », *in Etudes offertes à Pierre Kayser*, t. 2, PUAM, 1979, spéc. p. 114.

[606] Qui a pu être jugée trop complexe et impropre : v. J.-L. HALPÉRIN, « L'essor de la "privacy" et l'usage des concepts juridiques *», op. cit*., p. 765.

[607] « […] *il existe certainement dans la vie privée divers domaines formant des cercles concentriques, et l'intimité de la vie privée se situe davantage vers le centre que près de la périphérie, même si elle ne constitue pas le "noyau irréductible* » (G. LEVASSEUR, « La protection pénale de la vie privée », *in Etudes offertes à Pierre Kayser*, *op. cit.*, p. 114).

comme le souligne Monsieurs Ravanas : « *la vie sentimentale, conjugale et familiale est le siège privilégié des secrets de la personne* »[608]. Ces propos font écho à la polysémie du mot *secret* : *les* secrets de la personne sont sa sphère d'intimité – *Geheimsphäre* selon l'expression allemande –, tandis que le droit au respect du secret de la vie privée désigne les prérogatives dont dispose la personne pour se protéger de la curiosité des tiers. Ainsi, le droit au respect de *l'intimité* de la vie privée consiste notamment dans une prérogative d'opposition à des investigations relatives à *l'intimité* de la vie privée et dans celle de s'opposer à la divulgation de celle-ci.

115. L'intimité de la vie privée et les informations relatives à l'état de santé. Outre le respect de la liberté de la vie privée, la seconde prérogative porte sur des informations. Le critère de définition des informations appartenant à l'intimité de la vie privée est complexe à déterminer. L'utilisation de deux termes, intimité de la vie privée et vie privée, laisse supposer que d'autres informations que celles relatives à l'intimité pourraient être l'objet d'une prérogative. L'identité[609] peut également être l'objet d'un droit au respect du secret, de même que certaines autres informations qui ne font pas partie de l'intimité mais pour lesquelles la jurisprudence a reconnu la protection instituée par l'article 9 du Code civil. Ainsi en est-il des correspondances[610], de l'image[611] ou de la voix[612]. Cette protection s'est révélée nécessaire en raison, ici encore, du support rendant l'information accessible, mais aussi de la possibilité de fixer l'image ou la voix. Au-delà de toute dispute doctrinale relative aux critères abstraits de définition[613], et en admettant que l'intimité de la vie privée a été suffisamment définie par la jurisprudence, l'on peut soutenir que font partie de l'intimité de la vie privée, les informations

---

[608] J. RAVANAS, *Jcl. Civil Code*, Art. 9, Fasc. 10 (ancienne version), n° 40.
[609] Pour ne prendre que l'exemple de la santé, le droit d'accoucher « sous X » constitue une liberté et un droit d'opposition et permet de conserver l'anonymat. Sur la notion d'anonymat v. J.-C. SAINT-PAU, *L'anonymat et le droit*, th. dact. ss. la dir. de P. CONTE, soutenue en 1998, Université Bordeaux IV ; J.-C. SAINT-PAU, « Le droit au respect de la vie privée », *in* J.-C. SAINT PAU (ss. la dir.), *Droits de la personnalité*, *op. cit.*, n° 1173.
[610] Nous avons développé ce point sous l'angle de la protection des supports de l'information : v. *supra* n° 71.
[611] Sur cette construction jurisprudentielle v. A. LEPAGE, *Rép. civ.*, *V°* « Droits de la personnalité – De certains droits de la personnalité en particulier », sept. 2009 (mise à jour juill. 2019), n° 119.
[612] *Ibid.*
[613] Pour un panorama des propositions doctrinales sur le sujet, v. A. LEPAGE, « Personnalité (Droits de la) », *op. cit.*, n° 62 à 66, et n° 70 : « […] *il faut souligner que la jurisprudence témoigne de la diversité des informations protégées, laquelle s'apprécie à un moment donné de l'état de la jurisprudence. Sous un angle diachronique, permettant, avec la prise d'un certain recul, de faire apparaître les évolutions de la jurisprudence, cette diversité se double d'une variabilité des informations protégées, ce qui ne saurait surprendre. Le contenu de la vie privée est loin d'être une sphère figée, c'est une notion qui évolue en symbiose avec la société dans laquelle elle se développe* ».

relatives à la vie affective et familiale[614], à l'intimité spirituelle et morale[615], ainsi qu'à l'intimité corporelle[616]. S'agissant des informations relatives à l'intimité corporelle, le droit au respect du secret s'étend à l'image du corps[617], aux informations génétiques[618] ainsi qu'à celles relatives à l'intimité sexuelle et aux mœurs[619], mais également aux informations relatives à la santé. Ainsi, le secret des informations relatives à la santé est également assuré par les prérogatives attachées au respect du secret de la vie privée. Encore faut-il apprécier la portée de ce secret.

116. Portée de la protection du secret des informations relatives à la santé par l'article 9 du Code civil. La dichotomie mise en lumière par Pierre Kayser relative aux deux types de prérogatives permettant de faire respecter le secret de la vie privée, s'applique aux informations relatives à la santé : il faut distinguer le pouvoir de s'opposer à des investigations tendant à réunir celles-ci et le pouvoir de s'opposer à leur divulgation. S'agissant du pouvoir de s'opposer à des investigations, il a été jugé que la chambre d'hôpital était un lieu privé[620] , ce qui a rendu possibles des poursuites pénales sur le fondement de l'article 226-1 du Code pénal punissant le

---

[614] Entre autres : TGI Paris, 2 juin 1976, *D*. 1977, p. 364, 2ème esp., note R. LINDON. La divulgation d'une liaison est constitutive d'une atteinte à la vie privée (TGI Paris, 8 juill. 1970, *JCP G* 1970, II, 16550, note R. LINDON ; TGI Nanterre, 12 déc. 2000, *Légipresse* 2001, I, p. 45 ; Civ. 2ème, 24 avr. 2003, n° 01-01186, *Bull. civ*. II, n° 114 ; *Dr. et patr.* juill.-août 2003, p. 86, obs. G. LOISEAU ; TGI Nanterre, 1re ch., 28 avr. 2011, *Légipresse* juin 2011, p. 341), de même en est-il de la révélation d'informations concernant des fiançailles ou un mariage (Paris, 21 déc. 1970, *JCP G* 1971, II, 16653, note R. LINDON ; TGI Paris, 3 juill. 1971, *D.* 1972, somm. p. 47 ; Civ. 2ème, 7 janv. 1976, *Bull. civ*. II, n° 3 ; Civ. 2ème, 7 janv. 1976, *Bull. civ*. II, n° 3 ; Civ. 2ème, 18 mars 2004, n° 02-13529 ; TGI Paris, 9 févr. 2005, *Légipresse* 2005, I, p. 54 ; TGI Nanterre, 20 juin 2005, *Légipresse* 2005, I, p. 127), un concubinage (Civ. 1re, 6 oct. 1998, n° 96-13600 ; *D.* 1999, somm. p. 376, obs. J.-J. LEMOULAND ; *RTD civ.* 1999, p. 62, obs. J. HAUSER). Pour une liste complète des décisions portant sur des atteintes à l'intimité sentimentale et familiale, v. J.-C. SAINT-PAU, « Le droit au respect de la vie privée », *op. cit.*, n° 1200 et svt. ; A. LEPAGE, « Personnalité (Droits de la) », *op. cit.*, n° 71.

[615] Sur l'autonomie de la conscience v. D. LAZLO-FENOUILLET, *La conscience*, préf. G. CORNU, coll. Bibliothèque de droit privé, t. 235, LGDJ, 1993, n° 849 ; *Adde* J.-C. SAINT-PAU, « Le droit au respect de la vie privée », *op. cit.*, n° 1197 à 1199, A. LEPAGE, « Personnalité (Droits de la) », *op. cit.*, n° 79.

[616] J.-C. SAINT-PAU, « Le droit au respect de la vie privée », *op. cit.*, n° 1189.

[617] *Ibid.,* n° 1190.

[618] L'étude des caractéristiques génétiques et l'identification des personnes par leurs empreintes génétiques sont encadrées par des dispositions spécifiques (C. civ., art. 16-10 et 16-13). Certains auteurs considèrent toutefois que l'information génétique est une information relative à la vie privée. En ce sens, v. F. TERRE et D. FENOUILLET, *Droit civil. Les personnes, la famille, les incapacités,* 8ème éd., coll. Précis, Dalloz, 2012, n° 105 ; J.-C. SAINT-PAU, « Le droit au respect de la vie privée », *op. cit.*, n° 1191.

[619] Par exemple : Grenoble, 30 oct. 2000, *JurisData* : n° 2000-146355 concernant une condamnation pour révélation de l'homosexualité d'un individu ; Paris, 11ème ch. B, 21 oct. 2004, *JurisData* : 2004-253278, *Comm. com. électr.* 2005, comm. 48, obs. A. LEPAGE.

[620] Paris, 11ème ch. corr., 17 mars 1986 ; Sur l'accès des tiers à l'établissement de santé et les pouvoirs du directeur d'établissement, v. C. BERGOIGNAN-ESPER et M. DUPONT, *Droit hospitalier*, 10ème éd., coll. Cours, Dalloz, 2017, n° 924 et svt.

fait de capter, d'enregistrer ou de transmettre l'image ou la voix d'une personne dans un lieu privé sans l'autorisation de celle-ci[621]. Une telle qualification permet également de poursuivre la personne qui pénètrerait dans la chambre d'un malade sans y avoir été autorisée, sur le fondement de l'article 226-4 du Code pénal punissant la violation de domicile[622]. Quant au pouvoir de s'opposer à la divulgation de l'état de santé, la jurisprudence civile est prolixe. Il a ainsi pu être jugé que constituait une atteinte à l'intimité de la vie privée le fait de révéler une possible maladie héréditaire[623], mais également toute révélation portant sur les maladies physiques[624] ou psychiques[625] et même les informations relevant indirectement de la santé telles que le fait d'avoir recours à la chirurgie esthétique[626]. Aussi l'état de santé, élément de l'intimité de la vie privée, est-il l'un des objets du secret de la vie privée. La révélation d'une information ne peut constituer une atteinte à la vie privée que lorsqu'elle désigne une personne identifiable. L'identité est alors un élément qui conditionne l'existence d'une atteinte à la vie privée. Elle peut aussi être un élément de la vie privée protégé au titre du droit au respect de l'anonymat. Il faut alors distinguer ce droit à l'anonymat de l'identification de la personne, condition de l'atteinte.

2 - Les informations concernant le patient et l'identité

117. Identité, liberté de demeurer anonyme. L'identité fait partie de la vie privée dans son acception doctrinale la plus large. Par ailleurs, la Cour européenne des droits de l'homme a défini le droit au respect de la vie privée comme le « *droit à un développement personnel et le droit d'établir des rapports avec d'autres êtres humains et le monde extérieur* »[627]. Ce droit de

---

[621] CP, art. 226-1, 2°.
[622] H. MATSOPOULOU, *Jcl. Pénal Code*, fasc. 20 : « Violation de domicile », 2009 (mise à jour sept. 2016).
[623] Versailles, 16 janv. 2003, *Légipresse* 2003, I, p. 106.
[624] Civ. 2ème, 12 juill. 1966, *D.* 1967, p. 181, note P. MIMIN ; Paris, 9 juill. 1980, *D.* 1981, p. 72, 2ème esp., note R. LINDON ; Civ. 1re, 6 juin 1987, *Bull. civ.* I, n° 191 ; Paris, 26 juin 1986, *D.* 1987, Somm. p. 136 ; TGI Paris, 20 nov. 1985, *D.* 1987. Somm. p. 140 ; 17 déc. 1986, *Gaz. Pal.* 1988, 1, Somm. p. 145 ; CEDH, 6 févr. 2001, *JCP G* 2001, I, 342, obs. F. SUDRE ; TGI Paris, 5 mars 2007, *Légipresse* 2007, I, p. 162 ; TGI Nanterre, 4 avr. 2005, *Légipresse* 2005, I, p.145. La question s'est parfois posée s'agissant de maladies tel que le VIH. Si le fait qu'une personne soit atteinte du VIH ne constitue pas un fait justificatif permettant au médecin d'avertir le ou la partenaire du malade, la divulgation par un tiers porte atteinte à la vie privée du malade (Paris, 24 sept. 1990, *JurisData* : n° 023624).
[625] Paris, 5 déc. 1997, *D.* 1998, IR p. 32.
[626] TGI Paris, 20 juin 1973, *D.* 1974, p. 766, note R. LINDON.
[627] V. par exemple : CEDH, sect. II, 14 mai 2002, *Zehnalova et Zehnal c/ République tchèque*, n° 38621/97 ; CEDH, 22 févr. 1994, *Burghartz c/ Suisse*, série A n° 280-B, p. 37, § 47 ; CEDH, 31 janv. 1995, *Friedl c/ Autriche*, série A n° 305-B, avis de la Commission, p. 20, § 45. ; CEDH, 8 janv. 2009, *Schlumpf c/ Suisse*, n° 29002/06, § 77.

nouer des rapports aux autres, conçu négativement, consiste dans la liberté de ne pas nouer de tels rapports. Bien qu'elle soit spécifiquement protégée par les dispositions encadrant le traitement des données à caractère personnel, l'identité relèverait également de la vie privée dans la mesure où la révélation de l'identité conditionne l'atteinte à l'intimité de la vie privée. Par ailleurs, l'identité est également protégée par un *droit à l'anonymat*. Celui-ci ne se confond pas avec le droit au respect du secret de la vie privée dès lors que les prérogatives qui découlent de ce dernier consistent, comme il l'a été rappelé, en un pouvoir de s'opposer à des investigations ou des révélations. Le droit à l'anonymat s'analyse comme la possibilité de garder le secret sur son identité dans certaines situations[628]. Une personne a, par exemple, le droit au respect de son anonymat dans le cadre de son admission dans un service hospitalier ou lors de l'accouchement[629]. Mais l'anonymat est également une liberté « *de comportement anonyme dès lors que les principes d'identification permanente et ponctuelle sont respectés* »[630] et encore « *une liberté de créer certaines situations juridiques d'anonymat dans la vie extrapatrimoniale* »[631]. Il ne faut toutefois pas confondre le droit à l'anonymat avec l'anonymisation, technique permettant de retirer à une information tout caractère identifiant.

118. Identité, identification et atteinte à l'intimité de la vie privée. Il est largement admis que le secret de la vie privée porte sur un ensemble d'informations personnelles[632]. Pour être personnelle, une information doit nécessairement se rapporter à un individu, qu'elle l'identifie ou permette son identification. Révéler que l'on connaît quelqu'un atteint du diabète ne

---

[628] Dans la société contemporaine, la liberté de demeurer anonyme est inévitablement réduite par les règles d'identification permanentes qui caractérisent particulièrement le système de santé. Ainsi, la liberté de conserver son anonymat est mise en balance avec les « *impératifs administratifs* » (J.-C. SAINT-PAU, *L'anonymat et le droit,* th. dact. ss. la dir. de P. CONTE, soutenue en 1998, Université Bordeaux IV, n° 865) que le domaine de la santé connaît particulièrement puisque le remboursement des soins est par exemple conditionné par l'impératif de révéler son identité aux soignants ainsi qu'aux organismes de sécurité sociale.

[629] *Ibid.,* n° 590 et svt ; C'est le cas pour les personnes toxicomanes (CSP, art. R. 1112-38), comme pour les accouchements dits « sous X ». En effet « *Lors de l'accouchement, la mère peut demander que le secret de son admission et que son identité soit préservée* » (C. civ., art. 326).

[630] *Ibid.,* n° 869.

[631] *Ibid.* Au contraire, l'anonymat en matière de don des éléments du corps humain (CSP, art. L. 1211-5) n'est pas un anonymat administratif, c'est-à-dire une liberté de ne pas s'identifier, mais empêche le donneur et le receveur de connaître leurs identités respectives, cet anonymat est imposé par le législateur.

[632] D. GUTMANN, *Le sentiment d'identité*, préf. F. TERRE, coll. Bibliothèque de droit privé, t. 327, LGDJ, 2000, n° 259 et svt. ; *Adde* J. ROBERT avec la collaboration de J. DUFFAR, *Libertés publiques et droits de l'Homme*, coll. Domat, Montchrestien, 1988, p. 299 ; J. PRADEL, « Les dispositions de la loi du 17 juillet 1970 sur la protection de la vie privée », *D.* 1971, p. 3, n° 7 ; J.-C. SAINT-PAU « Le droit au respect de la vie privée », *op. cit.*, n° 1171.

constitue pas une atteinte à la vie privée dès lors qu'il est impossible de savoir sur qui porte cette information intime. Par contre, révéler que le voisin qui habite au dernier étage et occupe un poste à la mairie est atteint d'un cancer, constitue une atteinte au secret de la vie privée de ce dernier dès lors qu'il est *identifiabl*e. Si son nom est révélé en même temps que sa maladie, alors il est *identifié*. Ce n'est pas l'identité de la personne qui est protégée mais « *l'anonymat de l'intimité* »[633] car, comme le remarque Monsieur Saint-Pau : « *Le droit au respect de l'intimité de la vie privée se définit en effet comme le pouvoir de garder l'anonymat* […] *une atteinte à l'intimité emporte toujours une atteinte à l'anonymat car on ne saurait concevoir d'atteinte à l'intimité sans identification de la personne en cause* […] *chacun dispose du droit à la non identification de sa vie intime* »[634]. Ainsi, le droit au secret des informations relatives à la santé impose nécessairement que soit respecté l'anonymat de cette intimité. En ce sens, l'identité n'est pas objet du droit subjectif mais constitue une condition d'exercice de ce droit. En d'autres termes, la condition porte sur le régime de l'action et non plus sur l'aspect conceptuel de la vie privée : l'atteinte à la vie privée suppose de déterminer le sujet passif du droit subjectif, ce qui n'est possible que lorsque l'individu est identifié ou identifiable. Il s'agit à la fois d'une condition de l'atteinte et d'une condition de l'exercice du droit subjectif. Si les exemples jurisprudentiels concernent le plus souvent l'image des personnes[635], la condition relative à l'identification vaut peu importe l'objet de l'atteinte, qu'il concerne des informations ou des images.

B - Le régime de l'atteinte à la vie privée

119. L'atteinte à la vie privée justifiée par le consentement. Toute révélation d'une information relative à l'intimité de la vie privée ne constitue pas nécessairement une atteinte permettant la mise en œuvre des prérogatives attachées au droit subjectif, encore faut-il que cette révélation soit illicite. Cette condition d'illicéité de l'atteinte se détermine par le consentement du titulaire du droit à ce qu'il soit porté atteinte à sa vie privée. Cette autorisation

---

633 J.-C. SAINT-PAU, *L'anonymat et le droit*, *op. cit.*, n° 870.
634 *Ibid*.
635 Paris, 1re ch. section A, 17 déc. 1991, *JurisData* : n° 1991-024673 à propos de photographie d'un accouchement sous l'eau : même si le visage des personnes est dissimulé, les personnes étaient « *aisément identifiables* » en raison du contexte ; Civ. 1re, 9 avr. 2014, n° 12-29588, *Bull. civ.* I, n° 167 ; *Comm. Com. Electr.* 2014, comm. 57, obs. A. LEPAGE, s'agissant d'une photo diffusée par courriel représentant un orteil de nourrisson, élément qui ne permettait pas d'identifier l'enfant de sorte que sa diffusion ne pouvait constituer une atteinte à la vie privée.

constitue une limite à l'indisponibilité du droit à la protection de la vie privée, et plus largement des droits extrapatrimoniaux[636]. Concernant les informations relatives à la santé des personnes, et donc à l'intimité de leur vie privée, quand bien même il s'agirait d'informations couvertes par le secret professionnel, cette condition est également nécessaire. L'abus de ce droit peut être contrôlé[637] par le juge. Ainsi, dans les décisions évoquées précédemment à propos de l'existence d'une prétendue *renonciation au secret médical*, le juge a opéré une *balance* avec d'autres intérêts légitimes[638] au regard du droit au respect du secret de la vie privée.

120. La balance des intérêts et le secret des informations relatives à la santé. La question de la justification des atteintes à l'intimité de la vie privée, et particulièrement de la santé des personnes, se pose souvent dans le contexte des relations de travail. Il s'agit alors de fixer les limites des investigations que peut entreprendre l'employeur pour connaître des informations relatives à la santé des salariés. Le conflit le plus prégnant demeure celui entre la vie privée et la liberté d'expression et le droit à l'information. A propos des informations relatives à la santé, la question de la balance entre ces libertés et le droit au respect du secret de la vie privée s'est posée avec acuité pour la santé des personnes publiques[639]. Elle trouve encore une illustration particulière dans l'affaire du sang contaminé s'agissant de la publicité des débats en matière correctionnelle. A cette occasion, la Cour d'appel de Paris a déclaré que « *les dispositions de l'article 9 du Code civil relatif à la protection de la vie privée ne peuvent faire obstacle au principe de la publicité des débats judiciaires en matière correctionnel*le »[640]. La relativité caractérise les droits subjectifs puisque « *entre droits subjectifs, loin de l'impératif, la discussion est naturelle* »[641] et celle-ci se prolonge en matière pénale. La disponibilité de la

---

[636] G. CORNU, *Droit civil. Les personnes*, 13ème éd., coll. Domat droit privé, Montchrestien, 2007, n° 36.
[637] Les droits de la personnalité entrent dans la catégorie des droits dits « contrôlés » par opposition aux droits discrétionnaires (A. ROUAST, « Les droits discrétionnaires et les droits contrôlés », *RTD civ.* 1944, p. 1).
[638] C. CARON, « Brèves observations sur l'abus des droits de la personnalité », *Gaz. Pal.* 18-19 mai 2007, p. 47.
[639] La question du secret de l'état de santé des dirigeants est traditionnellement illustrée par l'affaire *Gubler,* relative à la publication de l'ouvrage relative à la maladie d'un ancien Président de la République. La publication avait été interdite et constituait, outre l'atteinte à la vie privée de la famille du défunt (le Président étant décédé au moment de la publication), une violation du secret professionnel. Au-delà de ce cas d'espèce, la légitimité d'informer le public à propos de tels sujets a pu être posée : « *La santé d'un chef d'état fait-elle encore partie de sa vie privée ?* » (J. RAVANAS, *Jcl. Civil Code*, art. 9, Fasc. 10 (ancien fascicule), n° 100).
[640] Paris, 1re ch. A, 24 mai 1994, *JurisData*, n° 022205.
[641] J. CARBONNIER, *Droit et passion du droit sous la Ve République,* coll. Champs essais, Flammarion, 2008, p. 126.

valeur sociale qu'est la vie privée se traduit dans la structure de l'infraction[642], qui se trouve anéantie par le consentement de la victime dont l'absence est un élément constitutif[643].

Les informations couvertes par le secret professionnel dans le domaine de la santé sont également des informations relatives à la vie privée. Le pouvoir accordé aux individus d'exiger le respect du secret de leur vie privée couvre donc également le secret des informations issues de la relation de soin. Si une telle affirmation semble relever de l'évidence, l'emploi de l'expression « secret médical » dans la jurisprudence relative au contrat d'assurance invitait à revenir sur cette question. Cette mise au point effectuée, il convient d'envisager les dispositifs techniques comme moyen d'atteinte au secret de la vie privée et donc au secret des informations relatives aux personnes prises en charge par un professionnel intervenant dans le système de santé.

§ 2 - La fixation ou la captation illicite de l'information secrète

121. L'idée selon laquelle les dispositifs techniques facilitent la commission de certaines infractions portant atteinte aux personnes n'est pas neuve. Madame Lepage constate ainsi « *l'originalité* ou […] *la force de nuisance du phénomène criminel que permet ou favorise l'internet* »[644]. Si l'utilisation des dispositifs techniques de l'information formant l'informatique engendre une désolidarisation des informations et de leur support, d'autres dispositifs peuvent pemettre de fixer et capter les informations à distance tandis que l'internet facilite leur communication à grande échelle. Le droit pénal s'est saisi de certains dispositifs facilitant l'intrusion dans la vie privée des personnes, des infractions ayant été spécifiquement érigées pour en sanctionner l'utilisation. Aussi, les agissements pénalement sanctionnés ont-ils une coloration technologique : ce sont les procédés utilisés pour porter atteinte à la vie privée qui justifient la répression. La protection offerte par l'article 226-1 du Code pénal ainsi que par les infractions obstacles et conséquences de celle-ci, concerne *l'espionnage audiovisuel*. S'il s'agit de sanctionner la captation, l'enregistrement ou la transmission de parole ou d'image, c'est

---

642 Il ne s'agit ici que d'infractions sanctionnant une atteinte à la vie privée (CP, art. 226-1 et svt.).
643 X. PIN, *Le consentement en matière pénale*, préf. P. MAISTRE DU CHAMBON, coll. Bibliothèques des sciences criminelles, t. 36, LGDJ, 2002, n° 60 et svt., spéc. n° 64.
644 Traitant spécifiquement de l'internet mais dont les propos peuvent être transposés à l'évolution des dispositifs techniques en général : A. LEPAGE, « Droit pénal et internet : la part de la tradition, l'oeuvre de l'innovation », *AJ pénal* 2005, p. 217.

toujours l'information[645] qui est l'objet de l'infraction et qui, partant, représente la valeur sociale protégée. Plus que l'intrusion dans la sphère intime de la vie privée, le fait pénalement sanctionné est celui consistant à procéder, de manière illicite, à la représentation des paroles ou à la fixation d'une image, ces deux actions pouvant donner lieu à la communication des informations représentées. Ces infractions peuvent ainsi avoir pour objet le « secret médical » objet juridiquement protégé. C'est-à-dire les informations couvertes par le secret professionnel **(A)**. La communication de l'objet du délit à des tiers constituant une infraction spécifique **(B)**.

A - Les investigations pénalement sanctionnées, un rempart contre la technique

122. L'infraction principale, le délit d'espionnage audiovisuel. Certaines atteintes à la vie privée, particulièrement graves du fait de l'usage de dispositifs techniques, sont pénalement sanctionnées aux articles 226-1 à 226-7 du Code pénal. Le délit prévu à l'article 226-1 peut être considéré comme le principal délit définissant et sanctionnant l'atteinte à la vie privée par ces moyens, puisque les textes d'incrimination qui lui font suite consistent en un délit-obstacle à cette infraction et en une infraction sanctionnant l'utilisation des informations obtenues suite à l'immixtion dans l'intimité de la vie privée[646]. L'infraction principale punit l'espionnage, uniquement par le biais de moyens techniques. Les termes volontairement larges employés pour définir l'élément matériel de l'infraction permettent de caractériser celle-ci indépendamment des évolutions de la technique[647]. La loi du 17 juillet 1970 créant cette infraction visait, à l'époque, des techniques d'espionnage sans commune mesure avec les moyens issus du rapprochement entre les dispositifs de l'information et de la communication à l'ère de l'internet[648]. La rédaction du texte d'incrimination a toutefois permis que le délit puisse être caractérisé alors que ces moyens se sont diversifiés et sont devenus plus efficaces et moins

---

[645] Qu'il s'agisse de capter des informations transmises oralement ou de fixer une situation pour produire une image, dès lors que l'information est définie comme un « *élément de connaissance susceptibles d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué* » (Arrêté du 22 déc. 1981 relatif à l'enrichissement du vocabulaire de l'informatique, *JOLD complémentaire*, 17 janv. 1982, p. 624) ou encore comme un « *renseignement ou élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement* » (Arrêté du 10 nov. 1984 portant enrichissement du vocabulaire des télécommunications, *JOLD complémentaire*, 10 nov. 1984, p. 10262).

[646] H. MATSOPOULOU et A. LEPAGE, *Droit pénal spécial*, coll. Thémis droit, PUF, 2015, n° 520.

[647] Si l'élément matériel a une coloration technique, les termes utilisés sont suffisamment neutres pour répondre à ces évolutions.

[648] Dans le même sens v. J. PRADEL et M. DANTI-JUAN, *Droit pénal spécial*, 7ème éd., coll. Référence, Cujas, 2017, n° 243.

visibles. La limite du champ d'application de l'infraction ne se trouve donc pas tant dans les moyens employés que dans leur objet : la parole et l'image. L'article 226-1 du Code pénal dispose en effet qu'est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, « *au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui : 1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privée ou confidentiel* ». Il en est de même pour l'image de la personne, l'adverbe « captant » étant remplacé par « fixant ». Cette infraction intéresse notre propos dans la mesure où elle s'applique nécessairement au secret des informations relatives à la santé qui sont, par ailleurs, couvertes par le secret professionnel. Son étude nous permet, surtout, de constater que l'expression « secret médical » est parfois utilisée par le juge lorsqu'il sanctionne une telle atteinte, ce qui confirme notre hypothèse selon laquelle le « secret médical » est entendu comme la protection des informations couvertes par le secret professionnel dans le domaine de la santé lorsque celles-ci sont représentées.

123. Du lieu privé aux paroles prononcées à titre confidentiel. L'intimité de la vie privée n'est pas délimitée par le lieu dans lequel sont captés les propos et les images mais par le caractère confidentiel de ces derniers. Si l'article 368 de l'ancien Code pénal posait comme élément constitutif de l'infraction le fait que l'image ou la voix soit captée dans un lieu privé, la modification apportée lors de la réforme du Code pénal a permis d'ajouter les paroles prononcées à titre confidentiel[649]. Sont des paroles prononcées à titre confidentiel celles échangées lors d'une consultation avec un professionnel de santé. Dès lors, tout système d'espionnage installé dans un cabinet médical, une salle d'attente et*, a fortiori*, dans une chambre d'hôpital, est susceptible de capter des informations couvertes par le secret. Il est, à cet égard, intéressant d'évoquer une affaire dans laquelle un dictaphone avait été installé par un dentiste dans le cabinet d'un confrère pour enregistrer ses conversations[650]. A l'occasion du pourvoi, le demandeur a, entre autres moyens, soutenu que les propos échangés dans le cabinet d'un professionnel de santé étaient « par nature confidentiels et couverts par le secret médical ». Outre l'emploi de l'expression « secret médical », on comprend que les informations couvertes par le secret professionnel sont *par nature* des propos confidentiels au regard du texte de l'article 226-1. Quand bien même le système installé n'aurait pas permis la captation de telles

[649] J. PRADEL et M. DANTI-JUAN, *Droit pénal spécial*, *op. cit.*, n° 248.
[650] Crim., 15 févr. 2011, n° 10-82808 ; *D.* 2012, pan. p. 765, obs. E. DREYER.

informations, la tentative d'atteinte à la vie privée est punie, comme le prévoit l'article 226-5[651]. Ce point mérite quelques commentaires.

124. Consommation de l'infraction et atteinte à la vie privée. L'article 226-1 vise le fait de porter atteinte à la vie privée, précision qui a amené les auteurs à s'interroger sur les conséquences de la structure de l'infraction. Soit le délit est consommé dès lors que l'espionnage a abouti au résultat visé, c'est-à-dire une atteinte à l'intimité ; soit le délit est constitué lorsque les actes d'espionnage sont réalisés, indépendamment du résultat et, dans ce cas, « *la preuve de l'obtention du résultat redouté n'a pas à être rapportée* »[652]. La question est alors de savoir s'il s'agit d'une infraction matérielle ou d'une infraction formelle[653]. Elle semble avoir été réglée dans l'arrêt évoqué : « *tout en admettant que la preuve d'une telle atteinte doit être rapportée pour que l'infraction soit consommée, la haute juridiction admet que l'auteur des actes d'espionnage engageait sa responsabilité pénale sur le fondement de la tentative, car de tels actes auraient pu atteindre le résultat redouté s'ils avaient perduré* »[654]. Il s'agit donc d'une infraction *matérielle*. Le régime de l'infraction ainsi éclairé, il apparaît que le simple fait d'installer un dispositif visant à capter des paroles échangées dans le cadre des soins, entre un professionnel et un malade, s'il ne suffit pas à caractériser l'infraction, permet au moins d'en caractériser la tentative, sans qu'il soit besoin de s'interroger sur la nature des paroles, dès lors qu'elles sont présumées être échangées à titre confidentiel puisque couvertes par le secret professionnel.

B - Une infraction-obstacle et une infraction de conséquence

125. La sanction des actes préparatoires à l'espionnage. L'infraction prévue à l'article 226-3 du Code pénal sanctionne les actes préparatoires à l'espionnage tels que définis par

---

[651] CP, art. 226-5. Dans l'affaire précitée, le demandeur soutenait que « *constitue une tentative du délit d'atteinte à la vie privée la mise en œuvre d'un procédé destiné à enregistrer, sans le consentement de leur auteur, des propos tenus dans le cabinet d'un professionnel de la santé qui,* ***par nature sont confidentiels et couverts par le secret médical*** ». La Cour de cassation accueille le moyen du demandeur au pourvoi et décide que la cour d'appel ne peut conditionner la consommation du délit à l'effectivité de l'atteinte et « *qu'en se déterminant ainsi, sans rechercher si les faits dont elle était saisie ne caractérisaient pas une tentative d'atteinte à la vie privée, également punissable, la cour d'appel a méconnu les textes susvisés (art. 226-1 et 226-5 c. pén.)* ». L'espèce avait notamment un intérêt quant à la question du caractère matériel ou formel de l'infraction inscrite à l'article 226-1 du Code pénal (E. DREYER, « Droit de la presse et droits de la personnalité », *D.* 2012, p. 765).

[652] E. DREYER, *Droit pénal général*, 5ème éd., LexisNexis, 2019, n° 750.

[653] A. DECOCQ*, «* Rapport sur le secret de la vie privé en droit français »*, in Le secret et le Droit,* Travaux de l'association H. Capitant, t. XXV, Dalloz, 1974, p. 467 s., spéc. p. 478 et 479.

[654] E. DREYER, « Droit de la presse et droits de la personnalité », *op. cit.*

l'article 226-1 du même code. En intervenant en amont de l'*iter criminis*, le législateur a entendu restreindre l'accès aux dispositifs techniques d'espionnage auditif et visuel. Le texte vise à sanctionner « *la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques* […] *conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1* ». Le champ de l'incrimination s'étend également aux techniques de cyber-espionnage telles que définies aux articles 706-102-1 du Code de procédure pénale. Sont ainsi visés les dispositifs techniques ayant « *pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels* ». Ces dispositifs sont définis dans une section du Code de procédure pénale portant sur la captation des données informatiques. Le champ de l'infraction s'étend, en outre, aux « *dispositifs techniques de nature à permettre la réalisation d'opérations pouvant constituer l'infraction prévue par le second alinéa de l'article 226-15* »[655]. L'infraction vise donc à prévenir les atteintes au secret de la vie privée ou des informations couvertes par le secret professionnel, mais également à empêcher les atteintes aux biens et les atteintes à l'identité puisque la captation illicite de données personnelles est sanctionnée par des infractions spécifiques. L'article 226-3 du Code pénal est alors une infraction-obstacle protégeant d'autres valeurs sociales que celle protégée à l'article 226-1 du Code pénal.

126. La sanction de l'utilisation de la captation et de la fixation. Une infraction de conséquence. A l'instar du recel, l'infraction définie à l'article 226-2 du Code pénal punit le fait « *de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide d'un des actes prévus par l'article 226-1* ». Cette infraction prévoit donc la sanction d'une révélation, celle du secret de la vie privée. Lorsque des paroles prononcées à titre confidentiel sont captées à l'insu d'un professionnel de santé dans son cabinet et que le contenu des conversations enregistrées ou captées est révélé, les informations objet de la révélation sont également l'objet du délit de violation du secret professionnel. Toutefois, les faits ne sont pas

[655] Ce dernier article sanctionne l'atteinte au secret des correspondances : V. PELTIER, *Le secret des correspondances,* préf. P. CONTE, PUAM, 1999, n° 515.

réprimés au regard de la relation entre le professionnel et le patient mais en conséquence de l'illicéité de l'espionnage. Il n'en demeure pas moins que les infractions prévues aux articles 226-1, 226-2 et 226-3 du Code pénal protégeant la vie privée peuvent avoir pour objet, au travers des attributs de la personnalité que sont l'image et la voix, les informations secrètes concernant la personne prise en charge par un professionnel ou un établissement de santé.

Section 2 - La violation du secret professionnel

127. Nous traiterons ultérieurement des conséquences de l'utilisation des dispositifs de l'information et de la communication – en nous intéressant particulièrement à leur fonction de traitement des données – sur le secret professionnel. Pour l'instant, il importe simplement de constater que les dispositifs techniques de la communcation peuvent constituer des moyens de révélation de l'information à caractère secret. Le texte d'incrimination définissant la violation du secret professionnel bénéficie d'une neutralité technologique qui permet de sanctionner la révélation sans égard au moyen employé **(A)** mais que son champ d'application est limité dans la mesure où il s'agit d'une infraction intentionnelle **(B)**.

§ 1 - La neutralité technologique du texte d'incrimination

128. Neutralité technologique des textes d'incrimination. A propos du droit pénal de l'internet, Madame Lepage remarque que « *Fréquemment, par le jeu de la qualification, un commun dénominateur permet de subsumer l'internet sous des règles qui lui préexistaient et dont la portée le dépasse, mais qui ont bel et bien vocation à l'embrasser au même titre que d'autres objets plus traditionnels* »[656]. Ces propos pourraient tout à fait constituer une définition de l'expression « neutralité technologique des règles juridiques »[657]. De manière générale, les

---

[656] A. LEPAGE, « Droit pénal et internet : la part de la tradition, l'oeuvre de l'innovation », *AJ pénal* 2005, p. 217.
[657] De manière non spécifique à la matière pénale, Monsieur Labbé explique que la technicisation des lois pose un problème de lisibilité, mais semble difficile à éviter dans la mesure où « *la normativité juridique* [est] *indissociable de la réalité qu'elle entend régir* ». Il ajoute : « *A défaut de ne pouvoir (ou vouloir) formuler des lois moins techniques et plus accessibles, les législateurs ont tenté de limiter le nombre de leurs interventions en libellant les textes législatifs de manière à éviter qu'ils ne deviennent rapidement obsolètes sur le plan technique, suivant ainsi le principe des lois dites* « technologiquement neutres » ». L'auteur souligne encore que le législateur a ainsi favorisé des « *normes de résultat* » et des « *définitions finalistes* » (E. LABBE, « L'efficacité technique comme

infractions de droit commun n'ont pas besoin d'être spécifiquement et systématiquement adaptées aux évolutions techniques[658], ce que rappelait d'ailleurs Monsieur Lucas dans une intervention relative à la réception des nouvelles techniques dans la loi[659]. Lorsque les faits incriminés sont visés de façon suffisamment générale, c'est-à-dire en observant « *une saine indifférence à ce qui peut constituer par ailleurs telle ou telle particularité* »[660] de l'objet de l'infraction ou du moyen de commission pour « *ne voir alors en lui que ce qui le fait ressembler à d'autres objets dont se saisit le droit pénal* »[661], la souplesse du texte lui permettra d'être appliqué, peu importe le contexte technologique.

129. Neutralité technologique du texte d'incrimination définissant la violation du secret professionnel. La violation du secret professionnel suppose, au regard de l'article 226-13 du Code pénal, la révélation d'une information à caractère secret par une personne qui en est dépositaire. Nous ne nous intéresserons, dans ce developpement, qu'à l'objet de l'infraction et à ses modalités constitutives. Il s'agit de confirmer que la violation du secret professionnel peut être constituée indifféremment des évolutions techniques et notamment de la commission de l'infraction sur l'internet. Il a, en effet, été relevé que l'utilisation de l'internet facilitait la violation du secret professionnel[662]. Par ailleurs, le Conseil national de l'Ordre des médecins s'est appliqué, ces dernières années, à rappeler les bons comportements que doivent avoir les professionnels de santé lorsqu'ils ont une activité en ligne en lien avec leur profession et

---

critère juridique ou la manière dont les lois se technicisent », *Lex-Electonica* 2004, 9-2 (disponible en ligne sur : <https://www.lex-electronica.org/s/774>).

[658] Bien qu'il soit vrai que le législateur veille à modifier de manière régulière les textes qui le nécessitent puisque le principe de légalité criminelle fait obstacle aux adaptations prétoriennes qui seraient trop éloignées de la lettre du texte d'incrimination : « *L'innovation technologique rend nécessaire une adaptation permanente de la loi pénale aux évolutions techniques qu'imposent tant le principe de légalité édicté par les articles 111-3 du Code pénal et 7 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, que celui d'interprétation stricte de la loi pénale, dont il constitue le prolongement naturel, tel qu'il est énoncé à l'article 111-4 du Code pénal* » (Cour de Cassation, *Rapport annuel 2005. L'innovation technologique*, La documentation française, p. 93).

[659] Intervention présentée le 26 octobre 2000 dans le cadre du cycle de conférences *Le lisible et l'illisible* organisé par le Centre de recherche en droit public et la Faculté de droit de l'Université de Montréal. Le texte est disponible en ligne sur <www.juriscom.net> : A. LUCAS, « La réception des nouvelles techniques dans la loi, l'exemple de la propriété intellectuelle » ; *Adde* E. LABBE, « L'efficacité technique comme critère juridique ou la manière dont les lois se technicisent », *op. cit.*.

[660] A. LEPAGE, « Droit pénal et internet : la part de la tradition, l'oeuvre de l'innovation », *op. cit.*

[661] *Ibid.*

[662] *Ibid.*

concernant les informations qu'ils diffusent sur les médias sociaux[663]. Il nous semble toutefois que l'affirmation selon laquelle la réalisation de l'infraction de violation du secret professionnel serait *facilitée* par l'internet ou tout autre dispositif technique est critiquable. Il n'est pas plus aisé de divulguer oralement une information que, par exemple, sur les réseaux sociaux. La seule question qui puisse éventuellement apparaître concerne les moyens de la révélation.

130. Indifférence quant aux moyens de révélation. Le texte de l'article 226-13 sanctionne la révélation d'une information à caractère secret. Comme le souligne Monsieur Mistretta, le terme « révélation » est suffisamment large pour « *sanctionner toute forme d'indiscrétion* »[664]. L'infraction s'applique donc aux révélations commises par le truchement des dispositifs techniques de l'information et de la communication, et notamment l'internet. Les décisions de première instance étant peu publiées, nous n'avons connaissance d'aucune condamnation de professionnels de santé ayant été poursuivis sur le fondement de l'article 226-13 du Code pénal pour des révélations commises, par exemple, sur internet[665]. Encore peut-on préciser qu'il suffit que la révélation ne soit faite qu'à une seule personne. En effet, « *la jurisprudence n'exige pas que le médecin indiscret ait cherché à diffuser l'information dévoilée notamment par publication ou voie de presse pour entrer en voie de condamnation* »[666].

§ 2 - Les limites du texte d'incrimination : les mésusages

131. La révélation suppose un acte positif. La « révélation » semble nécessairement exiger un acte positif de la part de l'agent. Il arrive toutefois, comme le souligne Monsieur Mistretta, qu'un médecin tienne une conversation téléphonique avec un patient tandis qu'il se trouve en présence d'un autre malade en consultation[667]. Comme le relève cet auteur, la jurisprudence

---

[663] CNOM, *Livre blanc : Déontologie médicale sur le web*, déc. 2011, *spéc.* p. 23 ; CNOM, *Rapport : Le médecin dans la société de l'information et de la communication. Information, Communication, Réputation numérique et Publicité. Réflexions sur la déontologie médicale*, sept. 2016, p. 23.
[664] P. MISTRETTA, *Droit pénal médical*, Cujas, 2013, n° 524.
[665] L'on peut évoquer, à simple titre d'illustration, la condamnation pour violation du secret professionnel d'un agent de police qui avait mis en ligne les images de vidéosurveillance de la RATP sur lesquelles se déroulait une agression. La décision n'a pas été publiée mais simplement relayée par un média spécialisé dans l'actualité du droit des *nouvelles technologies* (disponible sur : <https://www.legalis.net/actualite/video-dune-agression-sur-facebook-un-policier-condamne-pour-violation-du-secret-professionnel/> (dernière consultation le 10 sept. 2019)).
[666] P. MISTRETTA, *Droit pénal médical*, *op. cit.*, n° 526.
[667] *Ibid.,* n° 525.

retient une conception « *très restrictive de la matérialité du délit* »[668]. La Haute juridiction a ainsi pu juger que ne constitue pas une violation du secret professionnel le fait de mettre en place un système d'information informatisé dont les paramètres permettent au personnel administratif de prendre connaissance des informations relatives aux patients, dès lors que la commission du délit « *suppose un acte positif de divulgation, lequel n'a nullement été établi à l'encontre des prévenus* »[669]. Le verbe *divulguer* est ici mal choisi puisqu'il est synonyme de *publier* ; or, la révélation est punissable même si elle est faite à une seule personne[670]. Ainsi, l'envoi d'un courriel à une personne en particulier peut constituer une révélation punissable. Si cette question semble anecdotique, elle révèle les limites de l'adaptation de l'infraction pour répondre aux mésusages que peut engendrer l'utilisation des dispostifs techniques dont la complexité échappe aux professionnels de santé. Ces limites sont particulièrement notables s'agissant du caractère intentionnel du délit.

132. Une révélation intentionnelle. Pour être incriminée, la révélation du secret professionnel doit être intentionnelle, ce qui exclut les cas d'imprudence ou de négligence. Or, l'usage des dispositifs techniques est susceptible d'engendrer des révélations involontaires, qui peuvent être qualifiées de *mésusages*[671]. Des travaux désormais anciens dénonçaient déjà les lacunes de l'incrimination de violation du secret professionnel, estimant qu'il existait une concurrence et une complémentarité entre l'infraction punissant la violation du secret professionnel et les infractions érigées pour la protection des données à caractère personnel[672]. Pour l'instant, il doit seulement être souligné que, si *l'attitude* du professionnel est insuffisante pour protéger *les informations couvertes par le secret* lorsqu'elles sont représentées et, partant, pour garantir le *secret-état*, l'utilisation des dispositifs techniques par le professionnel lui-même peut engendrer une *rupture* du *secret-état* qui ne peut être qualifiée de violation du secret professionnel. La sanction de l'usage dévoyé des dispositifs techniques de l'information et de

---

668 *Ibid.*
669 Crim., 30 oct. 2001, n° 99-82136 ; *Adde* P. MISTRETTA, *Droit pénal médical*, *op. cit.*, n° 525.
670 Crim., 21 nov. 1874, *S.* 1875, 1, p. 89, rapp. BAUDOIN et note CAUWES ; Crim., 16 mai 2000 ; *Bull. crim.* n° 192 ; *Dr. pén.* 2000, obs. M. VERON.
671 Le terme peut désigner un abus (en ce sens v. V. GAUTRON, « Usages et mésusages des fichiers de police : la sécurité contre la sûreté ? », *AJ pénal* 2010, p. 266) mais également un mauvais usage d'une chose (TLFi, *V°* « Mésusages »).
672 J. FRAYSSINET, « Un concurrent associé du secret professionnel : le droit de la confidentialité du traitement des données personnelles », *Revue juridique de l'ouest* 2000, n° spéc. *Les médecins libéraux face au secret médical*, pp. 23-46. V. *infra* n° 213 et svt..

la communication par les professionnels tenus au secret est assurée par d'autres mécanismes relevant des dispositions spécifiques relatives à la protection des données à caractère personnel[673].

133. La violation du devoir déontologique, la sanction ordinale de l'imprudence. La particularité des règles de déontologie des professionnels de santé, s'agissant tant du devoir de préserver les supports de l'information que de celui de taire les informations relatives aux patients, réside dans leur souplesse. A titre d'illustration, l'Ordre des médecins a pu condamner l'un de ses pairs, qui avait diffusé sur son site internet les photos d'une patiente ayant subi une liposculpture du menton dès lors que cette dernière était parfaitement reconnaissable. Le médecin alléguait que le site était normalement au stade expérimental et n'aurait pas dû être accessible en ligne. Le Conseil de l'Ordre a jugé que « *ce site s'est révélé accessible à des tiers sans difficultés majeures peu important en l'espèce la circonstance qu'il se soit agi d'un site expérimental non vraiment mis en ligne ou d'un site personnel mal protégé* ». Aussi, sur le fondement de l'article R. 4127-4 du Code de la santé publique portant sur le devoir déontologique de respect du secret professionnel et de l'article R. 4127-73 du même code imposant au médecin de protéger les documents concernant les personnes qu'il examine ou soigne, le médecin a été condamné aux dépens par la chambre disciplinaire de l'Ordre des médecins et à une interdiction d'exercer de trois ans dont deux avec sursis[674].

134. Conclusion du second chapitre. Les informations relatives à la santé du patient sont juridiquement protégées au titre du droit au respect du secret de la vie privée. Sont visés, tantôt les « informations couvertes par le « secret médical », tantôt « l'atteinte au secret médical ». En ce sens, le « secret médical » est encore l'objet protégé par le droit, cette fois au titre du droit au respect de la vie privée. Aussi les immixtions ayant pour conséquence de porter atteinte au secret de ces informations peuvent-elles être sanctionnées sur le fondement des infractions prohibant les atteintes à la vie privée par l'utilisation de dispositifs techniques, désignés comme des moyens d'espionnage audiovisuel. Le caractère particulièrement intrusif de ces dispositifs légitime l'existence d'une prohibition à un stade précoce de l'*iter criminis*. La rapidité de

---

[673] V. *infra* Titre II Partie I.

[674] CDNOM, 2 déc. 2008, décision non publiée sur le site du Conseil national de l'Ordre des médecins, disponible en ligne sur : <https://www.legalis.net/jurisprudences/ordre-des-medecins-dile-de-france-chambre-disciplinaire-de-1ere-instance-decision-du-02-decembre-2008/> (dernière consultation le 12 sept. 2019).

diffusion et l'accès large à l'information diffusée par l'internet explique par ailleurs l'existence d'une infraction de conséquence.

Enfin, les techniques de l'information et de la communication peuvent être des moyens de révélation de l'information à caractère secret. La neutralité technologique du texte d'incrimination permet de sanctionner la révélation sans égard au moyen employé. Il apparaît, toutefois, que les mésusages engendrés par l'utilisation de l'outil informatique ne peuvent être sanctionnés sur le fondement de l'article 226-13 du Code pénal puisqu'il s'agit d'une infraction volontaire.

135. Conclusion du premier titre. Le « secret médical » objet juridiquement protégé consiste d'abord en une ou des informations. Elles sont protégées tant au regard de leur nature que de leur source – la relation entre le malade et la personne soumise au secret professionnel. Partant de la fonction première des dispositifs techniques de l'information qu'est la représentation de l'information, il a été démontré que la protection du « secret médical » s'entendait aussi de la situation de secret. Nous avons désigné cette situation sous le terme *secret-état*. Dès lors que l'information est représentée sur un support, cette situation de secret à l'égard des tiers ne peut être maintenue que par la protection du support qui incarne l'information secrète. L'évolution des technologies de l'information et de la communication, et particulièrement la convergence de l'informatique et de l'internet, permet l'appropriation de l'information indépendamment de son support. Plusieurs infractions sanctionnent une telle appropriation. Le « secret médical » ainsi entendu est protégé au travers de son support et lorsque l'information est dissociable de celui-ci. Cette protection peut être assurée tant par des mécanismes traditionnellement rattachés à la protection de la vie privée que par ceux protégeant la propriété.

Ensuite, le « secret médical » compris comme une situation, est juridiquement protégé des intrusions réalisées au moyen de dispositifs techniques de l'information et de la communication. Cette approche a le mérite de révéler les différents sens dans lesquels le syntagme « secret médical » est utilisé et, par là, de comprendre que c'est autant la situation de secret que l'information qui sont protégées. Toutefois, cette analyse ne peut être complète sans que ne soit envisagée la protection du « secret médical » par les dispositions spéciales protégeant les données à caractère personnel. Il apparaît, en dernier lieu, que l'ensemble des règles juridiques étudiées et protégeant, spécifiquement ou non, la situation de « secret

médical » ne permettent pas de sanctionner les imprudences et les négligences commises du fait de l'utilisation des dispositifs techniques.

TITRE II. Le secret comme objet en droit de la protection des données à caractère personnel

136. Nous nous sommes proposé d'envisager les rapports entre le « secret médical » objet juridiquement protégé et les technologies de l'information et de la communication. Notre étude nous a permis de déterminer que le syntagme « secret médical » était utilisé tant par le législateur que – lorsqu'elle adopte une approche dogmatique – par la doctrine. Le syntagme désigne alors soit l'état de secret, soit l'information couverte par le secret professionnel dans le domaine de la santé. Si la protection offerte par le droit commun est adaptée à l'utilisation individuelle des dispositifs techniques de l'information et de la communication, elle s'est révélée insuffisante au regard des emplois de la puissance informatique par l'Etat. Nous aurons l'occasion de revenir sur les enjeux politiques de ces emplois. Il importe, à ce stade de notre étude, de rappeler que la loi relative à l'informatique, aux fichiers et aux libertés[675] (LIL) est un exemple d'innovation juridique répondant aux évolutions des technologies de l'information et de la communication. Cette loi visait à réguler le traitement mathématique de l'information. Une telle fonction est différente de celles visant à représenter l'information, à la dissocier de son support ou à capter et fixer des sons et des images. D'aucuns y ont vu un outil de contrôle et de surveillance généralisée des populations[676].

Le dispositif prévu par le législateur en 1978 visait donc à réguler le traitement informatisé des informations relatives aux personnes afin de permettre l'utilisation de l'outil informatique sans qu'il ne soit porté atteinte aux droits et libertés des personnes dont les informations font l'objet d'un traitement. L'article premier de la loi, conservé en dépit des transformations, témoigne de cette ambition : *« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni*

[675] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dont les modifications successives seront abordées ultérieurement).
[676] V. *infra* n° 311 et svt.

aux libertés individuelles ou publiques »[677]. La logique adoptée est donc celle d'une conciliation entre les utilités de l'informatique et la protection des personnes, c'est l'un des traits caractéristiques de la régulation telle qu'elle est traditionnellement conceptualisée.

137. La régulation, dont nous évoquerons certains traits particuliers, peut, pour l'instant, être définie en prenant appui sur les travaux de Madame Frison-Roche[678]. L'auteur explique que la régulation « *désigne les mécanismes qui établissent et maintiennent sur certains secteurs des équilibres à long terme entre le principe de concurrence et d'autres principes, tels que la prévention des risques, l'accès aux biens essentiels, l'incitation à l'innovation, la protection de l'épargne ou celle des libertés* »[679]. Le traitement des données à caractère personnel est l'un de ces secteurs. De manière générale, l'auteur explique encore que si la régulation « *prend en charge des fonctions que la concurrence ne peut pas endosser, comme la prévention du risque systémique* »[680], elle a surtout pour fonction de mettre en « *équilibre la puissance de la concurrence et la nécessité de préserver les libertés et les vies privées* »[681]. C'est pourquoi la régulation juridique se conçoit au travers du triptyque « *de force, de pouvoir et de liberté* »[682] mis en jeu par les régulations. La Commission nationale de l'informatique et des libertés, créée par la loi de 1978 est, à l'instar des autres autorités de régulation « *au cœur des trois disciplines que sont l'économie, le droit et la science politique* »[683]. Les dispositions relatives à la protection des données à caractère personnel se sont ensuite enrichies et adaptées sous l'influence de la législation européenne. La protection des données à caractère personnel est désormais guidée par une logique de co-régulation dont nous traiterons ultérieurement.

Il importe de retenir, dans le cadre de nos recherches, que le droit de la protection des données a vocation à protéger le « secret médical » entendu comme les informations couvertes par le secret professionnel car elles sont issues de la prise en charge des personnes dans le système de santé. Dès lors qu'elles font l'objet d'un traitement, ce sont ces dispositions spécifiques qui s'appliquent. Nous nous intéresserons, dans un premier temps, au traitement

---

[677] LIL, art. 1er.
[678] Cette approche de la régulation est construite par l'auteur. Elle nous semble toutefois la plus à même de nous permettre d'appréhender la suite de notre étude. Une recherche portant sur la régulation juridique mériterait néanmoins d'autres développements essentiels, nous aborderons certaines questions en temps utile et lorsque cela présentera un intérêt pour nos travaux.
[679] M.-A. FRISON-ROCHE, *Les 100 mots de la régulation*, coll. Que sais-je ?, PUF, 2011, p. 3.
[680] *Ibid.*
[681] *Ibid.*
[682] *Ibid.*
[683] *Ibid.*

des informations couvertes par le secret **(Chapitre 1)**, avant d'envisager les opérations de traitement consistant à faire circuler les données couvertes par le secret **(Chapitre 2)**.

Chapitre 1 - Le traitement des informations couvertes par le secret

138. Le traitement des informations produites dans le système de santé est généralisé. Le fonctionnement du système de santé est aujourd'hui dépendant de ces traitements. Nous développerons ce point à l'occasion de propos ultérieurs mais l'on comprend au moins l'intérêt de s'interroger sur la protection accordée par ce droit spécial aux informations couvertes par le secret professionnel médical. Pour le déterminer, il faudra s'intéresser au champ d'application des dispositions relatives à la protection des données **(section 1)** puis à son régime **(section 2)**.

Section 1 - Les informations couvertes par le secret dans le champ d'application des dispositions relatives à la protection des données à caractère personnel

139. La loi informatique et libertés[684] n'a jamais eu pour objet d'interdire le traitement des informations relatives aux personnes, la logique a plutôt été celle du compromis[685]. De son entrée en vigueur jusqu'à celle du règlement général sur la protection des données[686] (RGPD) les dispositions de la loi nationale prévoyaient un régime de protection fondé sur des contrôles *a priori* opérés par la CNIL, laquelle vérifiait la mise en œuvre des formalités préalables aux traitements[687], des obligations incombant au responsable du traitement[688] et du respect des

---

[684] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[685] V. *infra* n° 315 et svt.

[686] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE).

[687] Avant l'entrée en vigueur du Règlement européen sur la protection des données (RGPD), la loi informatique et libertés prévoyait que les traitements de données à caractère personnel étaient soumis à des formalités préalables plus ou moins contraignantes, allant de de la simple déclaration à la CNIL à l'autorisation. Ces formalités préalables ont, en parties, été supprimées par le RGPD (c'est notamment le cas de la déclaration préalable, supprimée suite à la modification de l'ancien article 22 de la LIL opérée par l'article 11 de la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *JORF* n°0141 du 21 juin 2018). Sur l'ensemble des modifications opérées v. M. BOURGEOIS et M. MOINE, « La nouvelle loi informatique et libertés. Une transposition du RGPD ? », *JCP E*, 2018, 1417. Notons que les règlements européens sont d'application directe toutefois le RGPD comporte de très nombreuses marges de manœuvre ce qui expliquent que certains auteurs aient pu utiliser le terme « transposition ».

[688] Ces obligations figurent actuellement aux articles 37 à 39 de la LIL, au sein du chapitre V relatif aux obligations incombant aux responsables de traitements et droits des personnes. Elles ont également été modifiées par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. Le texte a ensuite fait l'objet d'une réécriture (Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la Loi n° 78-17

droits des personnes concernées par le traitement[689]. La détermination du champ d'application du règlement et de la loi informatique et libertés exige de s'intéresser, en premier lieu, à l'objet principal de ces dispositions : le traitement des données à caractère personnel[690]. Il s'agira d'envisager la qualification des informations couvertes par le secret au regard de ces dispositions **(paragraphe 1)** avant de déterminer en quoi consiste le traitement **(paragraphe 2)**.

§ 1 - La qualification des informations couvertes par le secret au regard des dispositions relatives à la protection des données personnelles

140. Au regard des dispositions relatives à la protection des données à caractère personnel, les informations couvertes par le secret professionnel dans le domaine de la santé sont des données à caractère personnel **(A)** mais également des données sensibles **(B)**.

A - Des données à caractère personnel

141. Des informations nominatives aux données à caractère personnel. Dans sa version originelle, la loi informatique et libertés avait vocation à s'appliquer aux traitements des *informations nominatives*. L'article 4 de la loi disposait : « *sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles selles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale* »[691]. L'expression « données à caractère personnel » n'est apparue qu'ultérieurement sous l'impulsion de la Convention du Conseil de l'Europe du 28 janvier 1981[692]. C'est finalement la

---

du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, *JORF* n°0288 du 13 déc. 2018).

[689] Art. 2 LIL dans sa version antérieure à la Loi du 20 juin 2018 : « *La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement* ».

[690] F. LESAULGNIER « *Définir la notion de données à caractère personnel au sens du règlement général relatif à la protection des données personnelles est une lourde tâche, car c'est à cette notion cardinale qu'est accroché le régime de protection des données en Europe* […]. *L'enjeu est d'autant plus important qu'il s'agit d'une définition commune, qui a vocation à être appliquée et interprétée de façon uniforme dans l'ensemble de l'Union européenne* » (F. LESAULGNIER, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p.573).

[691] Art. 4 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ancienne).

[692] CE, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités européens n° 108, 28 janvier 1981 (entré en vigueur le 1er octobre 1985).

loi du 6 août 2004[693], modifiant la loi informatique et libertés et transposant une directive européenne[694], qui intègre le vocable de *données à caractère personnel*. Au moment de l'entrée en vigueur de la loi du 6 août 2004 la question des conséquences de ce changement interroge la doctrine. Les deux expressions recouvrent le même objet. Tandis que, selon certains auteurs[695], la différence n'est que sémantique, d'autres considèrent que la notion de *données à caractère personnel* couvre un champ plus large car elle permettrait d'y faire entrer des objets tels que les images et les sons qui dépassent le champ couvert par la notion *d'information nominative*[696]. Madame Eynard, propose une autre approche. Tout d'abord l'auteur s'applique à définir les critères particuliers qui permettent non pas d'associer les deux notions en les superposant ou en les envisageant de manière concentrique, mais en admettant que la catégorie des *données à caractère personnel* doit être différenciée de celles des *informations nominatives*[697]. Pour ce faire, l'auteur s'emploie à déterminer ce qui caractérise les données à caractère personnel : elles toucheraient à l'essence humaine dans la mesure où il s'agit d'informations intrusives, ce qui permet notamment d'y faire entrer les données ADN, les informations relatives au réseau veineux de la main, l'empreinte génétique, les mouvements et déplacements d'une personne, les éléments déterminants de son iris[698]. Ensuite, elle considère que les données à caractère personnel sont également intrusives dans leur objet dans la mesure

---

[693] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la Loi n° 78-17 du 6 janvier 1978, *JO* du 7 août 2004, p. 14063.
[694] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, *JOCE* du 23 novembre 1995, p. 31.
[695] J. FRAYSSINET, *Informatique, fichiers et libertés*, Litec, 1992, n° 80 à 86 ; I. DE LAMBERTRIE et H.-J. LUCAS, *Informatique, libertés et recherche médicale*, coll. CNRS Droit, CNRS, 2001, n° 159 à 163. Ces derniers auteurs considèrent toutefois que le terme de *données* renvoie à l'information traitée informatiquement. Aussi selon ces auteurs la question n'est-elle que sémantique et les auteurs utilisent-ils indifféremment les mots *données* et *informations*.
[696] M.-L. LAFFAIRE, *Protection des données à caractère personnel*, Editions d'Organisation, 2005, p. 42 ; « *la définition donnée par la directive pourrait donner lieu à une extension du champ de la protection par rapport à la loi de 1978, dans des domaines où la notion d'identification indirecte est source d'incertitudes, comme ceux de la voix et de l'image* » (G. BRAIBANT, Rapport au Premier ministre, *Données personnelles et société de l'informations,* La Documentation française, 1998, p. 77).
[697] J. EYNARD, *Les données personnelles. Quelles définitions pour un régime de protection efficace ?*, *op. cit.* et ralliant cette conception R.-M. BORGES et C. LASSALAS, « Personnalisation des soins et risques liés aux données de santé », *in* C. CASTAING (ss. la dir.) *Technologies médicales innovantes et protection des droits fondamentaux des patients*, Mare et Martin, p. 113.
[698] J. EYNARD, *Les données personnelles. Quelles définitions pour un régime de protection efficace ? op. cit.*, pp. 87-98.

où elles permettent de tracer et de profiler les individus[699]. L'on peut ajouter que ces actions sont favorisées par le *Big data* et les algorithmes utilisés pour les traiter[700]. Enfin, l'auteur considère que *la donnée à caractère personnel*[701] échappe au contrôle de l'individu à un double titre : il n'en a pas la maîtrise intellectuelle, car elle est, pour lui, inintelligible[702], de même qu'il n'en a pas la maîtrise juridique[703]. Cette analyse a pour objet de démontrer l'autonomie de la notion de *donnée à caractère personnel*. Si elle est exacte, dans la mesure où l'on ne peut plus nier que les données échappent au contrôle des personnes concernées, elle nous semble toutefois erronée en ce qu'elle vise *la donnée*, or « *une donnée isolée n'a aucune valeur dans la mesure où elle ne permet pas d'opérer sur elle un traitement* »[704]. Il importe donc, avant de s'intéresser au contenu de la notion, de saisir le sens de l'utilisation du pluriel : les données à caractère personnel peuvent aussi bien être des informations sur le réel qu'une somme de données qui deviennent des informations grâce au traitement mathématique permis par l'informatique.

142. De l'information aux données, des données à l'information. Le substantif « donnée » apparaît d'abord dans le vocabulaire mathématique et désigne une « *quantité connue dans l'énoncé d'un problème et qui sert à trouver la solution* »[705]. En ce sens les données servent de base aux raisonnements[706]. En français le substantif peut également être masculin : *le donné* désigne « *ce qui est immédiatement présenté à l'esprit avant que celui-ci y applique ses*

---

[699] J. EYNARD, *Les données personnelles. Quelles définitions pour un régime de protection efficace ? op. cit.*, pp. 89-139, spéc. p. 99. Il faut noter qu'une telle définition des données personnelles renvoie uniquement aux données biométriques.
[700] A propos du *Big data* V. *infra* n° 384 et svt.
[701] L'auteur utilise le singulier (J. EYNARD, *Les données personnelles. Quelles définitions pour un régime de protection efficace ? op. cit.*, p. 141 et svt.).
[702] L'auteur avance que l'absence de maitrise peut avoir deux causes « *soit l'individu ne connaît pas l'élément de sa personnalité car sa connaissance nécessite de multiples recoupements et décodages que le cerveau humain ne peut réaliser, soit il connait l'élément de sa personnalité mais ne sait pas qu'il est devenu une information* » (J. EYNARD, *Les données personnelles. Quelles définitions pour un régime de protection efficace ? op. cit.*, p. 148). La seconde partie de son propos renvoie au fait qu'à partir d'une donnée isolée, tirée d'une information, il est possible de recréer une information dès lors qu'elle est mise en relation avec d'autres données (P. CATALA, « Ebauche d'une théorie juridique de l'information », *D.* 1984, p. 97).
[703] L'auteur considère que le lien juridique qui unit la personne à ses données à caractère personnel n'est ni un droit de propriété ni un droit de la personnalité (J. EYNARD, *Les données personnelles. Quelles définitions pour un régime de protection efficace ? op. cit.,* p. 171).
[704] A. GARAPON et J. LASSEGUE, *Justice digitale*, PUF, 2018, p. 32.
[705] TLFi, *V°* « Donnée », *op. cit.*
[706] A. LALANDE, *Vocabulaire technique et critique de la philosophie*, coll. Quadrige, PUF, *V°* « données ».

procédés d'élaboration »[707]. Le donné s'oppose ainsi au construit[708]. Au pluriel, les données sont à rapprocher du mot « *data* » dans la langue anglaise : « *considéré comme un « nom indénombrable », c'est-à-dire un mot qui sert à désigner des choses qui ne peuvent pas être comptées de façon unitaire et sont considérées dans leur ensemble* »[709]. La donnée prise isolément n'est pas pertinente, elle constitue une « *segmentation du réel* »[710]. La donnée ne devient *information* que lorsqu'elle est mise en relation avec d'autres données et selon l'usage qui en est fait. Cette mise en relation des données, en masse, est parfois désignée sous le terme de métadonnées. Madame Frison-Roche expose cette construction : « *La science, qui est désormais définie comme l'art subjectif d'élaborer des informations, est une construction du monde. Ainsi, ce que l'on désigne sous le nouveau vocable de « métadonnées » est le fait de construire des systèmes nouveaux d'information à partir d'éléments disponibles mais épars, prenant de la pertinence et de la valeur au regard d'un usage* »[711]. Aussi, si la donnée n'est qu'un élément de fait extrait du réel, son traitement en masse permet de produire de l'information. Les dispositifs techniques de l'information sont des outils de production de l'information. Outre ce passage des données à l'information qui relève d'un processus proprement technique[712], l'informatique favorise également la production de données à partir d'informations collectées. Le mouvement est donc double : le processus logique et technique, qui permet le passage de la donnée à l'information par une mise en contexte suivant une certaine finalité, se superpose à un processus que permet l'évolution des dispositifs de l'information, et qui consiste à isoler, dans l'information, une donnée qui, une fois traitée avec une quantité d'autres données, produiront une autre information. Ainsi, en raison de ce second processus, « les données » ont également un sens spécifique dans le vocabulaire informatique, définis

---

[707] *Ibid.*, *V°* « *donné* ».
[708] *Ibid.*
[709] L.WATRIN, *Les données scientifiques saisies par le droit*, Th. dact., ss. la dir. de M.- E. PANCRAZI, soutenue le 9 déc. 2016, Université d'Aix-Marseille, n° 2.
[710] M.-A. FRISON-ROCHE, « Repenser le monde à partir de la notion de « données » », *in* M.-A. FRISON-ROCHE (ss. la dir.), *Internet, espace d'interrégulation*, série « Régulation », coll. Thèmes et commentaires, Dalloz, 2016, p. 9.
[711] *Ibid.*
[712] F. CHAVAND, *Des données à l'information. De l'invention de l'écriture à l'explosion numérique*, coll. Histoire des sciences et des techniques, ISTE éditions, 2017, pp. 398-419.

comme « *Ensemble des indications enregistrées en machine pour permettre l'analyse et/ou la recherche automatique des informations* »[713].

143. Les données à caractère personnel sont des informations. L'information produite grâce à la puissance informatique et à la récolte de données éparses est également, en matière de santé, le fruit de ce double phénomène. Les acteurs du système de santé ont besoin d'informations pour prodiguer des soins, assurer le suivi des patients, poser des diagnostics et plus largement participer à la décision médicale[714]. Pour ce faire, les informations sont recueillies auprès des patients, tout au long de leur parcours de santé. Si toutes ces informations font aujourd'hui l'objet d'un traitement informatique, certaines consistent en des *indications brutes* mises en contexte dans un but déterminé, et destinées à produire de l'information car elles sont juxtaposées « *à d'autres réalités choisies* »[715]. Le lien de pertinence entre elles « *n'apparaitra que par l'usage qui en sera fait* »[716]. La polysémie du mot « *donnée* » a engendré une confusion entre la donnée « *segmentation du réel* », les données « *Ensemble des indications enregistrées en machine pour permettre l'analyse et/ou la recherche automatique des informations* »[717], et les informations faisant l'objet d'un traitement informatique devenant données car elles sont « *transformées en vue d'un traitement informatique* »[718] et qu'en ce sens elles possèdent « *une valeur ajoutée d'ordre technologique* »[719]. Ces dernières demeurent porteuses du sens d'origine. Ainsi le taux de cholestérol est une donnée, traitée informatiquement avec des dizaines d'autres taux de cholestérol déterminés, sur une personne identifiée et pendant un laps de temps déterminé. Ces données constituent une information sur l'évolution de l'état de santé de cette personne. C'est la masse de données et leur traitement dans un but déterminé qui produit l'information. Tandis que l'inscription dans un dossier informatisé d'un compte-rendu opératoire, bien que traité informatiquement, contient toujours des informations qui pourront toutefois être qualifiées de données au sens des dispositions relatives à la protection des données à caractère personnel, l'article 4 du RGPD définit

---

[713] TLFi, *op.cit.*, *V°* « donnée ».
[714] Sur les rapports entre l'information médicale et la décision médicale v. P. VERON, *La décision médicale*, Th. dact., ss. la dir. de F. VIALLA, soutenue le 9 décembre 2015, Université de Montpellier.
[715] M.-A. FRISON-ROCHE, « Repenser le monde à partir de la notion de « données » », *op. cit.*, p. 9.
[716] *Ibid.*
[717] TLFi, *op.cit.*, *V°* « donnée ».
[718] I. DE LAMBERTRIE, « Qu'est-ce qu'une donnée de santé ? », *in Le droit des données de santé*, numéro spécial, *RGDM* 2004, p. 13.
[719] *Ibid.*

désormais les données à caractère personnel comme : « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée* « personne concernée »*); est réputée être une* «personne physique identifiable» *une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale*»[720]. La possibilité d'assimiler *les données* à de l'information ne fait donc aucun doute. D'une part, la définition vise « toute information ». D'autre part, les données ne peuvent être personnelles qui si elles portent une indication qui permet de les relier à une personne, d'isoler cette personne de la masse des individus. Les données à caractère personnel font nécessairement sens. Mais la seconde partie de la définition, avec l'énumération qui la compose, nous apprend que cette qualification s'apprécie au regard de l'évolution des techniques : il ne peut donc s'agir d'une notion statique. Plus les capacités de recoupement des dispositifs techniques sont performantes, plus la masse de données portant sur un individu est importante, et plus la possibilité d'identification de cet individu sera importante. La qualification des données entrant dans le champ d'application des dispositions relatives à la protection des données à caractère personnel ne pourra se faire que de manière casuistique.

Aussi, pour revenir aux définitions formulées plus avant, il nous semble que les données à caractère personnel peuvent être des informations nominatives ou des données intrusives par leur contenu et leur objet. Les deux définitions ne se situant pas sur le même plan, l'image des cercles concentriques[721] peut tout à fait illustrer les rapports entre les différentes définitions. Les données à caractère personnel peuvent être une information nominative ou une partie seulement d'une information. Dès lors que cette *partie*, même infime, permet - par corrélation ou inférence[722] - de rendre la personne qu'elle concerne identifiable, elle redevient une

---

[720] RGPD, Art. 4 1).
[721] En ce sens v. G. BRAIBANT, Rapport au Premier ministre, « Données personnelles et société de l'informations », La Documentation française, 1998, p. 77.
[722] Le G29 (L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationales : « *Cette organisation réunissant l'ensemble des CNIL européennes a pour mission de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le*

information. Cette dernière peut varier dans son contenu en fonction des évolutions scientifiques et technologiques. Aussi, la remarque formulée par Monsieur Braibant en 1998 nous parait toujours d'actualité : « […] *la notion de "donnée à caractère personnel", qui recouvre toute information susceptible d'être rapportée à une personne identifiée ou identifiable, est beaucoup plus large que celle de donnée relative à la vie privée* »[723] mais elle l'englobe. L'application d'un régime de protection identique est, à cet égard, justifiée. La définition prend en compte l'information « source » des données et les données captées isolement mais qui, mises en contexte, formeront une information relative à la personne concernée. Toutefois, cette analyse doit être complétée au regard des autres transformations opérées par le droit de l'Union européenne. En effet, le RGPD, directement applicable en droit français depuis le 25 mai 2018, contribue à harmoniser la protection des données à caractère personnel dans l'ensemble des pays de l'Union. D'autres définitions ont été posées, elles permettent de préciser le champ d'application matériel des dispositions en apportant des précisions sur les limites de la notion de données à caractère personnel.

144. L'identification au centre de la définition, évaluation casuistique. La définition posée à l'article 4 du RGPD doit être lue au regard des précisions apportées au considérant 26 du même règlement, qui précise que : « *Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable* »[724]. Cette précision dessine les limites de la

---

niveau de protection dans les pays tiers et de conseiller la Commission européenne sur tout projet ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles » <https://www.cnil.fr/fr/le-comite-europeen-de-la-protection-des-donnees-cepd> elle ce nomme désormais Comité européen de la protection des données, ce dernier remplit les mêmes fonctions) propose d'évaluer l'efficacité des techniques d'anonymisation en tenant compte des critères suivants : « *L'individualisation : est-il toujours possible d'isoler un individu ? La corrélation : est-il possible de relier entre eux des ensembles de données distincts concernant un même individu ? L'inférence : peut-on déduire de l'information sur un individu ?* » (G29, Avis 05/2014 sur les Techniques d'anonymisation, 10 avril 2014, p. 3). Aussi l'individu concerné sera-t-il identifiable si l'individualisation à partir des données traitées est possible, si les données reliées entre elles ou déduites les unes des autres permettent l'identification. On parvient, en raisonnant *a contrario*, à saisir ce qu'est une donnée à caractère personnel puisque l'anonymisation *est* un traitement de données à caractère personnel (dès lors que les données faisant l'objet de l'anonymisation sont, à l'origine, des données à caractère personnel). Ce raisonnement sera d'ailleurs retenu dans le RGPD.

[723] *Ibid.* p. 7. al. 1 RGPD (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016).

[724] Consid. 26 RGPD (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016). La pseudonymisation est donc une anonymisation pouvant donner lieu à une réidentification de la personne. L'anonymisation des données empêche toute possibilité de pouvoir identifier l'individu concerné. Il

notion[725]. Le même considérant précise ensuite que « *Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage* »[726]. Cette seconde précision a pour conséquence de fixer les limites de la définition, non pas au regard de la nature des données mais des moyens d'identification. L'usage du terme *raisonnable* n'emporte pas de changements notables, cette même précision figurant déjà au considérant 26 de la directive de 1995, la France ayant alors fait le choix de ne pas la transposer estimant que la CNIL et le juge national prendraient soin de s'y reporter pour évaluer lesdits moyens[727]. Désormais, cette évaluation devra être menée en fonction des critères définit par le RGPD : il ne s'agit plus d'une simple possibilité. Pour ce faire, la CNIL comme le juge devront « […] *prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci* »[728]. Aussi le règlement ne s'applique-t-il pas aux données anonymes mais l'anonymisation[729] sera de plus en plus difficile à obtenir dès lors que plusieurs catégories de données seront traitées[730] et que les dispositifs techniques se

---

s'agit, pour le responsable du traitement de modifier le contenu ou la structure des données de sorte à rendre la « ré-identification » des personnes presque impossible. L'article 4 5) du RGPD définit le processus comme : « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* ».

[725] Déjà précisé par le G29 et affirmée par CE 10/9 SSR, 8 février 2017, n°393714, *Société JC Decaux*, *tables Rec. Lebon*, concl. A. BRETONNEAU, *op. cit.* v. note 757. En ce sens, F. LESAULNIER, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *op. cit.*

[726] Consid. 26 RGPD (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016).

[727] *« Il ne paraît pas utile de reprendre dans la loi les précisions données par le considérant 26 sur* " l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne.". *L'autorité chargée de la protection des données et le juge pourront en effet, en tout état de cause, se référer aux motifs de la directive pour éclairer les définitions données par la loi et lever toute difficulté d'interprétation.* » (G. BRAIBANT, Rapport au Premier ministre, « Données personnelles et société de l'information », *op. cit.*, p. 46).

[728] Consid. 26, RGPD, *op. cit.*

[729] A ce stade il convient simplement de remarquer que l'anonymisation doit empêcher toute identification.

[730] En ce sens v. F. LESAULGNIER, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *op. cit.*, p. 573 et R. PERRAY et J. UZAN-NAULIN, « Existe-t-il encore des données non personnelles ? », *Dalloz IP/IT 2017*, p. 286 ; Comme le souligne encore E. NETTER : « […] *au fur et à mesure que les techniques mathématiques d'analyse des informations se perfectionnent, le champ des données qui doivent être qualifiées comme personnelles augmente* » (E. NETTER, *Numérique et grandes*

perfectionneront[731], ce qu'illustre d'ailleurs la jurisprudence récente du juge national et de la CJUE[732].

Suite aux observations qui viennent d'être formulées il appert que toutes les informations recueillies dans le cadre d'une prise en charge par un professionnel intervenant dans le système de santé – lesquelles sont des informations couvertes par le secret professionnel –, peuvent être

notions du droit privé. La personne, la propriété, le contrat, Mémoire en vue de l'habilitation à diriger des recherches en droit privé, présenté et soutenu publiquement le 20 novembre 2017, note n° 136 (disponible sur <http://enetter.fr/wp-content/uploads/2018/09/E.-NETTER-Nume%CC%81rique-et-grandes-notions-du-droit-prive%CC%81-V.-1.06.pdf> dernière consultation le 14 oct. 2019).

[731] Notamment H. TANGHE et P.-O. GIBERT « L'enjeu de l'anonymisation à l'heure du big data », *Revue française des affaires sociales* 2017/4, pp. 79-93.

[732] Ainsi, les adresses IP dites *statiques* (qui demeurent les mêmes à chaque connexion) ont été qualifiées de données à caractère personnel par la CJUE (CJUE 24 nov. 2011, aff. C-70/10, Sté Scarlet Extended c/ Société belge des auteurs, compositeurs et éditeur SCRL, *D.* 2011, p. 2925, obs. C. MANARA ; *D.* 2012, p. 2343, obs. J. LARRIEU, C. LE STANC et P. TREFIGNY ; *D.* 2012, p. 2836, obs. P. SIRINELLI ; *RSC* 2012, p. 163, obs. J. FRANCILLON ; *RTD eur.* 2012, p. 404, obs. F. BENOIT-ROHMER ; *RTD eur.* 2012, p. 957, obs. E. TREPPOZ ; *Gaz. Pal.* 16 févr. 2012, n° 47, note L. MARINO). La Cour de cassation a également eu l'occasion de rendre une décision en ce sens (Civ. 1e, 3 nov. 2016, n° 15-22595, *AJDA* 2017, p. 23 ; *D.* 2016. 2285 ; *Dalloz IP/IT* 2017, p. 120, obs. G. PERONNE et E. DAOUD ; *RTD civ.* 2017, p. 94, obs. J. HAUSER ; *Légipresse* 2017, n° 345, p. 27, obs. N. BOTCHORICHVILI ; *JCP G* 2016, 1310, obs. R. PERRAY ; *Dr. pén.* 2015, chron. 11, n° 12, obs. A. LEPAGE ; *Gaz. Pal.* 15 nov. 2016, n° 40, p. 24, obs. Ph. INGALL-MONTAGNIER ; *RLDI* 2016, n° 4087, obs. L. COSTES). Puis s'agissant des adresses IP *dynamiques* à l'occasion d'un arrêt de la CJUE (CJUE, 19 oct. 2016, aff. C-582/14, Breyer c/ Bundesrepublik Deutschland, *D.* 2016, p.2215 ; *Dalloz IP/IT* 2017, p. 120, obs. G. PERONNE et E. DAOUD ; *RLDI* 2017, n° 4944, note B. PAUTROT ; *CCE* 2016. Comm. 104, note N. METALLINOS ; *Rev. int. compliance* 2016. Comm. 130, note M. GRIGER et J. SCHWARTZ). Une autre affaire a encore confirmé le caractère dynamique de la notion à propos des mesures d'audience des panneaux publicitaires de l'entreprise *JCDecaux*, traitement auquel la CNIL avait refusé son autorisation (Délibération n°2015-255 du 16 juillet 2015). Ce refus s'expliquait principalement par le défaut du respect des conditions relatives au traitement de données à caractère personnel, dont l'obtention du consentement de la personne concernée. L'argument principal de la société consistait dans la qualification des données traitées, *JCDecaux* affirmant que celles-ci étaient anonymisées et ne pouvaient donc plus être qualifiées de données à caractère personnel (CE 10/9 SSR, 8 février 2017, n°393714, *Société JC Decaux*, *tables Rec*. *Lebon*, concl. A. BRETONNEAU; *AJDA* 2017, p. 325; *JCP A* 2017, Act. 125, obs. C. FRIEDRICH ; *RLDI* 2017, n° 4961, obs. L. COSTES ; *RLDI* 2017, n° 4954, note E. DROUARD et C. MAROLLA ; *CCE* 2017. Comm. 37, note N. METALLINOS; *Dalloz IP/IT* 2017, p. 286, obs. R. PERRAY et J. UZAN-NAULIN). La mesure d'audience devait s'effectuer en captant les adresses MAC des passants via des bornes wifi, ces adresses, qui sont des données à caractère personnel (CNIL, délib. n° 2011-035, 17 mars 2011, *CCE* 2012. Étude 1, obs. A. DEBET) faisaient l'objet de deux processus (*salage* et *hachage à clef*) pour garantir une anonymisation, que la CNIL qualifie de pseudonymisation, permettant tout de même « la corrélation et l'inférence » du parcours des piétons entre deux bornes wifi. En conséquence, elle qualifie les données de données à caractère personnel et le CE de rappeler que « *ne peut être regardée comme rendue anonyme que lorsque l'identification de la personne concernée, directement ou indirectement, devient impossible que ce soit par le responsable du traitement ou par un tiers* ». Pour ce faire le CE a bien « *considér[é] l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* ». Partant, à l'occasion d'un commentaire de cet arrêt, deux auteurs ont posé, à juste titre, la question de savoir s'il existait encore des données qui ne soient pas personnelles (R. PERRAY et J. UZAN-NAULIN, *Dalloz IP/IT* 2017, p. 286).

qualifiées de données à caractère personnel dès lors qu'elles sont des informations relatives à la personne.

145. Toutes les informations à caractère secret sont des données à caractère personnel. Selon un auteur, la finalité première des droits sur les données à caractère personnel « *ne saurait se résumer à assurer aux individus le secret de leur intimité ; il s'agit plus largement d'assurer à chacun la maitrise de son anonymat et, corrélativement, de son identification* »[733]. Bien que la question du rapport entre vie privée et identité ait précédemment été évoquée[734], la doctrine interroge encore ces rapports pour cerner le champ d'application matériel des dispositions relatives à la protection des données, afin de trouver une place, de classer, les « *droits sur les données personnelles* »[735] au sein des droits de la personnalité. Ce faisant certains tentent de déterminer les spécificités de la protection juridique des données personnelles par rapport aux mécanismes protégeant le secret de la vie privée[736]. L'entreprise est tout aussi ardue que de prétendre déterminer le contenu de la vie privée. La démarche conduit à dresser une longue liste des données qualifiées de données à caractère personnel et à comparer cette liste à celle des informations personnelles entrant dans le champ de la vie privée. Une telle entreprise est possible grâce une étude attentive de la doctrine de la CNIL et de la jurisprudence[737]. Certains

---

[733] M. BENEJAT, « Les droits sur les données personnelles »*, in Droits de la personnalité*, J.-C. SAINT-PAU, (ss. la dir.), LexisNexis, n° 945.
[734] V. *supra* n° 39.
[735] L'expression est utilisée par M. BENEJAT, *op. cit.*, n° 945.
[736] Par exemple : Dans l'ouvrage *Droits de la personnalité* dirigé par J.-C. SAINT-PAU, l'étude des droits sur les données personnelles figurent dans un titre consacré aux droits sur l'identité, ces derniers constituant une catégorie de droits de la personnalité (J.-C. SAINT-PAU (ss. la dir.), *Droits de la personnalité*, *op. cit*.). C'est également la démarche de J. EYNARD (J. EYNARD, *Les données personnelles*, *op. cit.*).
[737] De manière non exhaustive, ont pu être qualifiées de données à caractère personnel directement identifiantes : le nom et le prénom (TGI Nantes, 16 déc. 1985 ; *D.* 1986, jurispr. p. 471, note J. FRAYSSINET ; *JCP E* 1986, II, 15791, obs. M. VIVANT et A. LUCAS ; T. com. Paris, 1re ch., 28 janv. 2014, M. X. c/ Google Inc. et Google France ; *RLDI* avr. 2014, n° 103, n° 3438, p. 57, obs. L. COSTES ; *RLDI* juin 2014, n° 3494, p. 36, note M. COMBE), l'âge (CNIL, délib. n° 2008-198, 9 juill. 2008 modifiant l'autorisation de certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour évaluer les risques en matière d'octroi de crédit), la nationalité (CE Sect., 30 octobre 2001, *Association française des sociétés financières*, n°204909; *Comm. Com. électr.* 2002, comm. 79, note A. LEPAGE et s'agissant du registre fédéral des étrangers en Allemagne : CJCE, 16 déc. 2008, aff. C-524/06, Heinz Huber; *Rec. CJCE* 2008, I, p. 9705 ; *Europe* 2009, comm. 53, obs. F. KAUFF-GAZIN ; *JCP A* 2009, n° 30, 2189, obs. M. GAUTIER), l'adresse postale et l'adresse électronique ainsi que les coordonnées téléphoniques (crim. 14 mars 2006 ; *Bull. crim.* 2006, n° 69 ; *Comm. com. électr.* 2006, comm. 131, note A. LEPAGE ; *D.* 2007, pan. P. 404, obs. T. GARE ; *AJ Pénal* 2006, p. 260, G. ROUSSEL; T. corr. Briey, 15 sept. 1992 : *Gaz. Pal*. 1993, 1, jurispr. p. 201 ; CE 10 SSJS 11 avr. 2014, n° 348111, JurisData n° 2014-007169 ; CNIL, délib. n° 2014-041, 29 janv. 2014 ; CE 10 SSJS, 30 déc. 2015, n° 376845, *Association Juricom et associés c/ CNIL*, JurisData n° 2015-029961 ; *Comm. com. électr.* 2016, comm. 36, note

auteurs s'y sont efforcés, soit pour confirmer l'idée selon laquelle les dispositions relatives à la protection des données personnelles participent de la protection de la vie privée[738], soit pour démontrer que les contenus se recoupent sans se confondre[739], soit encore pour démontrer que les données à caractère personnel touchent à l'essence de l'identité[740]. Aucune de ces propositions ne peut être disqualifiée, puisque selon la conception que l'on adopte de la vie privée, celle-ci peut concerner l'identité mais également ne l'intégrer que partiellement ; l'on peut encore considérer qu'il existe des droits sur l'identité au sein des droits de la personnalité. Une telle démarche nous semble impropre à démontrer que les informations couvertes par le secret professionnel sont des données à caractère personnel au sens des dispositions relatives à la protection des données. Les informations dont la révélation est sanctionnée par l'incrimination définie à l'article 226-13 du Code pénal sont des informations relatives à une

---

A. DEBET), l'identité des parties à une instance figurant dans une base de données de jurisprudence (CNIL, délib. n° 2011-238, 12 juill. 2011 : Comm. com. électr. 2011, comm. 115, obs. A. LEPAGE. – confirmée par CE 10/9 SSR, 23 mars 2015, n° 353717, Association Lexeek, tables Rec. Lebon : JurisData n° 2015-006473 ; *Gaz. Pal*. 16 avr. 2015, n° 106, p. 28 ; *AJDA* 2015, p. 1398 ; Comm. com. électr. 2015, comm. 52, note A. DEBET), la voix et l'image d'une personne (concernant la vidéosurveillance d'une habituation lorsque la caméra donne sur la voie publique : CJUE, 11 déc. 2014, aff. C-212/13, František Ryneš c/ Úřad pro ochranu osobních údajů ; JurisData n° 2014-032321 ; *Comm. com. électr.* 2015, comm. 15, note A. DEBET ; *RLDI* janv. 2015, n° 3655, p. 30, obs. L. COSTES ; *RLDI* déc. 2015, n° 3875, p. 21, note J. UZAN-NAULIN et R. PERRAY), certaines données publiques sont des données personnelles et, bien que disponibles au sens de la loi du 17 juillet 1978 sur les archives publiques elles n'en sont pas moins des données personnelles dont la disponibilité est limitée (CAA Lyon, 4 juill. 2012, n° 11LY02325 et n° 11LY2326 : JurisData n° 2012-014986 ; *Gaz. Pal*. 13 sept. 2012, n° 257, p. 28 ; *JCP A* 2012, n° 40, 2318, note J.-M. BRUGUIERE). Il faut également compter toutes les données permettant une identification indirecte de la personne : ont été qualifiées comme telles : le numéro de sécurité sociale, les coordonnées bancaires (qui par ailleurs sont également des informations relevant du secret de la vie privée (Civ. 1e, 9 déc. 2003, n° 01-11.587, JurisData n° 2003-021331 ; *Bull. civ.* 2003, I, n° 254 ; *Gaz. Pal.* 2005, somm. p. 1399, obs. P. GUERDER ; *RTD civ.* 2004, p. 264, obs. J. HAUSER), les informations relatives au régime matrimonial (CNIL, délib. n° 2008-004, 10 janv. 2008 autorisant le traitement de la direction générale des impôts visant la dématérialisation des échanges entre les notaires et la conservation des hypothèques), les données relatives à la géolocalisation des véhicules professionnels (CNIL, délib. n°2006-067 du 16 mars 2006 portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés ; Soc., 3 nov. 2011, n° 10-18.036, JurisData n° 2011-023703 ; *JCP G* 2011, act. 1284, obs. N. DEDESSUS-LE-MOUSTIER ; *JCP E* 2011, 1926, note D. CORRIGNAN-CARSIN ; *Gaz. Pal.* 17 nov. 2011, n° 321, p. 28, obs. C. BERLAUD ; *JCP S* 2012, n° 6, 1054, obs. G. LOISEAU ; *Comm. com. électr.* 2012, comm. 32, obs. A. LEPAGE ; *RJEP* 2012, chron. 2, obs. G. HENON et N. SABOTTIER ; *Dr. pén.* 2012, chron. 10, obs. A. LEPAGE ; *LPA* 3 juin 2013, n° 110, p. 5, obs. A. FIORENTINO). Ou encore à propos des segments comportementaux en vue d'établir des profils de consommation de services (CE 10/7 SSR, 7 juin 1995, *Rec. Lebon* n° 148659 ; *AJDA* 1996, p. 162, note J. FRAYSSINET), de même les adresses IP peuvent être considérées comme des données à caractère personnel (consid. 30 RGPD).

[738] R. PERRAY, *JCl Comm.* ; Fasc. 930, « Données à caractère personnel. – Introduction générale et champ d'application de la loi "Informatique et libertés" », *spéc.*n° 5 et svt.

[739] Considérant qu'il existe une « *dissociation au moins partielle, de l'identité et de la vie privée* » et que les intérêts protégés ne sont « *pas tout à fait identiques* ». (BENEJAT, « Les droits sur les données personnelles », *in Droits de la personnalité*, *op. cit.*, n° 940).

[740] J. EYNARD, *Les données personnelles*, op. cit.

personne identifiée ou identifiable, elles entrent donc dans le champ d'application des dispositions relatives à la protection des données à caractère personnel.

B - Des données sensibles

146. Contenu de la notion de données personnelles *sensibles*. Au-delà de leur qualification de données à caractère personnel, les informations couvertes par le secret professionnel dans le domaine de la santé[741] peuvent entrer dans une catégorie particulière de données à caractère personnel, considérées comme « sensibles ». La loi informatique et libertés, même suite aux modifications successives, avait conservé un régime particulier relatif aux données sensibles, lequel perdure partiellement sous l'empire du RGPD. Ce régime s'appliquait à une catégorie de données dont la sensibilité tenait à leur nature. Ainsi, l'article 8 du la LIL prévoyait une interdiction de principe de traitement des données « *qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* »[742]. L'article 9 du RGPD définissant les données sensibles est venu compléter cette liste en ajoutant les données relatives à l'orientation sexuelle[743], les données génétiques[744], les données biométriques[745]. Toutes les informations couvertes par le secret dans

---

[741] Pour reprendre la formulation utilisée à l'article L. 1110-4 du Code de la santé publique il s'agit des informations concernant toutes personnes prises en charge « *par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles* ».

[742] Art. 8 de la Loi n° 78-17 du 6 janvier 1978.

[743] Bien que la loi informatique et libertés ne mentionnait pas l'orientation sexuelle avant l'entrée en application du RGPD, le Conseil d'Etat avait déjà eu l'occasion de s'opposer à une opération de traitement, et plus précisément à l'accès au registre des greffes des tribunaux d'instance répertoriant les pactes civils de solidarité car « *bien que n'ayant pas pour objet de révéler les orientations sexuelles des signataires* » leur consultation peut « *permettre de déduire l'existence d'une vie de couple entre personnes de même sexe* ». (CE 4/6 SSR, 8 déc. 2000, *D*. 2002, p. 615, obs. J.-J. LEMOULAND). Ce sont bien les données relatives à l'orientation sexuelle qui sont visées en l'espèce.

[744] Les données génétiques sont désormais définies à l'article 4 13° du RGPD « *les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question* ».

[745] Les données biométriques sont également définies à l'article 4 14° du RGPD: « *les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques* ». Pour une étude complète sur la biométrie et traitant

le domaine de la santé peuvent, *a priori*, entrer dans cette catégorie : les informations médico-administratives[746], ainsi que les informations originellement confiées à un professionnel dans le cadre de la prise en charge sanitaire et médico-sociale sont des données *sensibles* telles que définies par le RGPD. De plus, ces informations peuvent également être relatives à la vie sexuelle des personnes ou à leur statut génétique[747].

147. Des données de santé. Pendant longtemps le législateur national n'avait pas prévu de définition des données de santé[748]. Aussi la recherche du contenu de la notion conduisait-elle à se référer à d'autres sources[749]. C'est finalement le RGPD qui pose une définition désormais commune à tous les Etats de l'Union européenne. Sont des données de santé « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* »[750]. Cette définition particulièrement compréhensive était celle retenue

---

notamment des données biométriques v. M. SZTULMAN, *La biométrie saisie par le droit public. Etude sur l'identification et la localisation des personnes physiques*, pref. X. BIOY, coll. Bibliothèques de droit public, t. 305, LGDJ, 2019

[746]Il s'agit des informations servant à l'évaluation des activités des établissements (P.M.S.I prévu à l'article L. 6113-7 CSP) mais également de toutes les données contenues dans d'autres bases de données. Celles-ci sont désormais rassemblées au sein du Système national des données de santé (SNDS) créé par la Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé (*JORF* n°0022 du 27 janvier 2016). Sur ce point v. notamment J. BOSSI-MALAFOSSE, « Les nouvelles règles d'accès aux bases médico-administratives : quel effet sur l'ouverture des données ? », *I2D Information, données & documents* 2016/3, Vol. 53, p. 84.

[747] Etant couvert par le secret, « *l'ensemble des informations concernant la personne venue à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes* » (art. L. 1110-4 CSP), les informations recueillies lors de la prise en charge d'un malade peuvent concerner des informations diverses qui ne sont pas seulement relatives à l'état de santé de la personne, elles sont donc toutes susceptibles d'être qualifiées de données sensibles.

[748] I. DE LAMBERTRIE, « Qu'est-ce qu'une donnée de santé ? », *RGDM*, *in numéro spéc.* « Le droit des données de santé », LEH, 2004, p. 11, *spéc.* p. 18.

[749] V. par exemple C. ZORN, *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, coll. « Santé, qualité de vie et handicap », PUN, 2010, n° 9 qui reprend la définition proposée par le Groupe européen d'éthique des sciences et des nouvelles technologies auprès de la commission européenne (GEE) (GEE, *Aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information*, 1999) qui définit les données de santé comme étant les « *données médicales de base (historique des interventions médicales subies par l'intéressé, médicaments qui lui ont été prescrits, résultats d'analyses diverses biologiques, radiologiques, [ou autres], mais aussi des données individuelles sensibles, telles que celles relatives à l'état psychique de la personne, à ses antécédents familiaux, à ses habitudes de vie, y compris sa vie sexuelle, sociale et économique), comme à des données administratives en rapport avec les premières (admissions dans des établissement de santé et décharges établies lors de ces admissions, données opérationnelles de routine, conditions d'assurance de la personne et autres données financières* ». Cette définition large était également retenue par I. DE LAMBERTRIE (I. DE LAMBERTRIE, « Qu'est-ce qu'une donnée de santé ? », *op. cit.*, p. 19).

[750] Art. 4 15° RGPD.

dès 2003 par la Cour de justice de l'Union européenne[751]. Elle renvoie évidemment aux informations relatives à l'état de santé de la personne lors d'un parcours de soins mais « *cette notion recouvre non seulement l'ensemble des données découlant des parcours de soins mais aussi celles qui, détenues par d'autres acteurs qu'ils soient techniciens (par exemple, les développeurs informaticiens) ou administratifs (par exemple, les gestionnaires de droits sociaux) constituent une information sur l'état de santé de la personne* »[752]. Par ailleurs elle : « […] *traduit un concept plus large de la donnée de santé prenant en compte le fait que la prise en charge sanitaire d'une personne emporte également la connaissance de sa situation familiale ou sociale et fait intervenir des acteurs multiples, professionnels de santé et personnels sociaux* »[753]. Il est en effet nécessaire de lire cette définition au regard du considérant 35 du RGPD qui précise « *Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro* »[754]. Ainsi, les informations couvertes par

---

[751] Retenant qu'étaient des données relatives à la santé l'indication du fait qu'une personne s'est blessée au pied et est en congé maladie partiel : CJCE, 6 nov. 2003, aff. C*101/01, *Bodil Lindvist*, *D.* 2004, p. 1062, obs. L. BURGOGUE-LARSEN; *RSC* 2004, p. 712; obs. L. IDOT; *Europe*, 2004, comm. 18, note F. MARIATTE; *RLDC* janv. 2004, p. 29, note G. MARRAUD DES GROTTES ; *Comm. com. electr.* 2004, Comm. 46, note R. MUNOZ.
[752] D. BOURCIER et P. DE FILIPPI, « Vers un droit collectif sur les données de santé », *op. cit.*
[753] D. BOURCIER et P. DE FILIPPI, « Vers un droit collectif sur les données de santé », *op. cit.*
[754] Consid. n° 36 du RGPD.

le secret professionnel dans le domaine de la santé peuvent être qualifiées de données de santé au sens du RGPD[755]. Il en est également ainsi des informations relatives au remboursement des prestations de soins[756], des informations médico-administratives contenues dans les systèmes d'information hospitalier ou de santé[757] ainsi que, par exemple, celles contenues dans les biobanques[758]. De plus, la définition et les précisions données par le RGPD invitent à considérer que les données de santé ne sont pas uniquement des données issues de la relation de soin[759]. Certains auteurs avaient proposé de restreindre la notion de données de santé aux seules données issues de la relation de soin afin de favoriser la circulation des autres données de santé[760]. Il apparaît néanmoins que l'expression *données médicales* est parfois utilisée par le

---

[755] En ce sens J. BOSSI MALAFOSSE : « *Celle-ci couvre désormais toutes informations relatives à l'identification du patient dans le système de soin ou le dispositif utilisé pour collecter et traiter des données de santé, toutes informations obtenues lors d'un contrôle ou d'un examen médical y compris des échantillons biologiques et des données génomiques, toutes informations médicales* […]. *Cette nouvelle définition traduit un concept plus large de la donnée de santé prenant en compte le fait que la prise en charge sanitaire d'une personne emporte également la connaissance de sa situation familiale ou sociale et fait intervenir des acteurs multiples, professionnels de santé et personnels sociaux* » (J. BOSSI MALAFOSSE, « Le règlement européen et la protection des données de santé », *Dalloz IP/IT* 2017, p.260).

[756] La sensibilité des données contenues dans le Système National d'Information Interrégimes de l'Assurance Maladie (ci-après SNIIRAM) a encore été soulignée récemment par la CNIL, à l'occasion d'une mise en demeure adressée à la caisse nationale d'assurance maladie des travailleurs salariés (ci-après CNAMTS) : « […] *la particulière sensibilité des données traitées par la CNAMTS, à savoir les actes médicaux, feuilles de soins et séjours hospitaliers qui révèlent les données de santé de patients très hautement identifiables par la présence de multiples informations : âge, code postal, date de soins, médecin traitant etc.* » (Délibération de la CNIL n° 2018-050 du 15 février 2018 décidant de rendre publique la mise en demeure n° MED-2018-006 du 8 février 2018 prise à l'encontre de la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés).

[757] Les systèmes d'information informatisés seront évoqués ultérieurement (v. *infra* n° 369).

[758] Sur ce sujet v. F. BELLIVIER et C. NOIVILLE, *Les biobanques*, coll. Que sais-je ?, PUF, 2009. Les biobanques (publiques ou privées) constituent des « *ensembles d'échantillons biologiques et de données associées* » (*Ibid.* p.18) dont la revitalisation (par rapport aux collections anciennes du vivant) tient au « *renforcement de la santé publique, d'une part, l'intérêt scientifique renouvelé recélé par les échantillons biologiques humains, d'autre part* » (*Ibid.*). Les échantillons et les données y afférant proviennent de « […] *la pratique médicale, qu'elle soit à visée thérapeutique, diagnostique ou pronostique* » (*Ibid.* p. 33) et de la recherche biomédicale, « *dans ce cas de figure, le prélèvement des échantillons et leur réunion en banque ne constituent plus l'accessoire d'un geste médical mais une activité et un but en eux-mêmes, spécifiquement menés à des fins de recherche* » (*Ibid.* p. 34). Les informations, dans le cadre de recherches, seront collectées en même temps que les échantillons biologiques ou génétiques, mais il arrive également que ces informations soient « *récupérées de documents préexistants : registres épidémiologiques, archives de médecins de ville, données généalogiques* » (*Ibid.* p. 35).

[759] Ce que souligne F. EON « *Les grands enjeux en termes de protection des données sont différents selon que les initiatives de génération de ces données proviennent d'acteurs « traditionnels » du monde de la santé (professionnels, autorités de santé, laboratoires) ou sont décidées par les individus eux-mêmes. Dans ce dernier cas, les données, même partagées par l'utilisateur, n'engagent que lui* » (F. EON, « Objets connectés : comment protéger les données de santé ? », *RLDI*, 1er avril 2016, nº 125).

[760] « *Dans une logique* […] *d'accès massif et facilité aux données de santé, la tentation est tout aussi grande de limiter la quantité des données susceptibles d'être appréhendées comme relevant de la santé. Ne relèverait ainsi de cette catégorie que les informations qui se rapportent strictement et directement à l'état de santé ou révèlent de cet état de santé. Suivant cette conception, la protection ne pourrait être accordée qu'aux informations médicales* » (I. COULIBALY, *La protection des données à caractère personnel dans le domaine de la recherche scientifique*, th. dact., ss. la dir. de E. VERGES et I. DE LAMBERTRIE, soutenue le 25 novembre 2011, Université

législateur et qu'elle correspond aux informations recueillies dans le cadre des soins[761]. Outre cette mention, relevée dans des travaux préparatoires, le considérant 35 du RGPD ne dispose que d'une catégorie spécifique d'informations qui sont celles issues d'une prise en charge sanitaire. Si la définition *comprend* ces données, elle ne s'y réduit pas. Aussi, les données de santé, qu'elles proviennent ou non d'une prise en charge sanitaire, et qu'elles soient ou non couvertes par le secret professionnel, répondent-elles, en principe, au même régime.

148. Existence d'un régime spécifique pour le traitement des données à caractère personnel dans le domaine de la santé. Il faut noter, par ailleurs, que le législateur français a également prévu un régime spécifique pour le traitement des données à caractère personnel dans le domaine de la santé[762]. Il ne s'agit pas uniquement d'une subtilité de langage mais d'une volonté d'encadrer spécifiquement le traitement des données issues de la prise en charge des personnes dans le domaine de la santé. Cette distinction, résultant de la modification de la loi informatique et libertés en 1994[763], tient au fait que les données à caractère personnel issues de cette prise en charge (et non pas seulement des données de santé) sont couvertes par le secret professionnel. La loi informatique et libertés prévoyait donc, dès cette date, un régime particulier accompagné d'une dérogation au secret professionnel médical. En d'autres termes, la législation française distingue la nature des données et leurs sources, ce qui entraine également une distinction de régime. Avant d'envisager le régime de traitement de ces données il est nécessaire de tenter de déterminer dans quelles mesures les informations couvertes par le secret peuvent être qualifiées données de santé au sens des dispositions relatives à la protection des données.

Grenoble Alpes, p. 382). Les données de santé recoupant alors complètement les informations couvertes par le secret, elles « *se caractérisent par le fait qu'il s'agit de données à caractère personnel ou d'informations protégées par le secret médical* » (P. PEDROT (ss. la dir.), *Dictionnaire de droit de la santé et de la biomédecine*, Ellipses, 2007, p. 161).

[761] Dans le rapport fait à l'occasion du projet de loi relatif à la protection des données personnelles par la député S. JOISSAINS, le terme « données médicales » est utilisé pour qualifier les données « *relevant de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé* », S. JOISSAINS, Rapport fait au nom de la Commission des lois sur le projet de loi relatif à la protection des données personnelles, n°350, 14 mars 2018, p.48.

[762] Désormais prévu aux articles 64 et svt. de la LIL.

[763] Loi n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

149. Toutes les données de santé ne sont pas des informations à caractère secret. Un élément d'identification de la personne, tel qu'un symbole ou un numéro utilisé à des fins de santé[764], peut entrer dans le champ d'application des dispositions relatives à la protection des données à caractère personnel. Or, la révélation d'un symbole ou d'un numéro attribué à un malade, par un professionnel soumis au secret, ne constitue pas systématiquement une révélation punissable au sens de l'article 226-13 du Code pénal. Cela se conçoit d'autant plus que la révélation de l'identité d'un malade – par exemple son nom – ne constitue pas systématiquement une révélation punissable. Ce n'est pas tant l'identité de la personne qui est couverte par le secret que l'élément de connaissance attaché à celle-ci[765]. Si le secret professionnel contribue à la protection des données à caractère personnel, les dispositions relatives à la protection des données protègent à la fois la vie privée – en considérant les données de santé comme des informations personnelles relatives à la santé – mais également l'identité des personnes – en protégeant les éléments d'identification à des fins de santé – des potentialités de l'informatique. Un auteur, pour différencier le champ d'application matériel des dispositions relatives à la protection des données et le domaine de la vie privé explique que « *l'identification possible de la personne compense le caractère non manifestement personnel de l'objet de l'information* »[766].

150. Le cas particulier du Numéro d'inscription au répertoire des personnes physiques de l'INSEE (ci-après NIR). Dans le RGPD le traitement du NIR fait l'objet d'une marge de manœuvre, son utilisation étant simplement conditionnée au respect « *des garanties appropriées pour les droits et libertés de la personne concernée* »[767]. Le NIR est un identifiant national, unique (il ne peut en être changé) et pérenne. Ce numéro figure au sein du *Répertoire national d'identification des personnes physiques* (RNIPP) qui est tenu par l'INSEE depuis

---

[764] Consid. n° 36 du RGPD.
[765] En ce sens D. GUTMANN lorsqu'il affirme que la vie privée relève de la connaissance (D. GUTMANN, « Du matériel à l'immatériel dans le droit des biens. Les ressources du langage juridique », *Arch. phil. droit* 1999, n° 43, pp. 65-78, *spéc.* p. 77).
[766] M. BENEJAT à propos d'une délibération de la CNIL (Délibération n° 89-35 du 25 avril 1989 portant avis sur le projet d'arrêté du ministre de la Solidarité, de la Santé et de la Protection sociale relatif à l'informatisation des bulletins statistiques d'interruptions volontaires de grossesse) dans laquelle la Commission avait notamment demandé la suppression de certains éléments pouvant faciliter l'identification de la personne et donc pouvant permettre, par recoupement, d'acquérir des connaissances sur les personnes concernées (M. BENEJAT, *in Droits de la personnalité*, *op. cit.*, n° 937).
[767] Art. 87 du RGPD.

1946[768]. Il est utilisé par la sécurité sociale afin de mettre en œuvre les prestations afférentes[769]. Il est composé de quinze chiffres qui sont signifiants puisqu'ils permettent de déterminer le sexe, le mois, l'année et le lieu de naissance ou une naissance à l'étranger. Sa conservation après la mort de la personne en fait un « *numéro clef de la reconnaissance de l'existence sociale* »[770]. Il se différencie donc de toutes les autres données en ce qu'il touche à l'existence, non pas biologique, comme le sont les informations génétiques ou biométriques, mais sociale. Contrairement au nom, par exemple, il ne peut jamais être modifié, ce qui en fait un élément consubstantiel à toute personne née en France. Ce n'est donc pas tant son traitement par les acteurs privés – comme pour de nombreuses autres données – qui suscite des inquiétudes. En effet, le recueil et le traitement du NIR n'a aucun intérêt si rien ne permet de consulter les informations qui y sont rattachées dans les différents secteurs qui l'utilisent, autrement dit : c'est le recoupement des fichiers qui permet d'avoir une vue d'ensemble sur la vie sociale de l'individu. Le sexe, la date et le lieu de naissance sont des données à caractère personnel qui peuvent être collectées et traitées dans des conditions relativement souples[771], aussi ce ne sont pas tant les informations qu'il donne sur la personne qui importent que la possibilité pour les administrations de l'Etat de recourir au NIR pour interconnecter les fichiers dont elles disposent sur les individus[772].

---

[768] A l'origine du recensement : R. CARMILLE, *La Mécanographie dans les administrations*, Recueil Sirey, Paris, 1936.

[769] Art. L. 114-12-1 al. 5 CSS (modifié par Loi n°2018-898 du 23 octobre 2018 - art. 6) : « *Le répertoire contient les données communes d'identification des individus, les informations relatives à leur affiliation aux différents régimes concernés, à leur rattachement à l'organisme qui leur sert les prestations ou avantages, à la nature de ces derniers, l'adresse déclarée aux organismes pour les percevoir, ainsi que les informations permettant d'attester du respect des conditions de résidence. Au 1er janvier 2016, il contient également le montant des prestations en espèces servies par les organismes mentionnés au premier alinéa* ».

[770] J. THOMAS, « Le fichier et l'inclusion de l'individu au sein de la collectivité », *in* F. EDDAZI et S. MAUCLAIR (ss. la dir), *Le fichier*, Actes du colloque organisé les 26 et 27 novembre 2015, par le Centre de recherche juridique Pothier de l'Université d'Orléans, coll. Grands colloques, LGDJ, p. 204.

[771] Il s'agit en effet de données à caractère personnel les conditions de traitement sont prévues à l'article 6 et svt. de la loi informatique et libertés modifiée par la Loi n° 2018-493 du 20 juin 2018.

[772] Ce qui aurait pour conséquence d'en faire un identifiant unique. Le Sénat dresse un panorama de la position des Etats européens dans un document de travail v. SENAT, *Le numéro unique d'identification des personnes physiques*, Les Documents de travail du Sénat, n° LC 181, déc. 2007.

Aussi la CNIL a-t-elle toujours adopté « *une politique de cantonnement* »[773] de l'utilisation du NIR. La question de sa qualification juridique au regard des dispositions relatives à la protection des données à caractère personnel, en l'absence d'une détermination exprès dans la loi informatique et libertés, a pu interroger et a donné lieu à des réponses différentes selon les instances amenées à se prononcer[774]. Pourtant, la particularité des conditions de son *utilisation* – opération de traitement *seconde* qui suppose un accès au répertoire – définies à l'article 30 de la LIL, permet d'affirmer qu'il s'agit de données dont la sensibilité impose un encadrement plus strict encore que celui prévu pour les données sensibles, au même titre que les données génétiques[775]. Ce que confirme la CNIL dans une délibération du 19 janvier 2017[776] relative à l'utilisation du NIR comme identifiant de santé et à l'occasion de laquelle la Commission désigne le NIR comme une donnée *particulièrement sensible*. Cette qualification se trouve également dans les travaux préparatoires de la loi du 20 juin 2018[777]. Le RGPD ayant laissé aux Etats la possibilité, à la faveur d'une marge de manœuvre[778], de décider des conditions spécifiques de traitement de ce numéro, la législation nationale est demeurée particulièrement protectrice et la CNIL en constitue le garde-fou. Au stade de notre analyse, il convient de relever que le NIR, dont l'utilisation a été longtemps cantonnée à la sécurité sociale

---

[773] CNIL, Rapport d'activité 2013, p. 11, disponible sur < https://www.cnil.fr/sites/default/files/typo/document/CNIL_34e_Rapport_annuel_2013.pdf> (dernière consultation le 14 oct. 2019).

[774] Comme le constatait C. ZORN (C. ZORN, *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, *op. cit.*, n°322-323) le Conseil d'Etat, à l'occasion d'une demande d'annulation pour excès de pouvoir du décret n° 2005-1624 du 22 décembre 2005 relatif au suivi de la recherche d'emploi, n'avait pas explicitement affirmé que le NIR était une donnée à caractère personnel, pas plus d'ailleurs qu'il n'est explicitement qualifié par l'ancien article 27 de la loi informatique et libertés. A l'inverse, le groupe de travail des CNIL européennes (G29) avait quant à lui proposé de qualifier le numéro d'identification, eu égard à son utilisation comme numéro de sécurité sociale et donc sa mention dans les dossiers médicaux des individus, comme une donnée sensible (Groupe de travail "article 29" sur la protection des données, *Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)*, Commission européenne, 2007). L'article 2 modifié par la Loi du 20 juin 2018 relative à la protection des données personnelles (Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *op.cit.*), n'a pas apporté plus de précisions sur cette qualification.

[775] V. *infra* n° 174 et svt.

[776] CNIL, délib. n° 2017-014 du 19 janvier 2017 portant avis sur le projet de décret relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant de santé (demande d'avis n°16024670).

[777] V. S. JOISSAINS, *Rapport fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif à la protection des données personnelles*, n° 350, p. 67.

[778] RGPD, art. 87

et à ses partenaires habituels[779] que sont notamment les personnes et les établissements intervenant dans le système de santé est désormais, après de nombreuses tergiversations[780], utilisé comme identifiant national de santé[781].

151. Le NIR, une information couverte par le secret ? La question peut surprendre dans la mesure où nous avons pu expliquer que toutes les informations couvertes par le secret au regard de l'article L. 1110-4 du Code de la santé publique sont également des données personnelles de santé ou sensibles, tout en admettant qu'une donnée isolée ne peut pas être considérée comme une information et qu'ainsi la révélation d'une donnée ne peut constituer une violation du secret professionnel. Notre démarche consistait donc à savoir dans quelle mesure les champs d'application de ces mécanismes de protection différents se recoupaient. Toutefois, si la révélation d'une simple suite de chiffres ne peut sans doute pas être qualifiée de révélation d'une information à caractère secret au sens de l'article 226-13 du Code pénal[782], le NIR est *signifiant*. Dès lors qu'il est attaché à des informations relatives à la santé des personnes il les rend identifiables. Partant, l'ensemble de ces informations, représentées et désormais traitées informatiquement, seront protégées afin d'assurer le *secret des informations relatives au malade*.

152. La protection du secret-état par les dispositions relatives à la protection des données à caractère personnel. La démarche entreprise au sein de ce développement consistait à savoir dans quelle mesure les informations couvertes par le secret peuvent également être

---

[779] J. THOMAS, « Le fichier et l'inclusion de l'individu au sein de la collectivité », *in* F. EDDAZI et S. MAUCLAIR (ss. la dir.), *Le fichier*, *op. cit.*, p. 204. En effet, cet identifiant est déjà utilisé pour la gestion administrative et médicale des professionnels et établissements de santé, dans le cadre de leurs relations avec l'assurance maladie.

[780] C. ZORN, *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, *op. cit.*, n° 324 et svt.

[781] La loi n°2016-41 du 26 janvier 2016 et décret d'application n° 2017-412 du 27 mars 2017, L 1111-8 et article R 1111-8-1 à 7 du CSP consacre l'utilisation du NIR comme identifiant de santé. La politique de la CNIL s'est donc infléchie sur ce point, puisqu'en 2007 elle avait rendu un avis favorable à la création d'un identifiant distinct généré à partir du NIR (Conclusions de la commission nationale de l'informatique et des libertés sur l'utilisation du NIR comme identifiant de santé, 20 février 2007). Dans son rapport relatif aux droits fondamentaux et au numérique, le Conseil d'Etat avait notamment proposé, à la suite d'un assouplissement de la position de la CNIL à partir de 2013 (CNIL, *Rapport d'activité 2013*, p. 10), un assouplissement de la loi afin que le NIR puisse être utilisé comme identifiant national de santé (Rapport du Conseil d'Etat, *Le numérique et les droits fondamentaux*,2014, p. 298). Sur les conséquences de son utilisation comme identifiant de santé v. F. EON, « La donnée au cœur de l'e-santé », *Expertises des systèmes d'information* 2016, n°419, p. 405.

[782] Que l'on considère que l'information est secrète en raison de la profession du déposant ou en raison de sa nature il demeure qu'elle doit porter sur une personne identifiable. Cette affirmation pourrait être relativisée si le NIR est révélé en plus du nom de la personne puisque le numéro est signifiant.

qualifiées de données à caractère personnel et de données sensibles. Nous avons ainsi pu affirmer que toutes les informations à caractère secret au sens de l'article L. 1110-4 du Code de la santé publique sont des données à caractère personnel et des données sensibles mais ces dernières ne sont pas nécessairement des informations dont la révélation est susceptible d'être sanctionnée au regard de l'article 226-13 du Code pénal. Nous en tirons un enseignement : le caractère compréhensif de la définition des données à caractère personnel et des données sensibles permet de faire entrer dans le champ d'application des dispositions relatives à la protection des données à caractère personnel, des éléments qui, sans être des informations à caractère secret, conditionnent la préservation du secret des informations relatives à la personne prise en charge par un professionnel intervenant dans le système de santé. Partant, les dispositions relatives à la protection des données à caractère personnel participent de la protection de l'état de secret, composant du « secret médical ».

§ 2 - Le traitement des données à caractère personnel dans le domaine de la santé

153. Le régime attaché à la protection des données à caractère personnel ne s'applique que dans la mesure où elles font l'objet d'un traitement. La notion de traitement détermine donc également le champ d'application matériel des dispositions relatives à la protection des données à caractère personnel, que celles-ci soient, ou non, sensibles. Comprendre ce que désigne le traitement impose de distinguer la nature des traitements **(A)** des opérations qui peuvent être qualifiées de traitement **(B)**.

A - La notion de traitement

154. Traitement automatisé ou traitement non automatisé. L'article 4 du RGPD portant sur le champ d'application matériel de l'Union précise que le règlement s'applique « *aux traitements automatisés en tout ou partie de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers* »[783]. Cette partie de la disposition a été insérée dans la loi informatique et libertés par la loi du 20 juin 2018, à l'article 2 au sein du premier titre portant sur les dispositions

[783] RGPD art. 4 2) première partie de la définition.

communes[784]. La précision apportée selon laquelle la loi s'applique aux *traitements automatisés en tout ou partie* n'engendre pas de transformation majeure quant au champ d'application matériel de la protection des données personnelles par rapport au droit national antérieur. En effet, avant la transposition de la directive de 1995 les traitements non automatisés n'étaient soumis aux dispositions nationales que lorsqu'ils étaient contenus ou appelés à figurer dans un fichier. Le traitement qui n'était pas informatisé, par exemple une collecte d'informations par le biais d'un questionnaire papier, n'entrait dans le champ de la LIL que si ce traitement avait vocation à intégrer un fichier. La question reposait donc principalement sur la définition des

[784] La particularité du RGPD tient aux très nombreuses marges de manœuvre laissées aux Etats membres. La loi informatique et libertés contient donc des dispositions qui lui sont propres et qui ont été, en quelques sorte, transposées au regard de ces marges. Ensuite, certaines dispositions d'application directe ont été insérées au titre I de la loi nationale portant « dispositions communes ». L'entrée en vigueur du Règlement a donné lieu à quelques difficultés. Le législateur a d'abord uniquement procédé *« aux modifications strictement indispensables à la mise en œuvre du RGPD […] (élimination des dispositions nationales manifestement contraires au règlement, introduction des nouvelles missions nécessaires à la CNIL, etc.)* » (S. JOISSANS, Rapport fait au nom de la commission des lois sur le projet de loi adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif à la protection des données personnelles, *op. cit.*, pp. 24-25). Jusqu'à l'ordonnance de réécriture de la loi informatique et libertés (Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel), trois niveaux de règles ont coexisté. D'abord les dispositions du Règlement ne consistant pas en des marges de manœuvre s'appliquaient directement tandis que certaines dispositions avaient continué de figurer dans le texte de la LIL de manière symbolique mais n'étaient plus applicables, par ailleurs le texte de la loi du 10 juin 2018 (*ibid.*) avait transposé une directive relative aux traitements mis en œuvre en matière policière et judiciaire (Directive UE 2016/680). La loi informatique et libertés a donc souffert d'un manque de lisibilité reproché par la CNIL (Délibération n° 2017-299 du 30 novembre 2017 de la CNIL portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janv. 1978 ; disponible en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/projet_davis_cnil.pdf>, dernière consultation le 14 oct. 2019) et le Conseil d'Etat (Avis n° 393836 CE, disponible en ligne : <file:///C:/Users/olech1/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/avis_ce_jusc1732261_cm_13.12.2017.pdf >, dernière consultation le 14 oct. 2019). Egalement critiqué par la doctrine : *CCE* 2018. Étude 17, obs. A. DEBET et N. METALLINOS ; *RFDA* 2018. 1101, obs. L. CLUZEL-METAYER et E. DEBAETS ; N. MARTIAL-BRAZ, « L'abus de textes peut-il nuire à l'efficacité du droit ? », *Dalloz IP/IT* 2018, p. 459. Le caractère inopportun du maintien symbolique de la loi informatique et libertés en raison du changement de paradigme du RGPD était notamment souligné. L'ordonnance de réécriture a permis d'évacuer quelque peu la complexité du dédale textuel sans la faire disparaître. Les nombreux renvois vers le RGPD mais également vers divers Code nationaux rendent la lecture des dispositions peu fluide. Un décret d'application est intervenu le 29 mai 2019, il comporte quelques 150 articles, les renvois y sont allègrement utilisés (Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). La lecture et la compréhension de l'ensemble de ces dispositions est donc toujours un exercice fastidieux (pour un panorama général de la première année d'application du RGPD et de la nouvelle loi informatique et libertés v. C. ZOLYNSKI et W. MAXWELL, « Protection des données personnelles. juin 2018 – juillet 2019 », *D.* 2019, p. 1673), au point qu'il a semblé utile de regrouper les textes au sein d'un code, il s'agit néanmoins d'une codification éditoriale (*Code de la protection des données personnelles 2020*, annoté et commenté par E. GEFFRAY et A. GUERIN-FRANÇOIS, 2eme éd., Dalloz).

contours du *fichier* [785]. La directive de 1995 a ensuite prévu que les dispositions relatives à la protection des données s'appliquaient aux traitements même partiellement automatisés. Le législateur français n'avait pas transposé cette formule. Toutefois la lecture combinée des articles de la LIL permettait de pallier une éventuelle lacune : l'ancien article 6 de la loi prévoyait que les données personnelles devaient être collectées au regard de finalités déterminées. Cette exigence est un principe cardinal du droit à la protection des données à caractère personnel et figure à l'article 2 de la loi nationale et du RGPD. Aussi, la collecte par des moyens non automatisés entrait-elle déjà dans le champ de la LIL dès lors que la finalité devait être déterminée et donc contrôlée par la CNIL afin, justement, de pouvoir prévoir de futures utilisations[786]. En somme, le changement opéré par la loi du 20 juin 2018 relative à la

---

[785] Ce qui avait notamment donné lieu - avant la directive de 1995 qui a finalement donné une définition des fichiers - à quelques discussions sur la définition du terme fichier et sur la distinction entre un fichier et d'autres objets s'en approchant. V. par exemple sur le contenu d'un cahier (TGI Créteil, 10 juill. 1987, *DS* 1988, p. 319, note J. FRAYSSINET). Mais ce sont les dossiers qui ont posé le plus de problèmes et la question de savoir si un dossier constituait un fichier. Il avait pu être jugé qu'un ensemble de dossiers papier ne constituait pas un fichier et que les notions de dossier et de fichier s'excluaient l'une l'autre (TGI de Nantes, 16 décembre 1985, D. 1986, jurispr. 471, note J. FRAYSSINET ; JCP E 1986.II.15791, obs. M. VIVANT et A. LUCAS ; CA Rennes, 24 juin 1986, Crim., 3 novembre 1987), la CNIL (8e rapport d'activité de la CNIL, 1987, p. 30) de même que la doctrine (M. VIVANT *et alii*, *Droit de l'informatique*, Lamy 1990, n° 1368 ; M. VIVANT et A. LUCAS, *JCP E* 1988, II, 15308, note H. MAISL ; J.-P. DOUCET, *Gaz. Pal.* 1988,1, 234 ; J. FRAYSSINET, « Contre l'excessive distinction entre fichier et dossier, le pas en avant du Tribunal de grande instance de Paris, *Cahier Lamy* 1989, E, p. 3; *contra* R. GASSIN « Commentaire du jugement de Tribunal correctionnel de Paris, du 2 mars 1989 ou de la distinction des fichiers nominatifs et des dossiers individuels », *Cahier Lamy* 1989, J, p. 9). Les fichiers ont ensuite été définis à l'occasion de la transposition de la directive de 1995 par la loi du 6 août 2004 (Loi n° 2004-801 du 6 août 2004 relative à la protection de personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 *op. cit.*) puis le RGPD est venu compléter cette définition : « *Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique* » (art. 4 du RGPD et art. 2 de la LIL modifié par la Loi n° 2018-493 du 10 juin 2018 relative à la protection des données personnelle, *op. cit.*, mais conservée symboliquement).

[786] Sur ce point v. par exemple l'avis du Commissaire du gouvernement au sujet de la légalité du décret n° 99-362 du 6 mai 1999 fixant les modalités de transmission à l'autorité sanitaire de données individuelles concernant les maladies visées à l'article L. 11 du Code de la santé publique et modifiant le Code de la santé publique. Dans le cadre d'une demande d'annulation pour excès de pouvoir introduite par Ligue française pour la défense des droits de l'homme et du citoyen, le Commissaire du gouvernement avait notamment soulevé la question de savoir si une collecte par voie postale ou par téléphone constituait un traitement de données au sens de LIL et de la directive de 1995 non encore transposée, il constatait alors : « *Certes, la simple collecte de données ne constitue pas un traitement au sens de la loi du 6 janvier 1978, qui définit la notion de traitement automatisé d'informations nominatives comme* « un ensemble d'opérations réalisées par des moyens automatiques », *même si certaines dispositions de la loi s'appliquent à la collecte*. *Mais la directive est plus exigeante, puisqu'elle considère comme un traitement une opération même isolée, qui peut être la collecte, et non pas seulement une chaîne d'opérations. Au surplus, la directive affirme à son article 6 que les données à caractère personnel doivent* être « collectées pour des finalités déterminées » *et* « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ». *Cela implique bien un contrôle dès le stade de la collecte, pour éviter notamment de rassembler des informations qui seraient inutiles au regard des finalités poursuivies. Telle est d'ailleurs l'opinion émise par le président Braibant dans son rapport remis au Premier ministre en février 1998, à propos de la transposition de la directive en droit français, qui affirme que* « les

protection des données personnelles n'engendre pas de changement significatif quant au champ d'application mais cela permet, à l'avenir, d'éviter toute discussion en se référant à la finalité de la collecte[787]. Pour finir de déterminer le champ d'application matériel de loi, il faut également définir les opérations qui constituent des traitements de données au sens du RGPD.

B - Distinction des opérations constituant un traitement : le temps et l'espace

155. Les opérations constituant un traitement. La seconde partie de la définition du « traitement » visé à l'article 4 2) du RGPD précise les opérations constituant un traitement : « *la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* »[788]. Le RGPD reprend la définition issue de la directive de 1995[789]. Le champ de la protection des données est donc particulièrement large en ce que toutes les opérations sur les données constituent un traitement. Par ailleurs la définition des données de santé concerne toutes les informations que la personne fournit à l'occasion de sa prise en charge par un professionnel intervenant dans le système de santé. Partant, toutes les opérations *automatisées en tout ou partie* et effectuées sur des

---

opérations de collecte des données constituent en elles-mêmes un traitement » et met en évidence cette différence entre notre législation actuelle et la directive (Données personnelles et société de l'information, La Documentation française, 1998, p. 78). Ajoutons qu'il s'agit bien d'un traitement entrant dans le champ de la directive, tel qu'il est défini à son article 3, selon lequel « *la présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* ». *En l'espèce, le décret ne traite que de la collecte des données, effectuée essentiellement par voie postale ou téléphonique sans automatisation. Toutefois, eu égard aux finalités assignées par la loi à cette collecte, il est évident que les informations collectées feront l'objet de fichiers, que ce soit pour assurer le traitement statistique des données à des fins de conduite de la politique de santé publique ou pour prendre les mesures de prévention nécessaires* » (P. FOMBEUR, « Un décret d'application ne peut renvoyer à un arrêté ultérieur la mise en œuvre des principes de la loi », *AJDA* 2000, p. 831). En somme, après la transposition de la directive de 1995, même en l'absence de la précision que la loi s'applique au traitement automatisé en tout ou partie, la LIL s'appliquait à toutes formes de collecte de données. La question de savoir si les informations étaient appelées à figurer dans un fichier devenait alors inutile.

[787] Ainsi, à l'adresse des professionnels libéraux, un guide conjointement rédigé par la CNIL et le Conseil national de l'ordre des médecins précise que les dispositions du RGPD s'appliquent dès lors que les professionnels utilisent dans le cadre de leur activité, un logiciel fourni par un prestataire informatique pour tenir ses dossiers patients, ou que ces professionnels tiennent un dossier patient sous format papier (CNIL et CNOM, *Guide pratique sur la protection des données personnelles*, juin 2018, p. 4-5, disponible en ligne : < https://www.cnil.fr/sites/default/files/atoms/files/guide-cnom-cnil.pdf > (dernière consultation le 14 oct. 2019)).

[788] RGPD art. 4 2).

[789] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, op. cit.

informations couvertes par le secret professionnel et dont la révélation par les personnes visées à l'article L. 1110-4 du Code de la santé publique est sanctionnée par l'article 226-13 du Code pénal, entre dans le champ du RGPD. Aussi, les établissements de santé publics ou privés, les établissements médico-sociaux ainsi que les professionnels libéraux, les fournisseurs de services numériques en santé et tous les acteurs de santé, peu important leur statut dès lors qu'ils traitent de telles données, doivent-ils répondre aux exigences posées par le RGPD dès lors qu'ils sont, à ce titre, responsables de traitement ou sous-traitants[790].

156. Les rapports entre les opérations de traitement et le secret des informations relatives aux personnes prises en charge par un professionnel intervenant dans le système de santé. La *collecte*, le *stockage*, l'*enregistrement*, l'*organisation*, la *conservation*, l'*adaptation* ou la *modification des données* constituent des traitements de données dont les fonctions premières sont la *mémorisation* de l'information et la *connaissance*. La mémorisation est une fonction également remplie par les supports papier. Les « dangers » à l'origine de la loi informatique et libertés apparaissent lorsque ces traitements forment des *fichiers*, et que la puissance informatique permet leur *interconnexion*[791]. La frontière entre connaitre et surveiller tend alors à s'effacer. Les inquiétudes portent aujourd'hui davantage sur le traitement des données de masse et ses conséquences, ce dont nous traiterons ultérieurement[792]. Pour l'instant, nous souhaitons souligner que ces deux premières fonctions des traitements de données doivent être distinguées d'une autre qui est de permettre le *trafic*[793] des données. S'agissant de cette dernière, les dispositions relatives à la protection des données s'appliqueront pour les opérations de traitement telles que le fait de *consulter*, d'*utiliser*, de *communiquer par transmission*, de *diffuser* ou de *mettre à disposition* sous n'importe quelle forme des données à caractère personnel. En ce sens l'on pourrait affirmer, dans un premier temps, que les dispositifs

---

[790] Au sens de l'art. 4 du RGPD est responsable du traitement : « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre* ».

[791] V. *infra* n° 311 et 320.

[792] Sur les théories mathématiques de l'information v. J. SEGAL, *Le zéro et le un*, coll. Sciences & philosophie, Editions Matériologiques, 2011.

[793] Le mot *circulation* généralement utilisé n'est sans doute pas le plus approprié pour qualifier le phénomène, la circulation supposant un mouvement circulaire et donc un retour au point de départ. Les informations ou les données ne suivent pas un tel mouvement, dès lors qu'elles recèlent un savoir, toute personne qui en prend connaissance ne peut « rendre » cette connaissance. Il serait sans doute plus exact de parler de *trafic* (en référence aux autoroutes de l'informations) ou de dissémination (qui correspond au mouvement actuel de réutilisation des données). La précision est importante car elle suppose, non pas un mouvement qui peut être mesuré, voire contrôlé, mais un processus qui, une fois amorcé, échappe aux individus qui en sont l'origine.

techniques permettant de traiter des données, tels qu'ils sont appréhendés par les dispositions relatives à la protection des données, ont une fonction de *mémoire/connaissance* et de *transport* des données. Il faut donc analyser les rapports entretenus entre ces opérations de traitement et le maintien du secret des informations relatives aux personnes prises en charge par un professionnel intervenant dans le système de santé dans ces deux dimensions.

Cette démarche a également une vertu méthodologique dans la mesure où elle nous permettra ensuite, selon les contextes, de découvrir ce qui est visé lorsque l'expression « secret médical » est utilisée dans le contexte du traitement des données à caractère personnel. Nous envisagerons donc les opérations de traitement selon une classification qui nous est propre : les opérations documentaires et de mémorisation **(1)**, puis des opérations supposant la communication ou la circulation des données **(2)**. Il s'agira enfin d'éprouver l'intérêt de différencier les opérations de traitement **(3)**.

1 - Les opérations documentaires et de mémorisation

157. Les opérations documentaires, la fonction de connaissance. La *collecte*, *l'enregistrement*[794], *l'organisation*, *l'adaptation* et *la modification* des données sont indissociables des finalités qui leurs sont assignées. Il ne s'agit pas des finalités du traitement telles que conçues par les dispositions relatives au traitement des données personnelles mais bien des finalités techniques de ces opérations. De ce point de vue, la finalité première de la collecte, du classement, de l'organisation, de l'adaptation et de la modification des données est la connaissance et l'organisation de ces connaissances. Sous cet angle, de telles opérations paraissent inoffensives pour les libertés mais comme l'explique un auteur : « *Les entreprises de classification et de classements présentent fréquemment un côté double tant les méthodes et outils d'organisation des connaissances sont souvent réutilisés dans des logiques d'indexation des existences qui forment davantage des dystopies ou contre-utopies de la surveillance* »[795].

---

[794] A propos de l'enregistrement, il a pu être décidé que ne constituait pas un traitement de données, le fait de retranscrire informatiquement un *listing* papier des patients d'un établissement dès lors que l'informatique n'était pas le support de cette liste, simplement retranscrite informatiquement pour être fournie à l'officier de police judiciaire à l'occasion d'une saisie : Crim., 6 juillet 1994, 93-83894, Bull. crim. n°267 (CNIL, *Rapport d'activité 1994*, p. 467).

[795] O. LE DEUFF, « Utopies documentaires : de l'indexation des connaissances à l'indexation des existences », *Communication & Organisation*, 2015/2, n°48, p. 93.

Ainsi, l'organisation des connaissances est toujours bifron. La recherche médicale et la pratique de la médecine clinique d'une part, puis l'évolution du système de santé d'autre part, imposent de connaître les patients d'une manière de plus en plus précise et parfois invasive. Si l'inquiétude liée à la surveillance de la population porte désormais sur l'atteinte à la vie privée lorsque la collecte des données de santé est effectuée par les géants du web[796], la question de la collecte de données et informations issues de la prise en charge médicale ou médico-sociale est différente. Cette organisation des connaissances par l'administration présente la particularité de porter en elle *le germe de l'action publique*[797]. Les données sont en effet collectées afin de *gérer*[798] le système de santé c'est-à-dire, de l'*administrer.* Ainsi les opérations de traitement visées interviennent en amont de la question du maintien du secret des informations dans le domaine de la santé et ont des conséquences en aval. En effet, le besoin de connaissance de l'administration va notamment influer sur le régime du secret professionnel[799]et faire une place grandissante à d'autres modes de régulation visant à protéger les informations couvertes par le secret[800]. Les enjeux politiques esquissent certaines évolutions dont nous traiteront ultérieurement[801].

158. De la connaissance au *New public management*[802]. Pour comprendre ce qui s'amorce au travers des éléments purement techniques, il faut introduire la notion de *New public*

---

[796] Sur la souveraineté numérique européenne et la concurrence mondiale entre les Etats et les GAFAM v. *infra* n°424 et svt..

[797] Nous visons ici ce que V. LASSERRE présente comme « *la puissance des données légitimantes* » (V. LASSERRE, *Le nouvel ordre juridique. Le droit de la gouvernance*, LexisNexis, 2015, n° 69 et svt.) et où l'auteur explique comment l'information est devenue un « *mode de légitimation de l'action publique* » (*Ibid.*n°76 et svt.) et un « *mode de « sociologisation » de l'action publique* » (*Ibidem.* n° 90 et svt.) notamment au travers de l'évaluation des lois (*Ibidem.* n° 91) mais également en amont à leurs production (*Ibidem* n° 78 et svt.).

[798] Le glissement de *l'administration* vers la *gestion* et le *management* est une question propre au *New management public*. Sur ce point v. P. DURAN, « Piloter l'action publique avec ou sans le droit ? », *Politique et management public*, 1993, n°4, pp. 1-45.

[799] V. *infra* Chapitre I Titre I Partie II .

[800] V. *infra* Titre II Partie II.

[801] V. *infra* Chapitre II Titre I Partie II.

[802] J. CHEVALLIER, *L'Etat post-moderne*, coll. « Droit et Société », 4ème éd., LGDJ, 2014, pp. 71-72 ; à propos du nouveau management public importé du management d'entreprise R. SALAIS énumère quelques méthodes « *pilotage par des indicateurs de performance, bonnes pratiques, benchmarking* » (R. SALAIS, « La donnée n'est pas un donné. Pour une analyse critique de l'évaluation chiffrée de la performance », *RFAP* 2010/3, n° 135, pp. 497-515), il précise que « *Ce qui importe pour ces méthodes, c'est le résultat, la performance. Les indicateurs sont utilisés pour mesurer la performance et pour classer, à des fins de mise en concurrence, les entreprises ou tout autre instance (organisation, politique…)* » (R. SALAIS, « Du bon (et du mauvais) emploi des indicateurs dans l'action publique », *Semaine sociale Lamy* 2006, 1272, p. 73 et svt.). Ce phénomène de rationalisation et d'efficacité s'est également étendu au droit (J. CHEVALLIER, *L'Etat post-moderne*, *op. cit.*) ; « *À la fin du XXe siècle, l'effectivité, l'efficacité et l'efficience se sont imposées comme des concepts fondateurs d'une logique juridique soumise à la puissance de la raison et de la science et au pragmatisme. L'effectivité exige une*

management : l'introduire, seulement, car nous ne pouvons tirer trop d'enseignements de la définition de ce que nous nommons les *opérations documentaires*. Nous avons formulé l'idée que, s'agissant du traitement des données ou informations relatives au malade, l'intérêt politique du recueil et du classement des données doit être appréhendé au travers du besoin de connaissance de l'administration. A ce titre les fichiers administratifs, dont les fichiers de santé[803], sont un point de départ éclairant. Monsieur Chevallier distingue trois utilités des fichiers administratifs comme instrument de l'action publique : *connaitre* « *pour réduire l'incertitude entourant la prise de décisions et rationaliser leur processus d'élaboration* »[804] ; *contrôler* lorsque les fichiers sont directement nominatifs (contrairement aux fichiers statistiques) car ils permettent une surveillance des individus et favorisent également l'action publique[805] ; *gérer* dans la mesure où les fichiers « *répondent à un souci d'efficacité, de rationalisation des tâches administratives et de réduction des coûts* »[806]. Ces trois utilités correspondent à une vision managériale de l'action publique - propre à l'Etat post-moderne - dans la mesure où elles participent à l'amélioration de la performance publique « […] *en permettant à l'administration d'atteindre les objectifs qui lui sont assignés par les autorités politiques à coût minimal* […] »[807]. Or, si l'Etat doit composer avec les dispositions relatives à la protection des données personnelles pour atteindre ses objectifs et rationnaliser ses efforts, le secret professionnel peut également constituer un frein à la connaissance qui conditionne toute gestion efficace du système de santé. Ces questions seront développées en amont, les opérations de traitement nous permettant de tracer les linéaments d'un mouvement que nous décrirons ensuite.

159. Le stockage ou l'externalisation de la mémoire, fonction évidente et trompeuse des dispositifs techniques. La première fonction que le sens commun prête aux dispositifs

---

comparaison entre les conduites réelles des destinataires au modèle normatif de comportement », V. LASSERRE, *Rep. civ.*, V° « Loi et Règlement », juill. 2015 (actu. janv. 2016), n° 218.

[803] Sur la collecte des données à caractère personnel de santé v. notamment F. GRANET, « Les fichiers sanitaires automatisés », *D.* 1995, p. 10 ; M.-C. PONTHOREAU, « La protection des personnes contre les abus de l'informatique », *RFDA* 1996, p. 796.

[804] J. CHEVALLIER, « Ficher, c'est encore administrer », *in* F. EDDAZI et S. MAUCLAIR (ss. la dir.), *Le fichier*, LGDJ, 2017, p. 129.

[805] *Ibid.* p. 129.

[806] *Ibid.* p. 134.

[807] J. CHEVALLIER, *L'Etat post-moderne*, *op.cit.,* p. 71.

techniques de l'information est celui de *mémorisation*, traduite dans les dispositions relatives à la protection des données comme des opérations de *stockage*. C'est en tout cas ce que laisse accroire le discours politique dans le domaine de la santé : il s'agit de ce que les chercheurs en sciences de l'information et de la communication nomment « *discours d'accompagnement* »[808] (discours qui a également diffusé la notion de *dématérialisation des informations, des données,* ou *des supports*). Un exemple récent et significatif peut témoigner de cette démarche discursive : en novembre 2018, le ministère de la santé a démarré une grande campagne de *relance* du Dossier Médical Partagé, le *slogan* de la campagne de communication, d'ampleur nationale, est ainsi formulé « *Dossier Médical Partagé (DMP) : la mémoire de votre santé* ». La fonction de mémoire de certains dispositifs techniques avait déjà été mise en avant dans les

[808] Les chercheurs en sciences de l'information et de la communication s'intéressent de longue date à ces productions discursives ayant pour but de développer l'utilisation des dispositifs techniques de l'information et de la communication à tous les niveaux de la société : « *Pour bien comprendre cette notion, il apparaît essentiel de distinguer entre le discours technique et le discours d'accompagnement d'une technique. Le discours technique est celui des spécialistes d'un domaine, à l'intérieur d'un système de compétence et d'action généralement inaccessible aux profanes. On le trouve dans les manuels techniques et plus généralement dans l'ensemble des interactions orales et écrites entre spécialistes à propos de l'invention et du fonctionnement des objets techniques. Le discours d'accompagnement est un ensemble d'énoncés caractérisés par le fait qu'ils sont tenus dans l'espace public et sont formés des commentaires extérieurs sur une technique, son emploi, le contexte et les conséquences de son usage* » (P. BRETON, « Que faut-il entendre par discours d'accompagnement des nouvelles technologies ? » *in Les dossiers de l'audiovisuel* mai-juin 2002, numéro spéc. « Les nouvelles technologies : quels usages, quels usagers ? », n° 103). Les travaux sur le sujet ont surtout une vocation de démystification (L. SFEZ, *Critique de la communication*, coll. Points essai, Points, 1992 ; P. BRETON, *L'utopie de la communication*, La Découverte, 1992). A propos du discours sur les techniques Jacques Ellul formulait : « *Le discours tenu sur la technique est un discours non pas de justification des techniques (elles n'en n'ont plus besoin), mais de démonstration des prodigieuses puissances, diversité, réussite, de l'application vraiment universelle et de l'impeccabilité des techniques* » (J. ELLUL, *Le bluff technologique*, Hachette, 1988, pp. 12-13). Dans sa thèse en science de l'information et de la communication Madame RENAUD offre une synthèse éclairante des recherches sur le sujet (L. RENAUD, *Dix ans de discours sur le téléphone mobile. Contribution à l'analyse des discours accompagnant l'insertion sociale des objets techniques contemporains*, ss. la dir. de J.-F. TETU, soutenue le 28 nov. 2007, Université Lumière Lyon II, disponible en ligne : (<http://theses.univ-lyon2.fr/documents/lyon2/2007/renaud_l#p=0&a=title>, dernière consultation le 14 oct. 2019). L'on trouvera un éclairage intéressant sur l'origine du mythe sur les dispositifs de l'information comme simple instrument de remémoration, au travers du *Pharmakon* dans le *Phèdre* de Platon dont l'étude par Monsieur JEANNERET apporte un éclairage intéressant (Y. JEANNERET, *Y-a-t-il (vraiment) des technologies de l'information et de la communication*, *op. cit.*). Ces discours ont également vocation à générer la confiance dans les dispositifs techniques afin de servir des desseins politiques : « *Il existe bien, parmi les discours politiques actuellement en circulation dans la société, une entreprise de discours, cohérente et puissamment relayée, pour doter les médias informatisés de vertus extraordinaires et faire avancer, sous couvert de cette révolution annoncée, divers projets de marchandisation de la culture, de libéralisation des échanges et des statuts, de mise en concurrence et en instabilité des salariés, de légitimation providentielle d'un modèle social et économique* » (Y. JEANNERET, « Autre chose qu'un discours, davantage qu'un accompagnement, mieux qu'une résistance , *Revue Terminal*, 2001, n° 85, disponible en ligne <http://www.revue-terminal.org/www/terminal-archives/no_speciaux/85/Jeanneret.html>, dernière consultation le 14 oct. 2019).

travaux préparatoires[809] de la loi du 13 août 2004 créant le dossier médical[810], alors nommé *personnel* et non *partagé.* Ce *discours d'accompagnement* est également diffusé dans la doctrine et l'on en trouve trace jusque dans la formulation des textes d'incrimination[811]. Partant, l'articulation entre le secret des informations relatives au malade et certains dispositifs techniques tels que les dossiers informatisés est d'abord pensée sous l'angle de la préservation de la *confidentialité* des dispositifs de stockage c'est-à-dire par simple transposition du problème qui pouvait déjà se poser pour le support papier. Ainsi présentés, les dispositifs techniques semblent toujours avoir une fonction dominante d'*externalisation de la mémoire*. Toutefois, dès la création du Dossier Médical Personnel l'argument économique donne une dimension bien plus dynamique à ces dispositifs techniques[812]. En dépit du discours relatif à la *mise en mémoire informatisée,* il n'est guère de disposition qui n'envisage celle-ci sans la circulation[813] (qu'il s'agisse de l'accès, de la transmission, de la mise à disposition). Celle-ci est évoquée à côté de la fonction de *stockage*. En témoigne d'ailleurs le passage du vocable *Dossier médical personnel* vers celui de *Dossier médical partagé*. Une brève analyse de la doctrine de la CNIL permet également de se convaincre que le traitement informatisé des données ne consiste jamais en une simple *mise en mémoire* mais appelle toujours la communication des données au travers de l'évaluation, par la commission, des *destinataires*

---

[809] Y. BUR et J.-M. DUBERNARD, *Rapport fait au nom de la commission spéciale chargée d'examiner le projet de loi (n° 1675) relatif à l'assurance maladie*, n° 1703 : *« La continuité des soins sera en partie garantie par le dossier médical personnel, qui sera en quelque sorte la* « mémoire » *du patient et des professionnels de santé* ».

[810] Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, *JORF* n°0190 du 17 août 2004 p. 14598.

[811]« *De telles pratiques* (le fait, pour le soignant, de compter sur sa mémoire) *ne sont plus possibles aujourd'hui, et nul ne peut faire confiance à sa mémoire pour prendre en charge la santé des patients* […] », F. STEFANI, « Le secret médical à l'épreuve des nouvelles technologies », *D.* 2009, p. 2636 ; « l'informatisation des données médicales offrira une mémoire exhaustive du passé sanitaire des individus » (D. TABUTEAU, « Le secret médical et l'évolution du système de santé », *D.* 2009, p. 2629). L'on peut noter qu'est sanctionné, à l'article 226-19 le fait de « *mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé* » des données sensibles.

[812] « *Ce seul rôle de mémoire est trop restrictif et ne suffit pas pour proposer un dossier patient informatisé. Le coût de cette fonction est trop élevé pour le bénéfice qu'elle apporte seule. Le dossier du patient doit être un outil garant de l'amélioration de la qualité des soins. Pour cela, les systèmes cibles devront gérer des connaissances permettant la supervision des données caractérisant la situation du patient, déclencher des alarmes utiles, proposer des aides à la décision, etc. De plus, tenant compte de la sémantique précise des informations et des règles de codification des données mémorisées, ils doivent permettre également l'évaluation de l'action de prise en charge* » M. FIESCHI, « Vers un dossier médical personnel », *Dr. soc.* 2005, p. 80.

[813] V. Par exemple les dispositions relatives à l'hébergement des données qui renvoient au cadre du secret partagé et aux modalités d'accès (art. L. 1111-8, L. 1110-4 et L. 1111-7 CSP).

des données traitées[814]. Aussi la *mémorisation* par le biais des dispositifs techniques induit une circulation des données, laquelle est également traduite en opération de traitement au sein des dispositions relatives à la protection des données personnelles.

2 - Les opérations de traitement visant la communication

160. La communication par transmission. Communiquer une information suppose en principe une personne émettrice et une personne réceptrice[815] : en ce sens la communication peut s'opposer au secret. L'*échange* et le *partage* d'informations, tels que prévus à l'article L. 1110-4 du Code de la santé publique, constituent des formes de communication. L'un et l'autre supposent une interaction entre deux ou plusieurs individus, l'échange étant l'action de « *donner une chose et d'en recevoir une autre en contrepartie* »[816] et le partage celle de « *diviser en parts* »[817] et plus précisément le « *fait d'avoir part à quelque chose avec quelqu'un* ». Il s'agit toujours d'un rapport, un lien. Pour le dépositaire du secret, cela suppose une révélation. La communication par transmission des données étant un *traitement* mais également une *révélation* d'informations couvertes par le secret, les conditions de cette communication vont nécessiter une articulation entre le secret professionnel et les dispositifs de protection des données personnelles.

161. La consultation, action unilatérale. La *consultation* ne suppose pas une relation entre des individus. Définie comme le fait de « *regarder* [quelque chose] *pour y chercher un*

---

[814] La remarque peut sembler anodine, elle est toutefois essentielle car elle confirme que les dispositifs techniques sont bien des dispositifs d'information-communication et non des dispositifs d'information ou de communication. Il faut garder à l'esprit quelques éléments de l'Histoire de la loi informatique et libertés. A. MATTELARD rappelle que le contexte est avant tout international. L'externalisation de la mémoire et la création des bases de données est une question de contrôle des flux de données, plus qu'externalisée la mémoire il s'agit de contrôler sa circulation et plus encore de la maîtriser pour des raisons de souveraineté « *Le processus d'extériorisation de la mémoire collective, accéléré par la numérisation, doit faire face au risque de monopolisation des banques de données étrangères : « Le savoir finira par se modeler sur les stocks d'information »*. Construire ses propres banques de données est un « *impératif de souveraineté* » (M. MATTELARD, « V. Les politiques publiques à l'épreuve du libre-échange », *in Histoire de la société de l'information*, La Découverte, 5ème éd., pp. 62-81. L'auteur fait référence à S. NORA et A. MINC, *L'informatisation de la société, Rapport au Président de la République*, janv. 1978, p. 13).

[815] C'est sur la base de la relation duale émetteur-récepteur que se sont construites les théories de la communication et ensuite les sciences de la communication dont les théoriciens les plus emblématiques sont N. WIENER (*Cybernetics or control and communication in the animal and the machine*, 1948) et C. SHANNON (*A Mathematical Theory of Communication*, Bell System Technical Journal, vol. 27, July and October, 1948 ; *Adde* A. MATTELART et M. MATTELART, *Histoire des théories de la communication*, 3ème éd., La Découverte, 2010).

[816] V° « Echanger », TLFi, *op. cit.*

[817] V° « Partager », TLFi, *op. cit.*

renseignement, une information, une explication »[818], cette action est unilatérale, elle ne suppose l'action que d'une personne par rapport au média qui supporte l'information. Celui qui consulte un fichier, un dossier informatisé ou une base de données, peut le faire sans que cela suppose une relation de communication. Dans la doctrine de la CNIL, la consultation correspond au fait d'accéder aux données, cette notion « d'accès » se trouvant également dans le Code de la santé publique[819]. Aussi, l'accès est-il ou non autorisé[820]. Il suppose une action d'ordre technique, plus qu'une action de communication. Les dispositions tant législatives que règlementaires permettent de saisir en quoi consiste cette opération. L'accès intéresse en premier lieu les personnes concernées par les données et certains membres de leur famille[821]. Toutefois, s'agissant de cette catégorie de personnes, la consultation n'est pas une opération de traitement au sens des dispositions relatives à la protection des données mais un droit qu'ils exercent, s'agissant des données et informations détenues par des établissement publics, à l'égard de l'administration et à l'égard des professionnels libéraux lorsque ce sont des responsables du traitement. La question de la préservation du secret des informations ne se pose pas, puisque le patient n'est pas extérieur à la relation qui fonde l'existence du secret. Le rapport entre secret des données et accès à celles-ci révèle une autre dimension lorsque l'accès est opéré par des personnes qui sont extérieures à cette relation. Le Code de la santé publique prévoit ainsi des conditions particulières d'accès aux données de santé collectées dans le cadre des soins. Pour les outils les plus connus et généralisés – le dossier pharmaceutique, le dossier médical partagé, les systèmes d'information en santé (SIS), la plateforme des données de santé (intégrant notamment le Système national de données de santé) – l'articulation entre les dispositions relatives à la protection des données personnelles, celles figurant dans le Code de

---

[818] V° « Consulter », TLFi, *op. cit.*

[819] Pour illustration l'article L. 1435-6 du Code de la santé publique portant sur l'accès aux données de santé et les articles R. 1461-11 à R. 1461-19 portant sur l'accès permanent de certains services publics au système national des données de santé.

[820] L'accès non autorisé à un traitement de données est sanctionné pénalement à l'article 226-16 du Code pénal qui puni « *le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende* ». De même que le fait de donner accès à un tiers non autorisé est pénalement sanctionné.

[821] CSP art. L. 1111-7 CSP s'agissant des dispositions générales relatives au droit d'accès ; CSP art. R. 1111-1 à R. 1111-8 CSP.

la santé publique et le secret professionnel, laisse à voir que *la consultation* s'appréhende différemment selon les finalités de l'accès, les personnes qui accèdent et la nature des données.

162. La mise à disposition ou diffusion, l'open data. La *mise à disposition* consiste dans l'action de mettre quelque chose « *à l'usage, au service* »[822] de quelqu'un, tandis que la diffusion consiste dans l'action de diffuser, c'est-à-dire « *Propager dans un large public par les moyens d'information* »[823]. Cette action suppose la volonté de donner connaissance des données, mais la mise à disposition implique également une liberté de celui qui en dispose et donc la possibilité de réutiliser les données. Le responsable du traitement peut procéder à la mise à disposition à des personnes déterminées[824] ou à un public plus large. Cette dernière modalité de diffusion est appelée *open data*. Plus qu'une simple possibilité de prendre connaissance des données, il s'agit de permettre leur *réutilisation*. Le mouvement d'accessibilité des informations puis des données est né dans les années soixante-dix en réponse à une exigence de transparence de l'administration que nous avons déjà évoquée[825]. L'*open data* constitue la poursuite du processus né du droit d'accès, droit subjectif pour les administrés dont l'administration est le débiteur[826]. Il consiste dans l'ouverture et la possibilité de réutiliser des données dites *publiques*[827]. Les données publiques ne sont pas publiques au sens d'une opposition avec les informations personnelles relevant de la vie privée : il s'agit de données produites ou reçues par l'administration au sens de l'article L. 300-2 du Code des relations entre le public et l'administration[828]. Les ensembles de données publiques constituent des documents

---

[822] V° « Disposition (mettre à) », TLFi, *op. cit.*
[823] V° « Diffuser », TLFi, *op. cit.*
[824] C'est par exemple le cas de la mise à disposition des données regroupées au sein de la Plateforme des données de santé.
[825] V. *infra* n° 49.
[826] Dès le XVIII[ème] siècle certaines exceptions au *secret de l'administration* voient le jour (décret du 7 septembre 1790 et loi du 7 messidor 1794). La question de la transparence de l'administration va devenir un sujet central, jusqu'à être qualifiée de « troisième génération des droits de l'homme » (G. BRAIBANT.), la loi informatique et libertés mais également la Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal ; v. art. L. 300-1 et s. CRPA.
[827] Sous l'influence de l'Union européenne, la France a progressivement procédé à une *ouverture* de plus en plus importante des informations et données publiques : Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public.
[828] Pour rappel CRPA, art. L. 300-2 al. 1 : « *Sont considérés comme documents administratifs, au sens des titres Ier, III et IV du présent livre, quels que soient leur date, leur lieu de conservation, leur forme et leur support, les documents produits ou reçus, dans le cadre de leur mission de service public, par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission. Constituent de tels documents notamment les dossiers, rapports, études, comptes rendus, procès-verbaux,*

administratifs au sens de ce texte[829]. Le domaine de la santé n'a pas échappé au processus d'ouverture de l'accès des données : les dispositions relatives à l'*open data* dans le domaine de la santé résultent – mais uniquement dans l'affirmation du *principe*[830] – de la loi pour une République numérique[831], des dispositions nationales et européennes relatives à la protection des données à caractère personnel, et de diverses dispositions du Code de la santé publique principalement issues de la loi de modernisation de notre système de santé[832] et de la loi relative à l'organisation et à la transformation du système de santé[833]. L'ouverture des données serait la reconnaissance d'un droit aux informations publiques[834] faisant suite au droit d'accès individuel

statistiques, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions, codes sources et décisions. »

[829] En ce sens v. Trib. UE, 26 oct. 2011, *Julien Dufour c. CBE*, aff. T-436/2001 ; Pour analyse circonstanciée de l'arrêt v. A. GARIN, *Le droit d'accès aux documents : en quête d'un nouveau droit fondamental dans l'Union européenne*, Ed. A. PEDONE, 2017, pp. 163-168.

[830] Au sens le plus commun du terme c'est-à-dire « ce qui est premier, à l'origine ». L'ouverture de l'accès aux données figure en effet à la première section du premier chapitre du premier titre de la loi qui porte sur « la circulation des données et du savoir ».

[831] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, *JORF* n°0235 du 8 octobre 2016.

[832] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, dont sont issues les dispositions relatives à la mise à disposition des données de santé prévues aux article L. 1461-1 et svt. du CSP.

[833] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, *JORF* n°0172 du 26 juillet 2019.

[834] En ce sens quelques rapports, généraux ou sectoriels sur l'ouverture des données publiques et les enjeux économique et démocratique de la transparence : C. BOUCHOUX, *Refonder le droit à l'information publique à l'heure du numérique : un enjeu citoyen, une opportunité stratégique*, Rapport d'information n° 589, fait au nom de la mission commune d'information du Sénat sur l'accès aux documents administratifs, 5 juin 2014, t. 1, p. 25 ; G. GORCE et F. PILLET, *La protection des données personnelles dans l'open data : une exigence et une opportunité*, rapport d'information n° 469, fait au nom de la commission des lois, 16 avr. 2014 ; sur l'open data des décisions de justice v. L. CADIET, *L'open data des décisions de* justice, Rapport à Madame la garde des Sceaux, nov. 2017 ; dans le domaine de la santé P.-L. BRAS, A. LOTH, *Rapport sur la gouvernance et l'utilisation des données de santé*, La documentation Française, 2013, p. 27. Sur le processus d'ouverture et son histoire (du droit d'accès aux documents administratifs par les personnes concernées à l'ouverture généralisée des données publiques), pour une approche générale v. H. VERDIER, S. VERGNOLLE « L'Etat et la politique d'ouverture en France », *AJDA* 2016, p. 92 ; P. YOLKA, « Open data : « L'ouverture, c'est l'aventure » », *AJDA* 2016, p. 79 ; et pour les monographie v. par exemple : H. MAISL, *Le droit des données publiques*, LGDJ, 1996 ; J.-M. BRUGUIERE, *Les données publiques et le droit*, Litec, 2002. Pour une approche sectorielle sur l'*open data* : s'agissant de l'ouverture des données des collectivités territoriales v. par exemple S. MANSON, « La mise à disposition de leurs données publiques par les collectivités territoriales », *AJDA* 2016, p. 97 ; A. CHERON, « La réutilisation des données publiques : bases de données et open data », *AJCT* 2011, p. 391 ; pour l'*open data* dans le secteur de l'énergie v. notamment O. BEATRIX, « Open data et secteur de l'énergie : le début de l'histoire », *RFDA* 2018, p.49 ; concernant l'*open data* des données scientifiques (hors le cas des données issues de la recherche biomédicale) v. A. ROBIN, « Les données scientifiques au prisme du dispositif open data », *Comm. com. électr.*, 2017, n° 9, étude 14 ; L. WATRIN, *Les données scientifiques saisies par le droit*, th. dact., ss. la dir. de M.- E. PANCRAZI, soutenue le 9 déc. 2016, Université Aix-Marseille, n° 341 et svt.

« *nouveau droit fondamental* »[835]. La mise à disposition des données publiques, obligation des Etats créanciers d'un droit à l'information publique, se trouve en conflit avec d'autres intérêts, individuels. Le conflit entre le droit à l'information et les secrets se manifeste encore à ce niveau d'ouverture et constitue autant de limites à l'*open data*[836]. S'agissant précisément de l'*open data* dans le domaine de la santé il faut le distinguer de l'*accès* (consultation) et de la communication. en ce que, dans le premier cas la protection du fait secret est entièrement technique tandis que dans le second l'*accès* et la communication par et à certaines catégories de personnes sont notamment conditionnés à la soumission au secret professionnel de celui qui accède où à qui les données sont communiquées.

163. L'utilisation des données, opération tierce. Il est encore utile de revenir à la définition commune du terme *utilisation* : il s'agit de l'action d'utiliser. Or le verbe *utiliser* se définit comme « *Tirer parti de (quelque chose), faire servir (quelque chose) à une fin déterminée* »[837]. Le traitement des données répondant nécessairement à une fin déterminée, affirmer que l'utilisation des données est un traitement de données semble relever de la tautologie. Cette mention n'est toutefois pas inutile car elle vise certains cas particuliers. En effet, les données peuvent être utilisées pour des finalités autres que celles pour lesquelles elles sont initialement traitées[838]. La précision permet également de faire entrer dans le champ des dispositions relatives à la protection des données les hypothèses de *réutilisation* des données, dans la mesure où les données peuvent être utilisées par une personne qui ne les a pas elle-même collectées et organisées. La *réutilisation* des données de santé trouve un écho particulier en certaines

---

[835] A. GARIN, *Le droit d'accès aux documents : en quête d'un nouveau droit fondamental dans l'Union européenne*, A. PEDONE, 2017.

[836] Si l'on pense au secret de la vie privée (D. BOURCIER, P. DE FILIPPI (ss. la dir.), *Open Data et Big Data ; Nouveaux défis pour la vie privée*, Mare et Martin, 2016 ; N. MALLET-POUJOL, « Protection des données personnelles et droit à l'information », *Legicom*, n° 59, 2017/2, p. 124 ; N. MALLET-POUJOL, «La protection des données personnelles à l'épreuve de l'open data des décisions de justice : l'exemple des données des justiciables », *Revue pratique de la prospective et de l'innovation*, 2018, n°1, dossier 4; N. FRICERO, « Collecte, diffusion et exploitation des décisions de justice : quelles limites, quels contrôles ? À propos du rapport sur l'open data des décisions de justice », *JCP G*, 2018, n° 7, p. 168 ; L. CADIET, « Les conditions de diffusion des décisions de justice représentent un enjeu essentiel de la mise en œuvre du projet de leur mise à disposition du public », *JCP G*, n° 7, 2018, p. 170) les autres faits dont le droit garantit le secret sont également en cause. C'est le cas du secret industriel et commercial (O. BEATRIX, « Open data et secteur de l'énergie : le début de l'histoire », *op. cit.*) ; du secret défense également (L. CLUZEL-METAYER, « Les limites de l'open data », *AJDA* 2016, p.102 ; L. CLUZEL-METAYER, « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », *AJDA* 2017, p. 340).

[837] V° « Utiliser », TLFi, *op. cit.*

[838] C'est le cas en matière d'*open data*.

matières, ces dernières se confondant avec des finalités[839] : réutilisation par la sécurité sociale à des fins de contrôle des dépenses de santé et de remboursement des actes de soins, réutilisation pour des finalités de recherche dans le domaine de la santé. A ces réutilisations pour des motifs d'intérêt général s'opposent les réutilisations à des fins commerciales, interdites lorsque les données ont été collectées par des professionnels intervenant dans la prise en charge du malade. En somme, toute *réutilisation* suppose un accès ou une mise à disposition[840], donc un mouvement des données en question.

3 - Intérêt de la distinction entre les opérations de traitement

164. Les limites de la distinction entre les opérations de traitement de l'information et les opérations de traitement relevant de la communication. Distinguer les opérations relevant de la mémorisation et de la documentarisation et celles relevant de la circulation réduit l'immense portée de la question du lien entre l'oral et l'écrit d'une part[841] et l'écrit et ses supports[842] d'autre part. L'information n'est représentée que pour être communiquée, plus

---

[839] Les finalités du traitement, telles qu'entendues par l'article 9 II h) du RGPD.

[840] Le propre des données ouvertes, participant à l'émergence du gouvernement ouvert (*open government*) réside d'ailleurs dans la liberté de réutiliser les données (L. WATRIN explique notamment le passage progressif des données quérables, aux données portables puis aux les données réutilisables dans le cadre de l'open data des données scientifiques : L. WATRIN, *Les données scientifiques saisies par le droit*, *op. cit.*n° 341 et svt.). Pour une étude sur la réutilisation des données publiques ouvertes v. D. BOURCIER et P. DE FILIPPI, « L'Open Data : universalité du principe et diversité des expériences ? », *JCP A*, 2013, n° 38, 2260, n° 12 et svt. et spéc. sur l'*open government* en France n° 41 et svt.

[841] Y. JEANNERET développe la question de l'écriture et de la parole dans leur rapport avec le *sens* et la connaissance, avec la mémoire et le savoir, afin distinguer l'écriture des dispositifs techniques que nous nommons technologies de l'information (*Y-a-t-il (vraiment) des technologies de l'information et de la communication*, *op.cit.*, chapitre 1 « Quatre lectures d'un texte fondateur »). C'est dans les commentaires du *Phèdre* de Platon qu'il puise l'essentiel de sa réflexion au terme de laquelle il affirme : « *Les* « nouvelles technologies » *sont* […] *essentiellement des technologies de production de signes visuels (des écrits d'écran), dans lesquelles l'appropriation des savoirs, leur construction et leur partage passent par le regard du lecteur : ceci, à la fois parce que toute disposition écrite se justifie par une anticipation de lecture, et parce que tout document ne devient un savoir que sous le regard d'un lecteur qui l'interprète. Ce sont donc des technologies de l'espace avant d'être des technologies du temps : ce ne sont des objets de mémoire que parce que ce sont des lieux de mémoire* » (*Ibid*. n° 69).

[842] Que nous avons envisagé sous un seul angle mais qui fait l'objet d'études tant en science du langage (par exemple en sémiotique A. ZINNA « L'interface : un espace de médiation entre support et écriture », disponible sur le site de l'association française de sémiotique ; en linguistique J. ANIS, *Texte et Ordinateur. L'écriture réinventée ?* coll. « Méthodes en sciences humaines », De Boeck Université,1998), qu'en sciences de l'information et de la communication (R. T. PEDAUQUE, *Le Document à la lumière du numérique : forme, texte, médium : comprendre le rôle du document numérique dans l'émergence d'une nouvelle modernité*, C&F éditions, 2006 ; Y. JEANNERET, *Y-a-t-il (vraiment) des technologies de l'information et de la communication, op. cit.*).

exactement, la représentation de l'information est une « *implication de communication* »[843] mais cela est également vrai pour toutes représentations graphiques[844]. Ce qui change, d'un point de vue technique, c'est que les données sont désormais recueillies, stockées, traitées, consultées, partagées, échangées en permanence, ces opérations pouvant être simultanées, si bien que la simplicité de la distinction entre les opérations de traitement des données n'est qu'apparente. Si elle permet d'affirmer que toute opération sur les données, effectuée à l'aide d'un dispositif technique d'information-communication, est un traitement de données, l'intérêt de la distinction se révèle limité dès lors qu'il s'agit d'étudier les lignes de tension entre secret des informations relatives au malade et traitement des données. La difficulté à distinguer, dans les faits, entre les opérations de traitement est un facteur de la perte de maîtrise des personnes sur les données qui les concernent[845]. Mais plus qu'un phénomène strictement technique, ce sont les différentes finalités assignées aux dispositifs techniques qui impliquent cette difficulté[846].

165. Une distinction peu opérante en l'état des dispositions européennes et nationales. La distinction entre les opérations de traitement interroge encore en ce que, si l'on ne peut nier ses vertus explicatives dans la mesure où elle permet de se représenter le champ d'application de la loi, elle n'a pas grand intérêt : les dispositions s'appliqueront de manière identique peu importe l'opération de traitement effectuée sur les données. Pourtant, donner une portée réelle à la distinction entre les opérations aurait sans doute pour vertu de resserrer le champ de la protection sans le diminuer. L'articulation avec le secret professionnel en serait plus aisée dans la mesure où cela permettrait d'affiner le niveau de protection en fonction des opérations et de réduire les difficultés à distinguer l'implication de chaque opération par rapport au risque qu'elle engendre. En effet, une opération de recueil de données ne pose pas les même questions

---

[843] « *Il n'y a pas de représentation de l'information en soi, mais seulement pour l'autre, car l'information est une relation qui s'établit entre un objet et un regard ; la constitution d'un document ou d'un ensemble documentaire n'est jamais une pure représentation du monde. Ce n'est pas une ontologie, c'est une proposition, ou plus exactement une implication de communication et de lecture, qui adopte un point de vue, procède de réécritures et d'adaptations, convoque une image des compétences, attentes et interprétations possibles de son utilisateur* » (Ibid. chapitre 2, n°71).

[844] Sur la révolution graphique du passage de l'écriture au numérique et les autres phénomènes qui sous-tendent ce changement v. A. GARAPON et J. LASSEGUE, *Justice digital*, PUF, 2018, p. 19 et svt.

[845] Perte de maîtrise déjà évoquée par J. EYNARD qui l'impute aux seules faiblesses des connaissances techniques des personnes concernées par les données (J. EYNARD, *Les données personnelles*, *op. cit.,* Pp. 143-154).

[846] Nous ne visons pas ici les finalités des traitements de données personnelles telles qu'elles sont conçues au travers des dispositions relatives à la protection des données personnelles mais les finalités que la société a assignées aux dispositifs techniques.

qu'une communication au regard du secret professionnel. Aussi, un régime différent pourrait-il s'appliquer en fonction de l'opération de traitement. La lisibilité du texte en serait également accrue tant pour les acteurs que pour les personnes concernées. C'est le choix opéré par la législation canadienne dans laquelle « […] *des régimes distincts sont proposés selon la « dangerosité » des opérations, que ce soit une communication, une diffusion, une collecte, une détention, une utilisation* […] *celles-ci ne s'équivalent pas et les risques afférents non plus* »[847]. Mais ce n'est pas là que se porte notre attention.

Concernant la notion qui nous occupe, l'on discerne au travers des opérations de traitement la manière dont se déploie la problématique du « secret médical », ce que l'on constatera par ailleurs au travers de l'étude de la doctrine de la CNIL. Le *stockage* implique une protection du secret des données contre les atteintes des tiers, à l'instar des supports papier. De l'*accès* résulte l'idée de donner autorisation à prendre connaissance des données ce qui implique un contrôle des accès au regard de règles qui dictent *comment* l'information circule. Enfin la transmission des données renvoie directement au secret professionnel.

Section 2 - Le secret des données relatives au malade et le régime des dispositions relatives à la protection des données à caractère personnel

166. Changement de perspective. Dès lors qu'il s'agit d'envisager le traitement des données personnelles et des données de santé, les dispositions sont généralement analysées au regard des conditions de licéités de traitement de ces données. C'est en raison de finalités spécifiques que les traitements de données sont autorisés, ces finalités permettant ensuite de différencier les régimes applicables à chaque situation. Aussi, s'agissant des données sensibles le responsable du traitement devra-t-il évaluer sa situation dans le cadre des exceptions afin de remplir les conditions permettant de traiter les données. Notre perspective n'est pas celle-ci, il s'agira plutôt de chercher les mécanismes de protection spécifiques aux données issues d'une prise en charge sanitaire. La source des données est essentielle puisque c'est en raison du contexte – le prise en charge dans le système de santé – que l'information est secrète. Ainsi, deux axes déterminants se dessinent. D'abord, la particularité tenant à la source des données se

[847] V. GAUTRAIS, « Différences culturelles en matière de vie privée : point de vue canadien », *Dalloz IP/IT* 2016, p. 128.

traduit au regard des conditions de licéité générale que sont le consentement et les finalités de traitement **(paragraphe 1)**. Ensuite et surtout, certains traitements, au regard de leur finalité, ne peuvent être mis en œuvre que par des personnes soumises au secret **(paragraphe 2)**.

§ 1 - La protection du secret des données dans le domaine de la santé et le consentement au traitement

167. Le consentement au traitement tient une place centrale dans les dispositions relatives au traitement des données à caractère personnel, l'autodétermination informationnelle étant au centre du dispositif. L'on constate toutefois qu'un régime spécifique s'applique s'agissant du traitement des données sensibles pour des finalités spécifiques **(A)**. Bien que cette question ne soit pas en lien avec la protection du secret des données, il est nécessaire de l'évoquer afin de préciser le contexte de nos propos. En aval, la protection du secret des données se traduit par une limitation de la portée du consentement des personnes au traitement de leurs données issues de leur prise en charge par un professionnel intervenant dans le système de santé : le patient est protégé contre lui-même **(B)**.

A - Précisions d'ordre générale sur le consentement au traitement

168. Bien que le consentement occupe une place essentielle dans la protection des données à caractère personnel **(1)** des dérogations sont prévues pour certaines finalités et sous certaines conditions **(2)**.

1 - Le consentement au traitement, principe matriciel

169. La place centrale du consentement, condition première du traitement des données à caractère personnel. A côté des principes généraux constituant la colonne vertébrale des dispositions relatives à la protection des données[848], la licéité d'un traitement de données est conditionnée au respect des conditions inscrites à l'article 5 de la LIL[849]. Le consentement est la condition première de la licéité du traitement des données à caractère personnel mais également des données *sensibles*[850]. Plus encore, le principe de l'autodétermination

[848] Il s'agit des « principes » inscrit à l'article 5 du RGPD. Dans la loi informatique et libertés ces dispositions figurent à l'article 4.
[849] Art. 6 RGPD.
[850] Aucune forme particulière n'est exigée pour le consentement de la personne au traitement de ses données à caractère personnel tandis que celui-ci doit être explicite lorsque les données traitées sont des données sensibles (RGPD art. 9; LIL art. 6 opérant un renvoi vers l'article du RGPD).

informationnelle, compromis entre le droit au respect de la vie privée et le droit de propriété consiste à affirmer que l'individu dispose d'une véritable maîtrise sur ses données. L'on constate toutefois une différence de régime entre le traitement des données de santé et le traitement des données à caractère personnel pour des finalités spécifiques correspondant à la prise en charge des personnes par le système de santé. Cette atténuation de la portée du consentement est prévue à l'article 9 paragraphe 2 h) du RGPD.

170. Exceptions à l'interdiction de traitement dans la LIL et le RGPD. Le champ d'application des dispositions spécifiques au traitement des données de santé est prévu à l'article 9 du RGPD et par renvoi à celui-ci à l'article 6 de la LIL. Au titre des exceptions au traitement des données sensibles et *a fortiori* des données de santé, le règlement prévoit les cas dans lesquels le traitement est possible en raison des finalités et/ou du respect de conditions particulières[851]. Avant d'envisager ces exceptions il faut replacer notre étude dans le contexte du traitement des données sensibles.

171. Traitement des données de santé en dehors d'une prise en charge sanitaire – distinction. Les données de santé n'ont pas toutes pour source la prise en charge sanitaire. Si les professionnels intervenants dans le système de santé et particulièrement les professionnels de santé sont des *accoucheurs*[852] d'informations et de données de santé, un individu peut fournir des informations et des données relatives à sa santé dans des cadres bien différents de sa prise charge par le système de santé[853]. Un individu peut par exemple les fournir à une entreprise quelconque en échange d'un service[854]. Aussi, le traitement ne sera licite que lorsque la

---

[851] RGPD art. 9 paragraphe 2 b) à j).

[852] Le terme est emprunté à I. DE LAMBERTERIE et H.- J. LUCAS (I. DE LAMBERTERIE et H.- J. LUCAS, *Informatique, libertés et recherche médicale*, coll. CNRS Droit, CNRS, 2001, p. 12).

[853] Le phénomène du *Quantified self* en est un exemple : La personne accepte que ses données physiologiques soient analysées par une application en l'échange d'un service. On connait nombre de ces applications sous des formes diverses : les montres connectées, smartphones assortis d'applications surveillant les paramètres physiologiques (nombre de pas, d'escaliers gravis, de pulsations cardiaques etc.), dans certaines de ces applications il est même possible d'avoir recours à des applications plus pointues (taux de glycémie, saturation en oxygène, utilisation d'un inhalateur etc.).

[854] Prenant l'exemple des objets connectés, un auteur remarque que ces applications n'ont que l'apparence de la gratuité : « […] *au sein des contrats de l'Internet, le professionnel ne se rémunère pas grâce au prix payé par le client, mais grâce aux données fournies par celui-ci, phénomène qui est désormais régulièrement présenté de la manière suivante : « Lorsqu'un service ou un bien est proposé gracieusement à un individu, c'est l'individu - ou plus exactement ses données - qui constituent la valeur marchande* » et d'ajouter s'agissant spécifiquement du phénomène du *Quatified self* que les applications brouillent « […] *la frontière entre le soin médical et le service*

personne aura donné son consentement au traitement pour des finalités déterminées, ou lorsque le consentement n'aura pas à être recherché, en raison d'une finalité particulière.

La collecte de données de santé par une entreprise privée, en dehors d'une prise en charge sanitaire, ne sera pas interdite dès lors qu'elle respecte les conditions prévues au paragraphe 2 a) de l'article 9 du RGPD. Cette disposition prévoit que l'interdiction de traitement des données sensibles ne s'applique pas lorsque « *la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée* »[855]. Ainsi, il est possible de traiter des données de santé à la condition d'obtenir le consentement explicite[856] de la personne concernée par celles-ci. Ce consentement est donné

---

marchand » (J. SENECHAL, *La fourniture de données personnelles par le client via Internet, un objet contractuel ?* », *AJCA* 2015, p. 212). Et plus généralement v. J. ROCHFELD « Le « contrat de fourniture de contenus numériques » : la reconnaissance de l'économie spécifique « contenus contre données » », *Dalloz IP/IT* 2017, p. 15. A propos du phénomène de *quantified self* et des objets connectés, le développement d'applications par des acteurs privés, qui ne participent pas à la relation renouvelle les problèmes de protection des données, particulièrement lorsque les données sont récoltées par des sociétés implantées à l'étranger v. sur ce point M. LANNA, « L'homme surveillé : les objets connectés », *in* C. CASTAING (ss. la dir.) *Technologies médicales innovantes et protection des droits fondamentaux des patients*, coll. droit public, Mare et Martin, pp. 84-87.

[855] RGPD art. 9 § 2 a).

[856] La notion de consentement explicite n'est pas nouvelle, elle n'est pas née avec le RGPD puisque l'exception dont il est question existait déjà dans la loi informatique et libertés avant même la directive de 1995. Aussi, les conditions du caractère explicite ont déjà fait l'objet de réflexion dans la doctrine de la CNIL, la doctrine juridique et le G29. La CNIL a par exemple considéré que l'accord doit être explicite, écrit et figurer dans un document distinct du formulaire de la collecte (CNIL, 7e rapport d'activité, 1986, p. 77 ; - *Adde* M. BENEJAT, « Les droits sur les données personnelles », *in Traité de droit de la personnalité*, J.-C. SAINT-PAU (ss. la dir.), LexisNexis, 2013, n° 958 ; CNIL, 8ème rapport d'activité, 1987, p. 17 et p. 28). Par ailleurs le G29 précisait : « *En droit, l'expression* « consentement explicite » *a le même sens que* « consentement exprès ». *Le consentement explicite couvre toutes les situations où il est proposé à une personne d'accepter ou de rejeter une utilisation particulière ou la divulgation des informations la concernant et qu'elle répond activement à la question, que ce soit oralement ou par écrit. En règle générale, un consentement explicite ou exprès est donné par écrit et est attesté par une signature manuscrite. Ainsi, un consentement explicite est donné lorsque la personne concernée signe un formulaire de consentement qui explique clairement pourquoi un responsable du traitement souhaite collecter et traiter ultérieurement des données à caractère personnel. Bien qu'un consentement explicite soit traditionnellement donné par écrit, sur papier ou sous forme électronique, […] cela ne doit pas nécessairement être le cas : il peut également être donné oralement, ce que confirme la suppression, dans la version finale de la directive, de l'exigence que le consentement* visé *à l'article 8 soit écrit. Toutefois, comme l'a montré cette même section, un consentement oral peut être difficile à prouver et, dans la pratique, il est donc recommandé aux responsables du traitement de recourir à un consentement écrit pour des raisons de preuve. L'exigence d'un consentement explicite signifie qu'un consentement qui est déduit ne satisfera normalement pas à la condition imposée par l'article 8, paragraphe 2* » (G29, avis n° 15/2011, 13 juill. 2011, WP 187, p.28-29). Finalement le RGPD précise la définition du consentement dans son article 7 lequel dispose notamment : « *1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant. 2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également*

au regard des finalités du traitement. Ces données sont issues d'informations qui peuvent relever d'une prise en charge médicale ou médico-sociale, mais dès lors qu'elles sont fournies par la personne concernée à un responsable de traitement[857] il ne peut s'agir d'une violation du secret professionnel ou d'une obtention irrégulière des informations couvertes par le secret[858].

Par ailleurs, le régime de protection s'accompagne d'un certain nombre de *principes*[859] qui représentent autant d'obligations pour le responsable du traitement et qui s'appliquent à tous les traitements de données personnelles, que celles-ci soient, ou non, des données sensibles.

2 - Les finalités spécifiques et la soumission au secret professionnel

172. Le traitement des données sensibles pour des finalités tenant à la prise en charge des personnes et à la gestion du système de santé et de sécurité sociale. L'article 9 paragraphe 2 h) du RGPD prévoit que les données sensibles peuvent faire l'objet d'un traitement sans qu'il soit nécessaire d'obtenir le consentement explicite de la personne lorsque « *le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise*

---

d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante ». La différence entre consentement et consentement explicite parait bien mince, dès lors que la preuve incombe au responsable du traitement il est préférable de formaliser ce consentement. La CNIL précise toutefois qu'il sera nécessaire, pour le consentement explicite de «*prévoir une case de recueil du consentement spécifiquement dédiée au traitement des données sensibles, demander une déclaration écrite et signée par la personne concernée ou l'envoi d'un courriel indiquant que la personne accepte expressément le traitement de certaines catégories de données, recueillir le consentement en deux étapes : envoi d'un courriel à la personne concernée qui doit ensuite confirmer sa première action de consentement* » (CNIL, *Conformité RGPD : comment recueillir le consentement des personnes ?*, 3 aout 2018, disponible en ligne sur : <https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes> (dernière consultation le 14 oct. 2019). La CNIL dans un souci de décryptage des dispositions du RGPD procède par le biais de publications qui n'ont qu'une valeur explicative mais, à laquelle il convient de se référer en ce qui concerne l'interprétation du RGPD).

[857] Art. 4 RGPD : « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre* ».

[858] Art. L. 1110-4-IV du Code de la santé publique.

[859] Ces principes sont prévus à l'article 5 du RGPD qui exige que les données à caractère personnel doivent être traitées de manière licite, loyale et transparente (a), leur traitement doit avoir des finalités limitées (b), les données doivent être adéquates, pertinentes et limités au regard de ces finalités (c). Les données doivent également être exactes (d).

en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3 »[860]. Il s'agit donc de restreindre la portée du consentement lorsque le traitement s'avère nécessaire tant pour la personne que pour des motifs d'intérêt public tenant à la gestion du système de santé et de protection sociale. En dehors de cette finalité spécifique, il faut encore mentionner la finalité décrite à l'article 9 paragraphe 2 i), lorsque « *le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel* ». La finalité d'intérêt public justifie que le consentement de la personne ne soit pas exigé. Les personnes concernées ont, en principe, toujours la possibilité de s'opposer au traitement, ce dont elles doivent être informées au moment de la collecte de leurs données[861]. Outre ces hypothèses qui rendent licite le traitement des données sensibles indépendamment du consentement des personnes concernées, d'autres dispositions visent, en aval du traitement initial, à limiter la portée du consentement des personnes afin de préserver le secret des données issues d'une prise en charge par un professionnel intervenant dans le système de santé.

173. La portée limitée du consentement, une protection spécifique des données couvertes par le secret professionnel. Dans un souci de protection des individus, le législateur a toutefois prévu de limiter la portée du consentement de la personne. On constate ainsi qu'il existe une protection accrue de ces informations en raison du contexte de leur production. En

---

[860] Le paragraphe mentionné *in fine* renvoie à la désignation des personnes soumises au secret professionnel.

[861] RGPD art. 21, dont l'interprétation est guidée par le considérant 69 du Règlement : « *Lorsque des données à caractère personnel pourraient être traitées de manière licite parce que le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, ou en raison des intérêts légitimes du responsable du traitement ou d'un tiers, les personnes concernées devraient néanmoins avoir le droit de s'opposer au traitement de toute donnée à caractère personnel en rapport avec leur situation particulière. Il devrait incomber au responsable du traitement de prouver que ses intérêts légitimes impérieux prévalent sur les intérêts ou les libertés et droits fondamentaux de la personne concernée* ». Le droit de recevoir des informations claires et transparentes concernant le traitement, inscrit à l'article 13 du Règlement est le corollaire du droit d'opposition.

effet, l'exception prévue au paragraphe 2 a) de l'article 9 du RGPD[862] est limitée dès lors que le droit de l'Union ou le droit d'un Etat membre « *prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée* »[863]. Le droit national prévoit effectivement certaines de ces hypothèses qu'il faut, s'agissant des données issues de la prise en charge sanitaire, rechercher dans le Code de la santé publique.

174. Le cas particulier des données génétiques. L'examen des caractéristiques génétiques, un accès aux informations génétiques. Bien que l'examen des caractéristiques génétiques[864] soit en principe interdit[865], la loi prévoit une exception lorsque cet examen est pratiqué pour des raisons médicales et de recherche[866]**.** L'examen des caractéristiques génétiques peut avoir des conséquences importantes sur la vie de la personne qui s'y prête car l'information à laquelle le patient accède grâce à cet examen consiste à la fois dans la « *révélation d'un risque* »[867] et d'une part de son identité[868]. Dès lors qu'elle révèle des informations sur l'état de santé d'une personne les données génétiques sont protégées en tant que données de santé[869].

175. Données génétiques, l'exigence du consentement exprès pour le traitement à des fins de recherche dans le domaine de la santé. Les données génétiques constituent une catégorie particulière de données car elles ne peuvent être systématiquement considérées comme des données de santé. En effet, elles sont également susceptibles de révéler les origines ethniques de l'individu concerné et peuvent également servir à l'identification des individus. Dans ces hypothèses les données génétiques sont protégées en tant que données relatives à l'origine ethnique et en tant que données biométriques[870]. Le considérant 35 du RGPD précise l'étendue de la notion de données de santé comme étant : « *des informations obtenues lors du*

---

[862] Egalement § 2) a) de l'article 8 de la LIL
[863] RGPD §2 a) art. 9 ; *Ibid.*
[864] Pour une étude des tests génétiques v. E. SUPIOT, *Les tests génétiques. Contribution à une étude juridique*, coll. Centre de droit de la Santé, PUAM, 2014 ; également J.-R. BINET, *Jcl. Civil Code, Synthèse n°20 « Bioéthique »*.
[865] C. civ. art. 16-10.
[866] *Ibid.*
[867] E. SUPIOT, *Les tests génétiques. Contribution à une étude juridique*, *op. cit.*, n° 34.
[868] *Ibid.* n° 36.
[869] CNIL, *Les données génétiques*, coll. Point Cnil, La documentation française, Version numérique EPUB.
[870] CNIL, *Les données génétiques*, *op. cit.*

test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro ». Un régime particulier s'applique aux données génétiques traitées dans le cadre d'une recherche dans le domaine de la santé puisque le consentement éclairé et exprès de la personne est requis[871], sauf dans le cas où l'examen des caractéristiques génétiques d'une personne à des fins de recherche scientifique a été réalisé à partir d'éléments du corps de cette personne prélevés à d'autres fins lorsque cette personne, dûment informée de ce projet de recherche, n'a pas exprimé son opposition[872].

B - Les limites du consentement, la protection du malade en dépit de sa volonté

176. L'accès aux données est considéré comme un traitement, de même que la transmission de celles-ci. La personne prise en charge par le système de santé devrait donc pouvoir autoriser le traitement des données qui sont issues de cette prise en charge. Le RGPD a toutefois laissé des marges de manœuvre aux Etats membres s'agissant notamment du traitement des données de santé car dans le domaine de la santé l'Union européenne n'a qu'une compétence d'appui[873]. Un régime particulier ressort des dispositions du Code de la santé publique : il y est prévu une interdiction d'accéder aux dossiers du patient **(1)** de cession des données à titre onéreux **(2)**.

1 - L'interdiction d'accéder au DMP et à l'espace numérique de santé malgré le consentement

177. L'interdiction de traitement des données contenues dans le dossier médical, une limite au consentement. La première hypothèse, explicitement prévue par le législateur concerne le traitement des données contenues dans le dossier médical. Il s'agit donc

[871] LIL, art. 75.
[872] CSP, art. 1131-1-1.
[873] C. CASTETS-RENARD, *Rep. dr. eur.*, « La protection des données personnelles dans les relations internes à l'Union européenne – La protection des données personnelles en matière civile et commerciale », oct. 2018, (mise à jour mai 2019), n° 109.

d'informations couvertes par le secret car issues de la relation de soins. A l'occasion de la transposition de la directive de 1995 par la loi du 6 août 2004[874], la commission des lois avait proposé de restreindre la portée du consentement en matière de traitement de données afin « *d'éviter que des organismes tels que des compagnies d'assurance ou des employeurs puissent, au seul motif qu'ils auraient obtenu le consentement de l'intéressé, procéder à la collecte et au traitement de données sensibles* »[875]. Il s'agissait de faire en sorte que les individus ne subissent aucune pression au moment de la conclusion de ces contrats[876]. A cette fin, l'article L. 1111-18 du Code de la santé publique interdit l'accès au dossier médical partagé et procède à une pénalisation par renvoi au texte d'incrimination punissant la violation du secret professionnel[877]. Plusieurs remarques peuvent être formulées à l'égard de ce texte. Outre le fait que la technique de pénalisation par renvoi soit « paresseuse »[878] et participe à l'éclatement du droit pénal[879], il faut constater une fois encore la piètre qualité du texte. L'article dispose en effet d'un *interdit* or les textes d'incrimination décrivent en principe un comportement : tel fait décrit est puni de telle peine. Interdire l'accès au dossier médical partagé ne permet pas de connaitre le comportement prohibé. Si l'on imagine bien que le médecin du travail pourrait se voir autoriser l'accès au dossier médical partagé[880] et pourrait alors le consulter grâce à sa carte de professionnel de santé[881], il en est de même pour les éventuels cocontractants ;

---

[874] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[875] A. TÜRK, *Rapport fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, n° 218, 19 mars 2003, p. 60.

[876] *Ibid.* p. 60.

[877] Art. L. 1111-8 CSP : « *L'accès au dossier médical partagé est notamment interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties. L'accès à ce dossier ne peut également être exigé ni préalablement à la conclusion d'un contrat, ni à aucun moment ou à aucune occasion de son application. Le dossier médical partagé n'est pas accessible dans le cadre de la médecine du travail. Tout manquement aux présentes dispositions donne lieu à l'application des peines prévues à l'article 226-13 du code pénal* »

[878] E. DREYER, *Droit pénal général*, LexisNexis, 2014, n° 412.

[879] *Ibid.* ; dans le domaine des assurances C. AMBROISE-CASTEROT, « Consommation d'assurances et choix des textes applicables : code de la consommation ou code des assurances ? », *RSC* 2018, p. 95.

[880] L'autorisation émanant du patient lui-même.

[881] La CPS est délivrée à tous les médecins inscrits au tableau de l'ordre et donc également au médecin du travail (v. CNOM, *Le dossier médical en santé au travail (dmst)*, 17 et 18 décembre 2015, p. 7).

particulièrement en matière d'assurance-crédit, domaine dans lequel la connaissance de l'état de santé du cocontractant est essentiel à la formation du contrat[882]. Le médecin conseil de l'assurance pourrait en effet également accéder au dossier médical[883]. On suppose alors que c'est le fait d'accéder directement au dossier médical partagé qui est prohibé bien que la formulation du texte ne permette pas de l'affirmer. En effet, doit-on considérer que l'accès prohibé est caractérisé lorsque c'est la personne qui y accède directement devant le professionnel en question ? Le terme d'*accès* laisse supposer un comportement positif de la part de l'agent. L'infraction telle que créée par la loi du 17 août 2004[884] a été d'abord transférée dans le Code de la sécurité sociale[885]. L'examen de cet article dans sa version d'origine, articulé avec une disposition relative au résumé standardisé de sortie (RSS) [886], permet de comprendre que c'est bien l'accès sur autorisation du patient qui est visée. Outre l'absence de clarté du texte, il faut remarquer, qu'à l'instar de l'incrimination figurant à l'article L. 1110-4 al. 5 du Code de la santé publique, c'est encore la curiosité du tiers qui est sanctionnée, la référence à la peine dont fulmine la violation du secret professionnel invite à penser qu'il a été créé « *des sous-catégories d'infractions unies entre elles par […] des préoccupations communes* »[887].

178. La préservation du fait secret malgré la volonté du malade. L'article L. 1111-18 du Code de la santé publique fulmine une peine qui sanctionne le comportement de la partie « forte » qui profiterait de la partie « faible »[888]. Cette interdiction de traitement et plus

---

[882] Sur cette question v. C. JAY, *Le risque santé et la souscription d'assurance-crédit*, B. PY (ss. la dir.), soutenue le 11 déc. 2017, Université de Lorraine.

[883] Un auteur semble d'ailleurs considérer que c'est bien l'accès direct, par certains professionnels de santé, qui est sanctionné : « *Certains professionnels de santé sont cependant interdits d'accès au DMP, notamment les médecins du travail, comme en dispose l'article L. 1111-18 du CSP* » (V. MESLI, « Quelles articulations entre le dossier médical personnel et le dossier médical en santé au travail ? », *RDSS* 2014, p. 266).

[884] Si la volonté de créer cette infraction avait émergé lors des travaux de préparatoire de la loi de transposition de la directive de 1995 sur les données personnelles, une telle infraction ne pouvait figurer dans la loi de transposition c'est donc au sein de la loi n°2004-810 du 13 août 2004 relative à la sécurité sociale (*JORF* 17 août 2004) que l'infraction est finalement créée et figure dans un premier temps au Code de la sécurité sociale.

[885] CSS art. L.161-36-3 (version en vigueur du 17 août 2004 au 22 décembre 2006).

[886] CSS art. L. 161-36-2 (version issue de la Loi n°2009-879 du 21 juillet 2009 - art. 50).

[887] E. DREYER, *Droit pénal général*, *op. cit.*, n° 412.

[888] La conception du contrat conçu comme « *un échange économique égalitaire* » (J. ROCHFELD, *Les grandes notions du droit privé*, coll. Thémis, PUF, 2011, notion n° 7, section 1) et reposant donc sur l'idée que les cocontractants sont libres et égaux et qu'ils agissent ainsi de manière rationnelle a été remise en cause depuis le XIX^{e} siècle et le droit comme le juge sont intervenus pour prendre en compte le fait social que sont les inégalités économiques entres les parties dans certaines relations contractuelles. Le contrat de travail est le premier contrat identifié et analysé par R. SALEILLES comme une catégorie de contrat dits « d'adhésion » et que l'auteur définit ainsi : « *il y a prédominance exclusive d'une volonté, agissant comme volonté unilatérale, qui dicte sa loi, non plus à un individu, mais à une collectivité indéterminée, et qui s'engage déjà, par avance, unilatéralement, sauf adhésion de ceux qui voudront accepter la loi du contrat* ». (R. SALEILLES, *De la déclaration de volonté :*

spécifiquement d'accès ne concerne toutefois que le seul dossier médical partagé. L'une des particularités de ce dossier informatisé réside dans la masse d'informations qu'il est censé contenir. En effet, il est conçu[889] comme le remplaçant du dossier patient informatisé de chaque établissement, des dossiers de médecine de ville et devrait, à terme, être interconnecté avec ou intégrer le dossier pharmaceutique[890].

Une seconde particularité réside dans le fait que le titulaire du DMP peut y accéder en ligne, et pourrait donc permettre à un tiers d'y accéder dès lors qu'il fournirait les codes d'accès en ligne ou y accéderait en présence de ce tiers, via une connexion internet depuis n'importe quel outil informatique. Le DMP, pensé comme un outil au service de la coordination et du suivi du malade, c'est-à-dire dans son intérêt, pourrait alors être détourné de sa finalité. L'informatique se trouverait au service de la partie forte. Le législateur a donc souhaité renforcer la protection de la personne partie à certains contrats en réduisant la maîtrise qu'il a de ses données de santé au travers de la sanction de la partie qui entendrait profiter du déséquilibre préexistant.

179. L'impossibilité d'exiger la transmission des données contenues dans l'espace numérique. L'espace numérique de santé a été créé par la loi du 24 juillet 2019[891], le contenu accessible via cette interface est fixé à l'article L. 1111-13-1-IV al. 2 du Code de la santé publique[892]. Le même article dispose : « *La communication de tout ou partie des données de*

Contribution à l'étude de l'acte juridique dans le Code civil allemand, Pichon, 1901, p. 229). Les contrats d'assurances entrent également dans cette catégorie (F. CHENEDE, « Le contrat d'adhésion de l'article 1110 du Code civil », *JCP G* 2016, n° 27, p. 1334). Si les modes d'intervention du législateur et du juge les plus couramment évoqués consistent dans l'obligation d'information renforcée (M. FABRE-MAGNAN, *De l'obligation d'information dans les contrats. Essai d'une théorie*, LGDJ, 1992), et s'agissant du contenu du contrat, sur les clauses abusives. L'article L. 1111-8 du Code de la santé publique constitue une modalité de protection de la partie faible intervenant *a priori* de la conclusion du contrat et pendant l'exécution du contrat de travail.

[889] Bien que sa mise en œuvre soit encore loin d'atteindre le niveau d'efficacité souhaité par le législateur.

[890] L'article R. 1111-30 du Code de la santé publique dresse une liste non exhaustive des informations contenues dans le DMP.

[891] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, *JORF* n°0172 du 26 juillet 2019.

[892] CSP art. L. 1111-13-1 : « *Ses données administratives ; Son dossier médical partagé ; Ses constantes de santé éventuellement produites par des applications ou des objets connectés référencés en application du III ou toute autre donnée de santé utile à la prévention, la coordination, la qualité et la continuité des soins ; L'ensemble des données relatives au remboursement de ses dépenses de santé ; Des outils permettant des échanges sécurisés avec les acteurs du système de santé, dont une messagerie de santé sécurisée permettant à son titulaire d'échanger avec les professionnels et établissements de santé et des outils permettant d'accéder à des services de télésanté ; Tout*

l'espace numérique de santé ne peut être exigée du titulaire de cet espace lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et lors de la conclusion ou de l'application de tout autre contrat, à l'exception des contrats relatifs aux services et outils numériques référencés en application du III du présent article ». Il nous semble que cette disposition doit être rapprochée de l'incrimination définie à l'article L. 1110-4-V du Code de la santé publique et de celle posée à l'article L. 1111-18 du même Code. Il nous paraît envisageable que le fait d'exiger la communication des données de l'espace numérique de santé lors de la conclusion d'un contrat puisse être sanctionné sur le fondement de l'article L. 1110-4-V du Code de la santé publique.

180. Une préoccupation commune. L'infraction prévue à l'article L. 1111-18 du Code de la santé publique ne peut être rattachée au seul respect de la vie privée, le consentement de la personne justifiant en principe l'atteinte à cet intérêt protégé il en est de même pour la disposition relative à la communication des données de l'espace numérique de santé. De même, l'infraction prévue à l'article L. 1110-4-V du même Code – en ce qu'elle protège également le fait secret de la curiosité des tiers – sanctionne spécifiquement l'atteinte au secret des informations relatives au malade, indépendamment du consentement de celui-ci. De plus, ce n'est pas le comportement du professionnel qui est visé. En cela les deux infractions et la disposition prévue à l'article L. 1111-13-1-IV al. 2 du Code de la santé peuvent être rapprochées. Leur préoccupation n'est pas tant le respect de la vie privée que la protection du secret des informations ou des données relatives au malade.

2 - L'interdiction de cession des données à titre onéreux

181. Portée de l'interdiction. Les limites du consentement de la personne au traitement de ses données sensibles trouvent encore un écho dans une autre infraction inscrite au Code de la santé publique à l'occasion de la loi relative à la sécurité sociale de du 13 août 2004[893]. Il s'agit, une fois encore, d'une infraction érigée lors de la création du DMP. L'article L. 1111-8- VII du Code de la santé publique qui porte sur l'hébergement des données de santé incrimine la cession

---

service numérique, notamment des services développés pour favoriser la prévention et fluidifier les parcours, les services de retour à domicile, les services procurant une aide à l'orientation et à l'évaluation de la qualité des soins, les services visant à informer les usagers sur l'offre de soins et sur les droits auxquels ils peuvent prétendre ainsi que toute application numérique de santé référencés en application du même III ; Le cas échéant, les données relatives à l'accueil et l'accompagnement assurés par les établissements et services sociaux et médico-sociaux mentionnés à l'article L. 312-1 du code de l'action sociale et des familles ».

[893] Loi n°2004-810 du 13 août 2004 relative à la sécurité sociale, *JORF* 17 août 2004.

à titre onéreux des données de santé directement ou indirectement identifiantes, même lorsque la personne concernée a donné son consentement. Le texte d'incrimination procède à une pénalité par renvoi à l'article 226-21 du Code pénal. La cession n'est pas expressément définie comme une opération de traitement mais il pourrait s'agir d'une forme d'utilisation des données. Cette infraction selon le législateur « *s'inscrit dans une démarche ancienne de protection des patients, actualisée en prenant en compte la diffusion des nouvelles technologies* »[894]. Cette démarche ancienne de protection des patients n'est pas sans rappeler les fondements du secret professionnel. Toutefois, bien que l'article L. 1111-8 du Code de la santé publique porte sur les conditions d'hébergement des données de santé, l'interdiction de cession des données de santé à titre onéreux est générale. Elle ne concerne pas uniquement les hébergeurs et sanctionne la cession à titre onéreux qui serait effectuée par n'importe quelle personne, la seule condition tenant au fait que les données de santé sont issues d'une prise en charge sanitaire[895]. Lorsque cette infraction est commise par un professionnel soumis au secret, deux qualifications semblent alors en concours. En effet, la cession de données de santé issues d'une prise charge sanitaire par un professionnel soumis au secret pourra être qualifiée de violation du secret professionnel et de cession illicite de données de santé à titre onéreux. C'est néanmoins la seconde qualification qui semble devoir être retenue en vertu du principe *specialia generalibus dérogeant*.

182. La pénalité par renvoi au texte d'incrimination sanctionnant le détournement de finalité. Le fait de procéder par renvoi à l'article 226-21 du Code pénal se conçoit dès lors qu'il s'agit moins de sanctionner la conséquence de la cession à un tiers – la prise de connaissance des données de santé par un tiers à la prise en charge – que le détournement de la finalité pour laquelle les données avaient été originellement traitées. Le traitement des données de santé étant autorisé sans qu'il soit nécessaire d'obtenir le consentement de la personne lorsque le traitement

---

[894] A. VASSELLE, Rapport n° 424 (2003-2004) fait au nom de la commission des affaires sociales, déposé le 21 juillet 2004, p. 36.

[895] En ce sens v. D. BOURCIER et P. DE FILIPPI, « Vers un droit collectif sur les données de santé », *RDSS* 2018, p. 444. Les auteurs précisent que cela concerne d'autres professionnels que les acteurs de soins puisque les données de santé peuvent être : « *détenues par d'autres acteurs qu'ils soient techniciens (par exemple, les développeurs informaticiens) ou administratifs (par exemple, les gestionnaires de droits sociaux)* ». De notre point de vue cette précision n'est pas utile puisque nous considérons que ce qui importe, s'agissant de la portée du consentement, c'est la source des données et non les personnes qui détiennent ces données.

a pour finalité la prise en charge sanitaire de la personne concernée, le consentement devient, en principe, nécessaire lorsque le responsable du traitement envisage une réutilisation de ces données à d'autres fins[896]. L'infraction sanctionne donc un détournement, indépendamment du consentement de la personne. Il s'agit d'une dérogation à l'exception de l'interdiction du traitement des données sensibles. Celle-ci paraît trouver sa justification dans la source des données sensibles en cause.

183. Comparaison avec l'abus de confiance. Il nous semble qu'une comparaison avec l'abus de confiance peut éclairer l'intérêt de l'incrimination et plus encore le sens de la pénalité par renvoi. L'abus de confiance sanctionne « *le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé* »[897] tandis que l'article 226-21 du Code pénal punit « *le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé ou par les déclarations préalables à la mise en œuvre de ce traitement* »[898]. Il apparaît que la qualification d'abus de confiance – dont la dématérialisation a été longuement étudiée par la doctrine[899] – et celle de détournement de finalité d'un traitement de données peuvent se trouver en conflit. Ces infractions s'apparentent non seulement quant à leur objet mais également en ce que chacune sanctionne un *détournement de finalité*. L'abus de confiance punit effectivement un « *usage contraire à la finalité de la chose* »[900] cette finalité ayant été déterminée par celui qui a remis la chose. Le détournement de finalité d'un traitement de données personnelles consiste également en un usage contraire à la finalité du traitement tel que déterminé par la loi,

---

[896] Il s'agit bien du principe car la réalité est plus nuancée, certaines réutilisations n'étant pas soumises au consentement de la personne concernée, v. *infra* n° 343.
[897] CP, art. 314-1.
[898] CP, art. 226-21.
[899] V. notamment G. BEAUSSONIE, *La prise en compte de la dématérialisation des biens par le droit pénal. Contribution à l'étude de la protection pénal de la propriété*, préf. B. DE LAMY, coll. Bibliothèque de droit privé, t. 532, LGDJ, 2012 ; « La dématérialisation de l'abus de confiance », *AJ pénal* 2017, p. 215 ; L. SAENKO, « Abus de confiance, remise précaire et dématérialisation », *RTD com.* 2017, p. 447 ; H. MATSOPOULOU, «Abus de confiance : détournement de clientèle », *Rev. sociétés* 2018, p. 56.
[900] A. LEPAGE et H. MATSOPOULOU, *Droit pénal spécial*, coll. Thémis droit, PUF, 2015, n° 782.

le règlement ou la décision de la CNIL qui a autorisé le traitement. Lorsque la personne consent à l'utilisation de ses données dans une finalité déterminée elle autorise un certain usage de ses données personnelles. Le RGPD précise que dans les cas où le consentement de la personne n'a pas à être recherché, le responsable de traitement « *lorsqu'il a l'intention de traiter les données à caractère personnel à des fins autres que celles pour lesquelles elles ont été collectées,* […] *devrait, avant de procéder à ce traitement ultérieur, fournir à la personne concernée des informations au sujet de cette autre finalité et toute autre information nécessaire* »[901]. Dans le cas du traitement de données sensibles, le responsable du traitement ne peut se contenter d'informer la personne mais doit obtenir son consentement explicite. Depuis l'entrée en vigueur du RGPD le consentement explicite au traitement des données de santé se substitue aux formalités préalables[902]. En rapprochant le fait de céder les données de santé à titre onéreux malgré le consentement de la personne à un détournement de finalité, le détournement de finalité pouvant s'apparenter à une forme d'abus de confiance, l'on est incliné à penser que c'est également la confiance qui est protégée. Mais ce n'est pas, dans ce cas, la confiance que la personne porte dans le responsable du traitement ou le sous-traitant puisque son consentement ne peut justifier la cession, mais la confiance générale dans les responsables de traitement et les sous-traitants[903], tels que les hébergeurs de données de santé.

184. Conflit de qualifications : violation du secret professionnel et cession de données à titre onéreux. Lorsque la cession des données de santé à titre onéreux est opérée par une personne soumise au secret au titre des articles 226-13 du Code pénal et L. 1110-4 du Code de la santé publique alors la cession peut également être qualifiée violation du secret professionnel. Dans les deux cas s'opère une transmission qui peut être qualifiée de *révélation*[904] ou de *cession* également prohibée. En pareilles circonstances – et tenant compte du fait que la violation du secret professionnel comme la cession de données de santé à titre onéreux porte atteinte à la confiance publique dans les personnes qui traitent ou recueillent l'information – il semble que ce soit l'infraction prévue au Code de la santé publique qui doive être retenue. La spécificité de

---

[901] RGPD consid. 61.

[902] Avant l'entrée en vigueur du RGPD la loi informatique et libertés prévoyait un certain nombre de formalités préalables selon la sensibilité des données et les finalités de traitement. La grande majorité de ces formalités disparaissent avec le RGPD.

[903] Défini à l'article 4 du RGPD comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ».

[904] Le moyen de la révélation est indifférent, de même que la forme des informations, il peut donc s'agir de données dès lors que la personne est identifiée ou identifiable.

l'incrimination impose une telle solution. Du point de vue disciplinaire, lorsque la cession est opérée par un professionnel de santé dont la profession s'est dotée d'un Code de déontologie, la violation du devoir de secret sera le seul fondement envisageable.

185. Neutralisation de la portée du consentement, préservation du fait secret et résistance à l'autodétermination informationnelle. Les infractions éparses figurant au Code de la santé publique semblent unies par une préoccupation commune : la préservation du fait secret en dépit de la volonté du malade. Tandis que nous avons démontré plus avant que les informations couvertes par le secret étaient prises en compte par les infractions protégeant la propriété et celles protégeant la vie privée des personnes, l'on trouve au travers des exemples évoqués matière à rejeter ces deux fondements. Les limites du consentement à autoriser l'accès et l'interdiction de la cession des données pourrait nous amener à envisager une troisième voie. Celle de l'autodétermination informationnelle. Nous avons souligné que l'atteinte à la vie privée est justifiée par le consentement de la personne. Le principe d'autodétermination, issu de la doctrine et de la jurisprudence allemandes, consiste à dépasser la conception traditionnelle de la vie privée dont la particularité est de faire intervenir le consentement comme une justification de l'atteinte. La perspective serait de « *passer d'une posture uniquement défensive de protection des données personnelles, à une posture plus offensive de maîtrise, de contrôle et plus encore de capacité pour l'utilisateur à mobiliser et utiliser ses données pour ses propres finalités* »[905]. Or, les quelques dispositions étudiées tendent à admettre que les données couvertes par le secret professionnel ne sont pas totalement maîtrisées par les individus. Sans doute est-il possible de trouver un début de justification dans la notion de *bien commun*. Les grandes bases de données de santé[906] ont pu être qualifiées de bien commun dès 2013 à l'occasion d'un rapport[907] ayant servi de point de départ à la réflexion sur la création du système national des données de santé[908]. Plus récemment, le Conseil National du Numérique a rédigé

[905] Conseil National pour le Numérique, *La santé, Bien Commun de la société numérique*, Rapport remis à la ministre des Affaires sociales, de la Santé et des Droits des femmes, octobre 2015.
[906] SNIIRAM et PMSI.
[907] P.- L. BRAS et A. LOTH, *Rapport sur la gouvernance et l'utilisation des données de santé*, septembre 2013 (disponible sur <https://solidarites-sante.gouv.fr/IMG/pdf/Rapport_donnees_de_sante_2013.pdf>, dernière consultation le 12 nov. 2018).
[908] Conseil National du Numérique, *La santé bien commun de la société numérique ; construire le réseau du soin et du prendre soin*, Rapport remis à la Ministre des Affaires sociales, de la Santé et des Droits des femmes, Oct. 2015, p. 15 (disponible sur <https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000719.pdf> ; dernière consultation le 12 nov. 2018).

un rapport intitulé « La santé, bien commun de la société numérique » portant, entre autre, sur les données de santé et à l'occasion duquel il propose à la fois de « *faciliter l'ouverture et la réutilisation des données médico-administratives en faveur de la recherche et de l'innovation, dans le respect des droits fondamentaux* »[909] tout en affirmant « *Concrétiser l'empowerment individuel et collectif sur les données de santé, en termes de protection, de maîtrise et de mobilisation à la faveur de nouveaux usages* »[910]. Pour concilier ces deux approches le recours à la notion de bien commun paraît être propice. Comme le souligne Madame Bourcier « […] *le renouveau assez spectaculaire de cette notion émerge de la critique radicale de l'individualisme et de la défiance vis-à-vis de l'Etat néolibéral* »[911], le même auteur dans un développement relatif aux données de santé envisagées comme *bien commun* ajoute que « […] *les données personnelles et, en particulier, des données de santé, ne peuvent pas être protégées avec une approche libérale concentrée sur la maximisation des libertés individuelles (par le biais du consentement ou de la patrimonialisation de ces données) mais il serait plutôt nécessaire d'adopter dans une optique plus communautaire ou collective, qui pourrait exiger une limitation de certaines libertés individuelles, au nom de l'intérêt général et du bien commun* »[912]. Nous aurons l'occasion de revenir sur cette question. Nous souhaitons à ce stade souligner que le secret des données relatives à une personne prise en charge par un professionnel intervenant dans le système de santé est assuré par les dispositions spécifiques prévues tant par le RGPD que par les dispositions inscrites au Code de la santé publique. Il nous faut à présent compléter notre étude du champ de la protection des données à caractère personnel dans le

---

[909] *Ibid.*
[910] *Ibid.*
[911] D. BOURCIER, « Le bien commun, ou le nouvel intérêt général », Mélanges en l'honneur du professeur Jaques Chevallier, LGDJ, 2013, p. 92.
[912] D. BOURCIER et P. DE FILIPPI, « Vers un droit collectif sur les données de santé », *op. cit.* ; Les auteurs résument d'ailleurs les travaux de Monsieur Cohen (J. E. COHEN, « Turning Privacy Inside Out », *in Theoretical Inquiries in Law* 20.1 (2019 Forthcoming) en affirmant que l'auteur défend « *une optique plus paternaliste, où l'État est responsable pour garantir une protection suffisante de la vie privée, non pas en conférant des droits aux individus, mais en introduisant des contraintes sur la façon dont les opérateurs peuvent collecter ou traiter les données personnelles, indépendamment du consentement des personnes concernées* ». Par ailleurs, la vision de Monsieur Bellanger rejoint celles de ces auteurs. Dans un article portant sur les données personnelles, l'auteur évoque la question du consentement. Expliquant que le réseau de données – il évoque à ce titre des données personnelles qui « *ne sont plus granulaires mais réticulaires, c'est-à-dire organisées en réseau* » –, situe nécessairement le débat entre les deux conceptions – patrimonialiste et personnaliste – évoquées plus avant. Il s'agirait donc encore d'une autre voie.

domaine de la santé en examinant l'articulation des dispositions dédiées et du secret professionnel.

§ 2 - Le secret professionnel, condition et conséquence du traitement des données pour certaines finalités déterminées

186. L'examen du régime dérogatoire propre au traitement des données sensibles nous apprend que ces données peuvent être traitées sans qu'il soit besoin d'obtenir le consentement explicite de la personne concernée dès lors que le traitement répond à des finalités spécifiques propres au domaine de la santé. Qu'il s'agisse de l'exception tenant à la prise en charge des personnes[913] ou de celle autorisant le traitement pour des finalités d'intérêt public dans le domaine de la santé[914], il est en outre exigé, dans le premier cas, que les données soient traitées « *par un professionnel de la santé soumis à une obligation de secret professionnel* »[915] et dans le second cas que l'Etat membre « *prévoi*[e] *des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel* »[916]. Cela révèle un double mouvement : la soumission au secret professionnel est une condition du traitement des données sensibles lorsque la finalité du traitement est la prise en charge des personnes par le système de santé et de protection sociale **(A)** mais il est également une garantie de protection des données sensibles et notamment des données de santé bien que ce ne soit pas le seul mécanisme – il y participe. La soumission au secret professionnel est alors une conséquence du traitement **(B)**.

A - L'assujettissement au secret professionnel, condition au traitement des données sensibles

187. Exception ou condition. Au titre des exceptions prévues par les dispositions relatives à la protection des données figurant à l'article 9 du RGPD, une liste prévoit les cas dans lesquels les données sensibles peuvent être traitées en dépit de l'interdiction de principe. La première de ces exceptions a pour condition le consentement explicite de la personne concernée. Le

[913] RGPD art. 9 paragraphe 2 h).
[914] RGPD art. 9 paragraphe 2 i).
[915] RGPD art. 9 paragraphe 2 h).
[916] RGPD art. 9 paragraphe 2 i).

règlement européen, dans la ligne de la loi informatique et libertés telle que modifiée à l'occasion de la transposition de la directive de 1995[917], prévoit une série d'exceptions qui correspondent à des finalités de traitement[918]. Il a pu être considéré que le secret professionnel constituait une exception à l'interdiction de traiter des données sensibles[919]. Il s'agit, à notre sens, d'un raccourci qui contribue à opacifier l'articulation entre les textes. La soumission au secret professionnel ne constitue pas une telle exception. Le traitement des données sensibles est possible pour certaines finalités déterminées inscrites à l'article 9 du RGPD, sans que la personne ait donné son consentement exprès. Le paragraphe 2 i) de l'article 9 du règlement prévoit ces finalités que sont, entre autres, la médecine préventive, les diagnostics médicaux, l'administration de soins ou de traitements et la gestion de services de santé. Les traitements pour de telles finalités doivent être mis en œuvre, selon le droit interne « […] *par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal* »[920]. Ainsi, la soumission au secret professionnel n'est pas une exception à l'interdiction de traitement mais une condition à la mise en œuvre du traitement pour certaines finalités, pour lesquelles le consentement exprès n'est pas exigé. Cela fait une différence importante puisque le champ de l'exception se trouve réduit par rapport à l'interprétation précédemment évoquée. Il faut donc ensuite préciser ce que recouvrent les finalités inscrites au paragraphe 2 h) de l'article 9 du RGPD et de l'article 44 de LIL.

188. Finalités relatives à la santé. Pour comprendre les conditions de traitement dans le cadre de cette exception il est nécessaire de saisir l'ensemble des dispositions générales puisqu'elles s'appliquent toutes, indifféremment de la nature des données : il s'agit d'abord, pour le responsable du traitement, de respecter les conditions de licéité applicables à tout

---

[917] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[918] Ainsi, finalités et conditions se confondent.
[919] A. DEROUDILLE, « Le secret professionnel dans le règlement général à la protection des données », *RFDA* 2018, p. 1112.
[920] Art. 44 1° de la loi informatique et libertés telle que modifiée par Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel ;

traitement de données à caractère personnel[921]. Ainsi, le responsable du traitement devra en principe obtenir le consentement de la personne concernée sauf lorsque le traitement a pour finalité « *l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* »[922]. L'exposé des motifs du règlement est éclairant pour savoir ce qui est entendu par « *intérêt public* »[923] et nous apprend notamment qu'il peut s'agir des finalités de santé entendues comme *finalités de santé publique et de gestion des services de soins de santé* mais ne s'y limite pas. Lorsque ces intérêts légitimes sont poursuivis le traitement des données à caractère personnel ne nécessite pas le consentement de l'individu pour être licite. La condition de consentement, explicite cette fois, reparait s'agissant du traitement des données sensibles. Toutefois le consentement n'est plus exigé lorsque les données sont traitées « *aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé* »[924]. Il semble, a priori, que les finalités de santé permettant de ne pas rechercher le consentement explicite de la personne pour le traitement de ces données sensibles soient plus restreintes que celles prévues pour le traitement des données à caractère personnel. Plusieurs indications permettent de relativiser une telle interprétation du texte. Les motifs du règlement européen permettent encore d'interpréter cette exception au traitement des données sensibles. Ainsi, le considérant 52 du RGPD énonce que « *Ces dérogations sont possibles à des fins de santé, en ce compris la santé publique et la*

---

[921] Art. 4 LIL (tel que modifié par l'Ordonnance n° 2018-1125 *préc.*) également article 5 RGPD.
[922] *Ibid.* n°5
[923] Ainsi le considérant 52 du RGPD précise (nous soulignons) « *Des dérogations à l'interdiction de traiter des catégories particulières de données à caractère personnel devraient également être autorisées lorsque le droit de l'Union ou le droit d'un État membre le prévoit, et sous réserve de garanties appropriées, de manière à protéger les données à caractère personnel et d'autres droits fondamentaux* ***lorsque l'intérêt public le commande****, notamment le traitement des données à caractère personnel dans le domaine du droit du travail et du droit de la protection sociale, y compris les retraites, et* ***à des fins de sécurité, de surveillance et d'alerte sanitaire, de prévention ou de contrôle de maladies transmissibles et d'autres menaces graves pour la santé. Ces dérogations sont possibles à des fins de santé, en ce compris la santé publique et la gestion des services de soins de santé, en particulier pour assurer la qualité et l'efficience des procédures de règlement des demandes de prestations et de services dans le régime d'assurance-maladie, ou à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques*** » (nous soulignons).
[924] Art. 6 de la LIL (modifié par l'Ordonnance n° 2018-1125 *op. cit.*) qui renvoie à l'article 9 du RGPD. Toutefois en droit national l'exception est restreinte et ne comprend pas la médecine du travail et l'appréciation de la capacité de travail du travailleur.

gestion des services de soins de santé »[925]. C'est l'interprétation qui avait déjà été retenue sous l'empire des anciennes dispositions, c'est-à-dire la loi informatique et libertés modifiée à l'occasion de transposition de la directive de 1995[926]. Les finalités de traitement des données sensibles n'imposant pas l'obtention du consentement exprès de la personne concernée devraient donc être appréciées largement.

189. Des finalités conçues largement. Toujours dans les considérants, le RGPD donne une indication de l'interprétation que les Etats devraient avoir de la *santé publique*. Les motivations du règlement renvoient à un règlement européen qui définit la santé publique : « *désigne tous les éléments relatifs à la santé, à savoir l'état de santé, morbidité et handicaps inclus, les déterminants ayant un effet sur cet état de santé, les besoins en matière de soins de santé, les ressources consacrées aux soins de santé, la fourniture des soins de santé, l'accès universel à ces soins, les dépenses de santé et leur financement, ainsi que les causes de mortalité* »[927]. Cette définition est particulièrement large. L'incertaine portée des considérants[928] impose néanmoins de rechercher l'interprétation faite par le juge national. Cette dérogation n'étant pas neuve, plusieurs décisions peuvent étayer notre propos. Tout d'abord dans un arrêt du 17 novembre 2017[929], le Conseil d'État confirme la légalité d'un décret et d'un arrêté autorisant la transmission par les biologistes médicaux[930] à l'Agence française de biomédecine (ABM) de données relatives au dépistage prénatal de la trisomie 21. La Fondation qui contestait les textes alléguait leur illégalité en ce qu'ils ne prévoyaient pas le consentement des parturientes comme condition à la transmission de leurs données de santé. Pour le Conseil d'Etat la transmission ne nécessite pas le consentement de la patiente en application de l'exception figurant à l'ancien article 8 de la LIL, la transmission de ces données entrant dans le cadre « *des traitements nécessaires aux fins [...] des diagnostics médicaux [...] et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions*

---

[925] Consid. 52 RGPD.
[926] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, *préc.*
[927] Règlement (CE) n° 1338/2008 du Parlement européen et du Conseil du 16 décembre 2008 relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail, art. 3.
[928] S. LEMAIRE, « Interrogations sur la portée juridique du préambule du Règlement Rome I », *D.* 2018, p. 2157.
[929] CE Sect., 17 novembre 2017, n° 401212, *Fondation Jérôme Lejeune* ; *AJDA* 2018, p. 428 ; *D.* 2018, p. 1033, obs. B. FAUVAQUE-COSSON et W. MAXWELL ; *AJ Fam.* 2017, p. 615, obs. A. DIONISI-PEYRUSSE.
[930] Qui sont des médecins, des pharmaciens ou des professionnels de santé v. art. L. 6213-1 et svt. CSP.

l'obligation de secret professionnel prévue par l'article 226-13 du code pénal »[931]. Il ressort de la décision que la finalité de diagnostics médicaux est entendue largement[932]. Au regard de la définition de la santé publique il s'agit de la qualité des techniques de dépistage et de diagnostics prénataux[933]. La condition tenant à la soumission au secret professionnel est ainsi nécessaire mais non suffisante[934]. Dans un arrêt du 8 juillet 2015 concernant la conservation de données relatives à l'homosexualité des personnes se présentant pour un don de sang, sans leur consentement[935], la chambre criminelle de la Cour de cassation jugeait également que le délit prévu à l'article 226-19 du Code pénal sanctionnant le fait de traiter des données sensibles sans le consentement de la personne concernée n'était pas constitué dès lors que l'article 8 de la loi informatique et libertés l'autorisait, et de préciser que « *constitue une mesure légitime, nécessaire à la protection de la santé, définie par la loi avec suffisamment de précision pour éviter l'arbitraire, et de nature à assurer, en l'état, entre le respect de la vie privée et la sauvegarde de la santé publique, une conciliation qui n'est pas déséquilibrée* »[936]. Une question prioritaire avait été rendue dans cette même affaire[937]. Le Conseil constitutionnel, amené à se prononcer sur la constitutionnalité du texte d'incrimination prévue à l'article 226-19 du Code pénal avait estimé que le traitement des données relatives aux donneurs entrait dans une des

---

[931] CE Sect., 17 novembre 2017, n° 401212, *op. cit.*, point n° 14.

[932] La médecine préventive, les diagnostics médicaux, l'administration de soins ou de traitements, sont des activités – avant d'être des finalités de traitement – qui ne peuvent, en principe, être mises en œuvre que par des professionnels de santé. Les conditions de licéité sont donc identiques pour les actes thérapeutiques et préventifs. Outre les actes médicaux qui ne peuvent être pratiqués que par des personnes exerçant une profession médicale (médecin, sage-femme, pharmacien), certains actes de soins, de prévention ou traitements peuvent être effectués par des professionnels de santé dont les compétences juridiques sont fixées par décret (nommés décrets d'actes). Sur les conditions de licéité de l'acte médical v. B. PY, *Recherches sur les justifications pénales de l'activité médicale*, th. dact. ss. la dir. de J.-F. SEUVIC, 1993, Nancy II. La gestion des services de santé incombe à une pluralité d'acteurs qui ne sont pas seulement des professionnels de santé mais des personnels administratifs ou techniques (en ce sens v. D. BOURCIER et P. DE FILIPPI, « Vers un droit collectif sur les données de santé », *RDSS* 2018, p. 444). Aussi toutes les informations récoltées à l'occasion de ces activités sont-elles couvertes par le secret puisque toutes ces personnes sont soumises au secret professionnel (soit par l'article L. 1110-4 du Code de la santé publique soit par des textes spécifiques inscrits au Code de la santé publique. Pris dans leur acception la plus restreinte, les traitements de données sensibles, pour les finalités prévues à l'article 9 RGPD ne pourraient être mis en œuvre que par les professionnels autorisés à pratiquer de telles activités.

[933] *Ibid.* point n° 11.

[934] En l'espère les moyens permettant une protection adéquate « *de la vie privée* » des personnes tient dans le fait que la sécurité et la confidentialité sont assurées par le responsable du traitement, que les données transmises sont ensuite agrégées et que pour ce faire la durée de leur conservation n'excède pas ce qui est nécessaire à ce traitement (*Ibidem.* n° 11).

[935] Crim., 8 juill. 2015, *Bull. crim*., n°49 n° 13-86.267, *RSC* 2015, p. 651, obs. Y MAYAUD ; *D.* 2015, p. 1541; *Dr. pén.* 2015, n° 9, comm. 109, M. VERON.

[936] *Ibid.*

[937] Cons. Const., 19 sept. 2014, n° 2014-412 QPC, *AJDA* 2014, p. 1798 ; *D.* 2014, p. 1826 ; *Com. comm. électr.*, 2015, n° 1, comm. 7, A. DEBET.

exceptions prévues par la loi. Il visait l'exception autrefois prévue au paragraphe II 6° de l'article 8 de la LIL, et désormais inscrite à l'article 44 1° de la même loi, portant sur les finalités de « *médecine préventive, de diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel dont l'atteinte est réprimée par l'article 226-13 du code pénal* ». Un commentateur souligne la particularité d'une telle interprétation en ce que cette exception est « *généralement plutôt comprise comme s'appliquant aux dossiers médicaux tenus par les médecins ou par d'autres professionnels de santé* »[938]. Les finalités dont dispose l'article 44 de la LIL et le paragraphe 2 h) de l'article 9 du RGPD consisteraient donc dans celle, très vaste, de la protection de la santé.

190. Les conséquences d'une telle interprétation. Il nous semble que l'interprétation extensive de l'exception prévue au paragraphe II h) de l'article 9 du RGPD doive se comprendre au regard du régime de l'autre exception prévue au même article. Le paragraphe II i) de l'article 9 du RGPD prévoit qu'il est possible de traiter des données sensibles pour des motifs d'intérêt public dans le domaine de la santé publique. Cette possibilité existait avant l'entrée en vigueur du RGPD. La législation française prévoyait un régime spécifique pour cette exception, lequel figurait aux chapitres IX et X de la LIL qui visait les traitements pour des finalités d'intérêt public de recherche dans le domaine de la santé[939]. A l'occasion de la loi de modernisation de notre système de santé[940] et de la création du système national des données

---

[938] A. DEBET, « L'exclusion des hommes homosexuels du don de sang examinée sous l'angle de la protection des données », *Com. comm. électr.* 2015, n°1. Interprétation que confirme la doctrine de la CNIL qui, dans une fiche explicative à destination du public précise que cette exception concerne, entre autres, le « *dossier médical ou logiciel de gestion médico-administratif, télémédecine, PACS utilisé dans le domaine de l'imagerie médicale* », elle considère donc que cette exception vise la prise en charge des patients (<https://www.cnil.fr/fr/quelles-formalites-pour-les-traitements-de-donnees-de-sante-caractere-personnel>, consulté le 14 oct. 2019).

[939] Sur l'ancien régime du traitement des données à des fins de recherche médicale v. I. DE LAMBERTRIE et H. –J. LUCAS (ss. la dir.), *Informatique, libertés et recherche médicale*, coll. CNRS Droit, CNRS éditions, 2001 ; Pour une analyse des difficultés inhérentes au traitement des données en matière de recherche médicale v. notamment A. BAHR, C. BULACH, S. FABER, « Comment appliquer la loi Informatique et Libertés à la recherche médicale ? », *RGDM*, n°45, 2012, pp. 47-70 ; R. PERRAY, « Traitement de données personnelles dans le cadre de recherches médicales : vers un allégement des formalités », *Revue Lamy droit de l'immatériel*, 2007, n° 24, pp. 64-66 ; L. TILMAN, « Recherche et utilisation des données médicales : un cadre inadéquat ? », Cahiers *Droit, Sciences & Technologies*, 5 | 2015, pp. 89-98.

[940] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF*, n°0022 du 27 janvier 2016.

de santé[941], la loi informatique et libertés a été modifiée pour permettre plus de souplesse et notamment une réutilisation accrue des données de santé issues de la relation de soins[942] en ajoutant une sous-section consacrée au traitement pour des finalités de recherche, d'étude et d'évaluation ayant un intérêt public. Ensuite, par la loi du 20 juin 2018[943], le législateur a encore étendu cette possibilité en distinguant les finalités d'intérêt public et celles relatives à la recherche, à l'étude et à l'évaluation dans le domaine de la santé[944]. La possibilité de traiter des données à caractère personnel dans le domaine de la santé est donc étendue tout en conservant un régime spécifique en raison de l'application d'une marge de manœuvre prévue par le RGPD[945]. Si la nécessité d'obtenir le consentement de la personne se trouve réduite par l'élargissement du champ de cette exception, le législateur a en effet souhaité maintenir un régime particulier pour ce type de traitement. Les formalités préalables disparaissent[946]

---

[941] Art. L. 1460-1 et svt. modifiés par la Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé.

[942] Notamment souhaité par la Cour des comptes dans son rapport de 2016 (Cour des comptes, *Les données personnelles de santé gérées par l'assurance maladie. Une utilisation à développer, une sécurité à renforcer*, Communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale, Mars 2016)

[943] Loi n° 2018-493 du 18 juin 2018, *op. cit.*, art. 193.

[944] Le vocable utilisé mérite d'ailleurs d'être souligné : il s'agit du traitement des données à caractère personnel *dans le domaine de la santé*. Il ne s'agit pas uniquement de traiter des données de santé (les professionnels intervenant dans le système de santé peuvent être amenés à traiter des données à caractère personnel qui sont des données sensibles mais ne sont pas nécessairement des données de santé. Cela avait notamment été souligné lors des travaux relatifs à loi de 2004 créant le dossier médical personnel (devenu dossier partagé) « *Il est très important de souligner que dans les dossiers médicaux peuvent se trouver des données dont le recueil est strictement interdit dans tous les autres cas, par exemple l'origine raciale puisqu'elle peut être une source de prédisposition à certaines maladies. L'appartenance religieuse est également importante puisqu'elle peut déterminer l'exclusion de certains aliments de l'alimentation quotidienne. A ces données, peuvent s'ajouter des renseignements sur la vie sexuelle dont l'importance s'est accrue avec la propagation du sida* » (J.-C. ETIENNE et J. DIONIS DU SEJOUR, Rapport « Les télécommunications à haut débit au service du système de santé » Assemblée nationale, n° 1686 (12ème législature) – Sénat, n° 370 (2003-2004), p. 49) mais surtout, le *domaine de la santé* se distingue a priori de la stricte prise en charge des malades.

[945] Art. 9 4° RGPD.

[946] Le modèle pour la majorité des traitements de données à caractère personnel est désormais celle de la *responsabilisation des acteurs* traduction du terme anglais *accountability*. L'article 2° 5 du RGPD relatif au principe du traitement des données, autrement dit, les conditions de licéité, prévoit que « *Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité)* ». Le terme responsabilité est traduit de l'anglais *accountability*. Des auteurs remarquent que « *L'accountability, au sens du Règlement, serait donc une situation dans laquelle l'entreprise serait capable de démontrer qu'elle agit en conformité avec les principes du Règlement.* » (W. MAXWELL et S. TAÏEB, « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles ? » *Dalloz IP/IT* 2016, p.123). Les mêmes auteurs expliquent que cette notion est issue d'une norme ISO (ISO/IEC 29100 :2011, *Information technology - Security techniques - Privacy framework*) et précisent que « *L'accountability est, selon l'ISO, une obligation de diligence (duty of care) à laquelle s'ajoute l'adoption de mesures concrètes et pratiques assurant la protection des données* » (W. MAXWELL et S. TAÏEB, « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles », *op. cit.* Le G29 propose également une définition de cette notion, comme le fait de mettre « *l'accent sur la manière*

s'agissant du traitement tant des données personnelles que des données sensibles[947] mais elles sont partiellement maintenues dans le cadre de ces finalités. Les conditions du traitement des données à caractère personnel dans le domaine de la santé, qui figurent aux articles 64 et suivant de la LIL, prévoient en effet que les traitements de données à caractère personnel dans le domaine de la santé ayant une finalité d'intérêt public[948] et plus spécifiquement, ceux ayant une finalité de recherche, d'études ou d'évaluation dans le domaine de la santé[949] sont soumises à une formalité préalable et nécessite, en principe, une autorisation de la CNIL[950]. Les conditions de mise en œuvre des traitements ayant une finalité d'intérêt public et de recherche dans le domaine de la santé sont donc plus strictes que celles prévues pour les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé, pour lesquels aucune formalité préalable n'est exigée. L'interprétation large de ces dernières finalités peut s'analyser comme un contournement des dispositions plus protectrices. Notre opinion est que ce contournement est en quelque sorte *temporisé* par la garantie apportée par le fait que les personnes traitant les données sont **originellement** soumises au secret professionnel bien que, dans les exemples du traitement des données relatives au dépistage prénatal de la trisomie 21 et du traitement des données relatives à l'homosexualité des donneurs, ni le Conseil d'Etat ni la Cour de cassation n'expliquent de manière lisible la façon dont est effectué le contrôle de proportionnalité. Au

---

dont la responsabilité (responsability) est assumée et sur la manière de le vérifier » (<https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp173_fr.pdf>, consulté le 14 oct. 2019).

[947] S'agissant du traitement des données sensibles dans le domaine de la santé les formalités préalables ne sont pas exigées lorsque la personne a donné son consentement explicite au traitement ; lorsque le traitement est nécessaire à la sauvegarde de la vie humaine ; lorsque les données sont rendues publiques par la personnes concernées ; lorsque les données sont traitées au fin de la médecine préventive ; des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mises en œuvre par un membre d'une profession de santé ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel (il s'agit des traitements relevant du 1° de l'article 44 de la loi informatique et libertés et des a et c à f du 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016).

[948] Les conditions de traitement pour des finalités d'intérêt légitime dans le domaine de la santé sont prévues aux articles 65 à 71 de la LIL.

[949] Les conditions de traitement pour ces finalités de traitement sont également prévues aux articles 65 à 71 de la LIL et répondent en outre aux dispositions spécifiques prévues aux articles 72 à 77 de la même loi.

[950] La CNIL dispose d'un pouvoir de simplification en la matière, elle peut par exemple créer des référentiels ou des méthodologies de recherche (art. 73 LIL). Lorsque le traitement est conforme à un référentiel ou à une méthodologie de recherche, le responsable du traitement où le sous-traitant devra simplement adresser une déclaration de conformité afin de pouvoir mettre en œuvre le traitement. Dans le cas contraire la procédure d'autorisation devra être suivie et s'articule autour de trois dispositions de la loi : Les articles 66, 73 et 76.

stade de l'élaboration de la loi transposant la directive de 1995 le rôle des professionnels de santé dans la protection de ces données était plus évident. Ainsi, le rapport de Monsieur Türk[951] affirmait que l'exception à l'interdiction de traitement des données sensibles pour des finalités de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé, constituait une contrepartie à l'ajout des données de santé dans la catégorie des données sensibles. Le rapport précisait ensuite que « *tout en encadrant strictement le traitement de ces données, désormais restreint à des finalités et à des destinataires étroitement définis. La limitation par* ***la directive des personnes autorisées à effectuer le traitement des données constitue une garantie essentielle*** »[952]. Cette logique a donc ensuite été étendue.

B - L'assujettissement au secret professionnel, conséquence du traitement des données

191. Soumettre au secret professionnel pour justifier le traitement de données. La participation du secret professionnel à la protection des données à caractère personnel a sans doute contribué à accélérer le mouvement de généralisation du secret professionnel[953]. Au grès des modifications les auteurs de la loi informatique et libertés, ont ainsi entendu astreindre au secret professionnel « *toute la chaîne de ceux qui les* [les données issues de la relation de soin] *manipulent »*[954]. Si les prémisses d'une telle vision figurent dans la loi de 1994 citée en amont, elle s'est confirmée au travers de la transposition de la directive européenne n° 95/46 du 3 mars 1995. Lorsque les données sensibles sont traitées pour des finalités d'intérêt public dans le domaine de la santé[955], le législateur national a ainsi prévu que « *Les personnes appelées à mettre en œuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au secret professionnel sous les peines prévues à l'article*

---

[951] A. TÜRK, *Rapport relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,* Sénat, n° 218.
[952] *Ibid.* p. 63.
[953] Sur la dilution du secret professionnel consécutive de la généralisation v. *infra* Chapitre II Titre I Partie II.
[954] A. TURK, *Rapport sur le projet de loi relatif au traitement de données nominatives ayant pour fin la recherche en vue de la protection ou l'amélioration de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, n° 209, 21 déc. 1993, p.11. Dans le rapport ce sont les données médicales qui sont visées puisqu'elles sont issues de la relation médicale, cette expression a été, depuis, abandonnée.
[955] Art. 9 II i) du RGPD et 68 de la LIL.

226-13 du code pénal »[956]. La soumission au secret professionnel intervient, dans ce contexte, non pas comme une condition au traitement mais comme une conséquence de la réutilisation des données initialement collectées et traitées dans le contexte de la prise en charge médicale et médico-sociale des individus.

192. L'amorce d'un mouvement de généralisation du secret professionnel. La soumission au secret professionnel comme conséquence du traitement de ces données ne tient aucun compte du fait que le traitement des données à des fins d'intérêt public peut s'effectuer par le biais d'un accès au système national des données de santé et concerne donc des personnes qui ont accès à des données pseudonymisées[957]. Les dispositions relatives au système national des données de santé disposent également : « *Les personnes responsables de ces traitements, ainsi que celles les mettant en œuvre ou autorisées à accéder aux données à caractère personnel qui en sont issues, sont soumises au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pénal* »[958]. Il s'agit, par ces quelques remarques, de commencer à tracer les linéaments d'un mouvement de généralisation du secret professionnel lié au traitement des données à caractère personnel dans le domaine de la santé. Nous nous appliquerons à décrire ce mouvement dans la suite de nos développements.

193. Conclusion du premier chapitre. Le champ d'application matériel des dispositions relatives à la protection des données personnelles a pour point nodal, pour critère principal, la nature des données traitées. Les informations couvertes par le secret professionnel peuvent, par ailleurs, faire l'objet d'un traitement, à l'instar de toutes informations. Ainsi, la nature de ces données devrait déterminer l'application des dispositions relatives à la protection des données personnelles sans les distinguer d'autres données de même nature. Ces dispositions recèlent, toutefois, des spécificités tenant non plus à la nature des données mais à leur source. Si les données étaient protégées en raison de leur nature, leur régime de protection répondrait aux mêmes mécanismes que toutes les autres données sensibles, dès lors qu'elles relèvent de la vie privée. En d'autres termes, la nature des informations réservées ne les distingue pas des autres informations personnelles et, *a fortiori*, des autres données personnelles, sensibles ou non. Le critère de distinction – qui va permettre l'application d'un régime spécifique – tient au contexte

[956] Art. 68 de la LIL.
[957]CSP, art. L.1461-1. Cet article n'a pas subi de modification suite à l'entrée en vigueur de la Loi n° 2019-774 du 24 juillet 2019, *préc.*
[958] CSP, art. L. 1461-1-IV-2°.

dans lequel les informations et les données sont collectées et traitées. Il s'agira de maintenir l'état de secret tout en favorisant le traitement des données pour les besoins du système de santé.

Chapitre 2 - La circulation des données couvertes par le secret

194. Parmi les opérations de traitement, certaines consistent en une action de communication des données, il s'agit de les faire circuler. Les dispositions relatives à protection des données prévoient un mécanisme spécifique fixant les critères selon lesquels les données devraient circuler, tandis que le secret professionnel a précisément pour fonction d'empêcher la communication et la circulation des informations à caractère secret. Afin d'évaluer la protection offerte au « secret médical » – compris comme l'état de secret –, il convient de mettre en lumière les rapports entre le secret professionnel et la confidentialité **(Section 1)** avant de les étudier au regard de la doctrine de la CNIL **(Section 2)**.

Section 1 - Dévoilement des rapports entre confidentialité et secret professionnel

195. Au titre des obligations qui incombent au responsable du traitement et désormais au sous-traitant, la loi informatique et libertés et le règlement européen relatif à la protection des données à caractère personnel font une place essentielle à celle imposant de mettre en œuvre les mesures de sécurité adaptées aux particularités du traitement qu'ils mettent en œuvre. Si la *mise en œuvre* des obligations – au travers des logiques de *compliance* et d'*accountability* – guide désormais la protection des données et constitue la véritable innovation du RGPD notre approche de l'obligation de sécurité est essentiellement substantielle[959]. Sous cet angle il convient de remarquer que cette obligation consiste notamment à garantir la confidentialité des données traitées **(paragraphe 1)**. L'étude de l'infraction sanctionnant la violation de confidentialité des données permet de mettre en exergue le rapport étroit entre la *confidentialité* et le secret professionnel **(paragraphe 2)**.

§ 1 - Le maintien de la confidentialité, corrolaire de l'obligation de garantir la sécurité des traitements

196. L'obligation de sécurité qui incombe au responsable du traitement des données et au sous-traitant consiste dans une protection générale des traitements **(A)** elle conditionnel le respect de l'obligation de confidentialité des traitements **(B)**.

---

[959] Sur ces notions et la mise en œuvre de la sécurité et de la confidentialité v. *infra* titre II Partie II.

A - Garantir la sécurité, protection générale des traitements

197. De la sécurité. De la sécurité de l'information à l'obligation de sécurité des traitements. La sécurité, dans le sens commun, est définie comme un « *état d'esprit confiant et tranquille qui résulte du sentiment, bien ou mal fondé, que l'on est à l'abri de tout danger* »[960] ou dans une seconde acception comme une « *situation objective, reposant sur des conditions matérielles, économiques, politiques, qui entraîne l'absence de dangers pour les personnes ou de menaces pour les biens et qui détermine la confiance* »[961]. La sécurité[962] tient une place centrale dans la « *société du risque* »[963]. En droit[964] la question de la sécurité innerve tous les domaines[965] au point que la doctrine se pose la question de savoir s'il existe un droit subjectif

---

[960] TLFi, *op. cit.*, V° « sécurité ».
[961] *Ibid.*
[962] Proposant une étude philosophique, historique et politique de la notion de sécurité : F. GROS, *Le principe sécurité*, coll. NRF Essais, Gallimard, 2012
[963] Pour une étude sociologique : U. BECK, *La société du risque. Sur la voie d'une autre modernité*, Flammarion, 2008 ; Pour une approche anthropologique : J. MERIC, Y. PESQUEUX et A. SOLE, *La « Société du risque : analyse et critique »*, Economica, 2009 ; Sur la gouvernance des risques : O. GODARD, C. HENRY, P. LAGADEC et E. MICHEL-KERJAN, *Traité des nouveaux risques*, Folio, Gallimard, 2002 ; v. Egalement des propos généraux sur le risque en droit : C. NOIVILLE, *Du bon gouvernement des risques. Le droit et la question du risque acceptable*, Les voies du droit, PUF, 2003.
[964] La sécurité *du droit* c'est-à-dire la sécurité juridique en est un exemple édifiant. Le sujet est tentaculaire et la doctrine ne cesse de discuter la question (pour une approche complète de la notion et une synthèse éclairante des conceptions doctrinales v. J. VAN MEERBEECK, *De la certitude à la confiance. Le principe de sécurité juridique dans la jurisprudence de la Cour de justice de l'Union européenne*, Publication USLB, Anthémis, 2014, spéc. Introduction) d'autant qu'elle émet des propositions (v. par exemple le rapport public du *club des juristes* présidé par N. MOLFESSIS et H. DE CASTRIES, intitulé « sécurité juridique et initiative économique » dans lequel les chercheurs formulent 63 proportions pour lutter contre l'insécurité juridique). Il est impossible de reproduire dans cette note l'intégralité de bibliographie sur le sujet de la sécurité juridique tant générale que particulière et cela n'aurait aucun sens. Au regard de la masse des écrits de doctrine, des occurrences de la notion dans la jurisprudence et la législation une telle entreprise serait, en plus, vouée à l'échec. La question de la sécurité juridique est autant une question philosophique que théorique, pour en tirer l'essence et la bibliographie il nous semble que c'est encore vers la thèse de Jérémy VAN MEERBEECK qu'il faut se tourner (J. VAN MEERBEECK, *De la certitude à la confiance. Le principe de sécurité juridique dans la jurisprudence de la Cour de justice de l'Union européenne*, *op. cit.*), ainsi que vers celle de T. PIAZZON (T. PIAZZON, *La sécurité juridique*, coll. Doctorat & Notariat, Defrénois, t. 35, 2009). Un rapport du Conseil d'Etat a également été publié que le sujet en 2006 (CE, Rapport public 2006, *Sécurité juridique et complexité du droit*, coll. Etudes et documents, n° 57, La documentation Française). Enfin, les nombreux travaux de N. MOLFESSIS dont, entre autres : N. MOLFESSIS, « Les illusions de la codification à droit constant et la sécurité juridique », *RTD civ.*, 2000, p. 186 ; « La sécurité juridique et la jurisprudence vue par elle-même », *RTD civ.* 2000, p. 666 ; « La sécurité juridique et la fonction normative de la loi », *RTD civ*., 2000, p. 670 ; « Les « avancées» de la sécurité juridique», *RTD civ.*, 2000 p. 660.
[965] Pour ne citer que quelques exemples, le principe de précaution comme outil de sécurité irrigue la responsabilité tant civile que pénale (L'influence *du principe de précaution sur le droit de la responsabilité civile et pénale comparé* Rapport pour la Mission de recherche Droit et Justice, Septembre 2016, M. HAUTERAU-BOUTENNET et J.-C. SAINT-PAU (ss. la dir.)). A propos de l'expertise comme source de sécurité juridique V. LASSERRE formule un constat qui nous paraît décrire avec justesse la place de la sécurité dans la société, sécurité aussi attendue en droit que du droit lui-même : « […] *depuis la Seconde Guerre mondiale, la sécurité s'est peu à peu imposée comme une valeur fondamentale des sociétés industrielles par la rencontre de deux phénomènes,*

à la sécurité[966]. Notion universelle, la sécurité entretient des liens d'interdépendance avec la notion de risque. La sécurité de l'information appartient au domaine des spécialistes en informatique. Les normes juridiques garantissant la réservation de l'information constituent des techniques de protection des personnes et des biens : l'on parle alors de protection de l'information et non de sécurité. La sécurité de l'information est de l'ordre du fait : la pratique du cachetage des lettres constituait une forme très archaïque de sécurité de l'information, de même le fait de placer une enveloppe dans un coffre-fort relève également d'une forme de sécurité de l'information. A partir de la Seconde Guerre mondiale, l'informatique va développer ses propres méthodes et ses propres normes de sécurité de l'information. La sécurité de l'information se distinguera ensuite de la sécurité des systèmes d'information. Il s'agit *a priori* du domaine de la technique informatique[967]. Un néologisme, formé sur la racine grecque *cyber*[968] désigne le contrôle de la sécurité : Cybersécurité[969].

A ce stade de notre raisonnement il s'agit d'analyser l'obligation de sécurité telle que définie par les dispositions relatives à la protection des données à caractère personnel afin d'en saisir le contenu. Le terme de sécurité figure dans la loi informatique et libertés depuis 1978. L'article 29 de la loi prévoyait ainsi que « *Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment*

---

antinomiques. D'un côté, les avancées de la science ont fini par imposer l'idée que la science est omnipotente, ce qui rend inacceptables les champs incertains et les erreurs. De l'autre, la société de l'innovation, que l'Europe à reconnue dans sa stratégie de Lisbonne et dont la nécessité est rappelée chaque jour par la crise des industries européennes, est par définition une société du risque » (V. LASSERRE, *Le nouvel ordre juridique. Le droit de la gouvernance.* LexisNexis, 2015, n° 46). Enfin et surtout le droit de la responsabilité dont le fondement a évolué de la faute (responsabilité subjective) vers le risque (responsabilité objective), pour une synthèse de ces transformations v. J. ROCHFELD, *Les grandes notions du droit privé*, 2011, V° « Responsabilité », n° 6.8 et svt.

[966] V. par exemple P. JOURDAIN « Existe-t-il un droit subjectif à la sécurité ? », *in* M. NICOD (ss. la dir.), *Qu'en est-il de la sécurité des personnes et des biens ?*, *op. cit.*, p. 77; G. RIPERT, *Les forces créatrices du droit*, LGDJ, 2ème éd., 1955, n° 118 ; J. MESTRE (ss. la dir.), *Le droit face à l'exigence contemporaine de sécurité*, PUAM, 2000.

[967] L'évolution des techniques a nécessité une gestion globale de la sécurité de l'information. Elle n'est plus seulement technique mais également organisationnelle. Ce qui implique qu'elle répond non seulement à des normes techniques mais aussi à des normes managériales.

[968] Le mot *cyber* est issu du grec «κυβερνάω» qui signifie gouverner, diriger (A. BAILLY, Dictionnaire Grec - Français, Hachette, 1935, v° «κυβερνάω»). Le terme a été utilisé par N. WIENER pour former le mot *cybernetics*, objet de son premier ouvrage qu'il consacre à la maîtrise de la machine (N. WIENERT, *Cybernetics : Control and Communication in the Animal and the Machine*, Hermann, 1948).

[969] V. *infra* n° 409.

d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés ». L'effectivité de la sécurité des informations était alors contrôlée par la CNIL à l'occasion des formalités préalables[970], et celle-ci avait par ailleurs le pouvoir de prendre des mesures pour garantir la sécurité des traitements d'informations[971].

198. L'obligation de sécurité des traitements depuis l'entrée en vigueur du RGPD. La spécificité de l'obligation de sécurité des traitements consiste dans son caractère préventif. Cette particularité des mécanismes juridiques de protection était déjà remarquable dans de la loi informatique et libertés dès l'origine et permettait à Monsieur Ancel de souligner : « *En droit commun, la protection de la personnalité passe surtout par la sanction des atteintes une fois qu'elles se sont produites. La loi de 1978 n'ignore pas ce point de vue : mais, parce qu'on a affaire à des atteintes difficiles à déceler, donc à sanctionner, elle organise aussi — et surtout — un système de prévention des atteintes éventuelles* »[972]. Tandis que le système de prévention s'est longtemps caractérisé par le choix d'une régulation *ex ante*[973], l'entrée en vigueur a emporté un changement majeur sur ce plan puisque le système est désormais guidé par une logique de *compliance*[974]. Depuis l'entrée en vigueur du RGPD l'approche préventive s'illustre

---

[970] Art. 19 de la loi informatique et libertés dans sa première version (Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) puis article 34 suite à la transposition de la directive de 95/46/CE (Loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

[971] Art. 21 3° de la LIL dans sa première version (*Ibid.*).

[972] P. ANCEL, « La protection des données personnelles. Aspects de droit privé français », *RIDC* 1987-3, *spéc*. p. 614.

[973] Le choix du législateur national a ensuite été affermi par la directive européenne de 1995 consistant dans une approche régulatoire caractérisée par l'intervention de la CNIL, autorité administrative indépendante, qui procédait à l'examen des traitements *avant leur mise en œuvre*. Envisagé sous cet angle « *Le recours à une autorité administrative s'explique par la plus grande capacité des autorités administratives, par opposition au juge judiciaire, à remplir une mission de prévention* » (E. BREEN, « La « compliance », une privatisation de la régulation ? », *RSC* 2019, p. 327).

[974] A ce stade de notre étude il convient simplement de signaler que la *compliance* n'est pas un mode de régulation auquel le juriste français est habitué, le modèle ayant été importé des Etats-Unis. La *compliance* peut se définir, pour l'essentiel, comme « *la capacité d'une entreprise d'agir en conformité avec la loi et avec ses réglementations internes dans toutes les juridictions où elle exerce une activité. Elle désigne donc avant tout un ensemble de processus d'entreprise visant à détecter, à sanctionner, mais encore à prévenir les infractions qui pourraient être commises en leur sein* » (*Ibid.*). Il s'agit donc pour les responsables de traitement et les sous-traitants de se *mettre en conformité* (bien que le terme de conformité soit une traduction malheureuse du terme anglais) avec le RGPD. A ce titre K. FAVRO affirme : « *la compliance qui suppose que l'on se débarrasse progressivement des contraintes extérieures pour faire prévaloir l'éthique* » et encore « *La conformité et sa démonstration permettent d'affirmer de toute part l'attachement à la protection des données personnelles, en octroyant une efficience que la seule applicabilité de la norme peinait à garantir* » (K. FAVRO, «La démarche de compliance ou la mise en œuvre d'une approche inversée », *Légicom*, 2017/2, n°59, pp. 21 à 28). Sur les conséquences de la *compliance* sur

notamment par le renforcement de l'obligation de sécurité des traitements de données consacrée[975]. Or, cette obligation n'a pas pour seule fonction de protéger la personnalité. La lecture conjointe de l'article 32 du RGPD et du considérant 49 du règlement européen en éclaire le contenu. La sécurité des traitements doit en effet permettre d'assurer la disponibilité, l'authenticité, l'intégrité et la confidentialité des données traitées[976]. La perte, l'altération des données ou leur indisponibilité peut engendrer un préjudice pour les personnes concernées par le traitement. Une illustration tout à fait explicite peut-être trouvée dans le domaine de la santé : l'indisponibilité des données contenues dans un dossier médical électronique du fait d'un défaut de sécurité du système d'information supportant le traitement peut engendrer un retard de prise en charge dont les conséquences peuvent être plus ou moins importantes en fonction des individus. En assurant la sécurité des traitements, le responsable du traitement et le sous-traitant veillent également à ce que des tiers non-autorisés n'aient pas accès aux données[977]. Il s'agit d'une définition négative de la *confidentialité*. Assurer la confidentialité des données consiste en effet à ne permettre l'accès aux données qu'aux seules personnes autorisées. Avant d'envisager ce que recouvre la notion de confidentialité il convient d'évoquer la nature de l'obligation.

199. Une obligation de moyen ? L'obligation qui pèse sur les responsables de traitement et les sous-traitants ne correspond pas à la définition traditionnelle de l'obligation, fondement de la responsabilité civile. Une brève comparaison entre ce que l'on nomme obligation de sécurité dans les dispositions de la loi informatique et libertés et l'obligation civile suffit à s'en convaincre.

---

le choix des outils de régulation pour le maintien du secret des données à caractère personnel dans le domaine de la santé.

[975] Evoquant les obligations préexistantes (licéité des traitements, proportionnalité, loyauté et transparence) Monsieur Poullet précise : « Le principe de sécurité s'y est ajouté, comme une préoccupation nettement renforcée » (Y. POULLET, *La vie privée à l'heure de la société du numérique*, coll. Essai, Larcier, 2019, p. 115). Plus que l'existence d'une telle obligation, la règle de *l'accountability* est le point d'ancrage de l'esprit de prévention qui guide le RGPD puisqu'il s'agit, pour le responsable de traitement et le sous-traitant, d'être en mesure de faire la démonstration, si cela lui est demandé, de ce qu'il a effectivement mis en œuvre les mesures nécessaires, en fonction des risques présentés par le traitement pour les droits et libertés des personnes concernées (Consid. 74 du RGPD).

[976] Consid. 49 RGPD.

[977] Art. 32 paragraphe 2 du RGPD.

L'obligation de sécurité figurant dans le RGPD est généralement qualifiée d'obligation de moyen renforcée[978]. Si tel était le cas cette obligation devrait remplir certains critères propres à cette qualification juridique. L'exemple historique de l'obligation de moyen est celui de l'activité médicale[979]. La responsabilité du médecin est fondée sur la faute[980]. Débiteur d'une obligation de moyen[981] dont le patient est créancier, il doit réparer les dommages éprouvés par le patient en raison de cette faute. La faute est appréciée *in concreto* au regard, notamment, des données acquises de la science[982]. Selon la formule de l'article L. 1110-5 du Code de la santé publique, toute personne a « *le droit de recevoir, sur l'ensemble du territoire, les traitements et les soins les plus appropriés et de bénéficier des thérapeutiques dont l'efficacité est reconnue et qui garantissent la meilleure sécurité sanitaire* »[983]. La mention des « *soins appropriés* » renvoie à l'obligation de moyen. Il ne s'agit pas d'exiger un résultat, la guérison, mais de prodiguer des soins les plus efficaces au regard des données acquises de la science. Cette formulation fait écho à celle de l'article 34 du RGPD qui prévoit que « *le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles*

---

978 En ce sens v. C. CASTET-RENARD, *Rep. eur.*, V° « La protection des données personnelles dans les relations internes à l'Union européenne », 2018, n° 65 à 67 ; A. DEBET, J. MASSOT, N. METTALINOS, *Informatique et libertés*, *op. cit.*, n° 1337 ; R. PERRAY, *Jcl. comm.*, Fasc. 940, « Données à caractère personnel. – obligations des personnes mettant en œuvre des traitements de données à caractère personnel et droits des personnes concernées », n° 54 à 72.

979 Depuis l'arrêt *Mercier* du 20 mai 1936 (Civ., 20 mai 1936, *DP* 1936, 1, p. 88, concl. P. MATTER, rapp. L. JOSSERAND ; *S.* 1937, 1, p. 321, note A. BRETON. – M. HARICHAUX, « L'obligation du médecin de respecter les données de la science, À propos du cinquantenaire de l'arrêt Mercier : bilan d'une jurisprudence », *JCP G* 1987, I, 3306).

980 Bien qu'il existe des hypothèses de responsabilité sans faute pour les dommages causés par les produits de santé, les infections nosocomiales et l'aléa thérapeutique (S. PORCHY-SIMON, *Jcl. civil code*, Art. 1382 à 1386 - Fasc. 440-20 : Santé. – Responsabilité médicale. – Principes généraux, 2011, (mise à jour mai 2018), n° 37).

981 R. DEMOGUE, *Traité des obligations en général*, Rousseau, t. V, n° 1237, et tome IV n° 180 à 182) entre le médecin et son patient est désormais considérée, bien que la question soit encore discutée, comme une obligation légale ou statutaire (Pour un état des questions, une bibliographie non exhaustive : P. MALAURIE, « La responsabilité civile médicale », *Defrenois*, 2002, 37632, n°17 Comp., un peu plus nuancé, M. GIRER, *Contribution à une analyse rénovée de la relation de soins : Essai de remise en cause du contrat médical*, ss la dir. de F. Vialla, thèse de doct., version numérique 2010, coll. Thèses, LEH, t. 18. Comp. E. RASCHEL, *La pénalisation des atteintes au consentement dans le champ contractuel*, préf. R.-N. SCHÜTZ, M. DANTI-JUAN coll. Thèses, Faculté de droit et des sciences sociales de Poitiers, 2014, n°20. F. DREIFUSS-NETTER, «Feue la responsabilité civile contractuelle du médecin? », *RCA*, oct. 2002, chron., 17, p. 6. Comp. P. Lokiec, « La décision médicale », *RTD civ.*, 2004. A. LAUDE, B. MATHIEU et D. TABUTEAU, Droit de la santé, 3ème éd., PUF, 2012, pp. 435-436, n°383 ; A la marge de ces analyses mais étudiant les catégorie du contrat et de l'acte juridique au travers de l'analyse de la relation médicale v. B. MORON-PUECH, *Contrat ou acte juridique? Étude à partir de la relation médicale*, th. ss. la dir. de D. FENOUILLET, soutenue le 4 avril 2016, Université Panthéon-Assas, (édité sur HAL le 13 nov. 2018).

982 S. PORCHY-SIMON, *Jcl. civil code*, *op. cit.*, n° 44.

983 Art. 1110-5 CSP.

appropriées afin de garantir un niveau de sécurité adapté au risque »[984]. Le régime de l'obligation de sécurité n'est pas celui d'une obligation de moyen, ni même d'une obligation au sens civil du terme. La différence tient d' abord au fait que la CNIL peut prononcer des sanctions sans considération de l'existence d'un dommage lié à une faute. La Commission ne recherche donc pas les éléments traditionnels de la responsabilité[985]. Le terme d'obligation devrait alors être compris *largo sensu*, comme norme *impérative*[986], obligation légale. Ensuite moyen et résultat se confondent, comme le relève Madame Frison-Roche à propos de l'obligation d'avoir des données exactes et complètes[987] : « Prendre des mesures appropriées « *n'engendre pas qu'une obligation de* « faire au mieux ». *Le régulateur* « retourne le texte comme un gant » *: prendre des mesures pour rectifier des données se révélant inexactes est interprété comme l'obligation objective d'avoir en permanence des données exactes et complètes* »[988]. Ainsi, l'obligation de sécurité a longtemps été contrôlée *a priori* par la CNIL,

---

[984] Art. 34 du RGPD et article 34 de la loi informatique et libertés (le qualificatif « approprié » est remplacé par « utiles » dans le texte de la LIL, cette formulation est issue de l'ancienne rédaction de la LIL mais les travaux préparatoires reprennent le qualificatif employé par le RGPD : « ils [les responsables de traitement et les sous-traitants] ont l'obligation de mettre en place des mesures de protection des données appropriées [en fonction du risque pour la vie privée des personnes]» (S. JOISSANS, *Rapport au Sénat*, *op.cit.*, p. 16).

[985] En ce sens « La CNIL considère que les moyens mis en œuvre doivent être efficaces et que la responsabilité de l'organisme de traitement est encourue du simple constat de l'inefficacité des mesures, sans considération de la faute » (A. DEBET, J. MASSOT, N. METTALINOS, *Informatique et libertés*, op. cit., n° 1228). En ce sens notamment v. CNIL, délib. n° 2014-238, 12 juin 2014. – CNIL, Fuite de données clients : avertissement pour DHL, 19 juin 2014. Dans cette délibération la CNIL précise que « *plusieurs centaines de milliers de fiches comportant des données à caractère personnel relatives aux clients de la société étaient indexées et librement consultables sur internet sans manipulation technique particulière* ».

[986] La vocation instrumentale de la norme, comme l'a expliqué P. AMSELEK est d'indiquer « *une mesure du possible* » (P. AMSELEK, *Cheminements philosophiques dans le monde du droit et des règles en général*, coll. Le temps des idées, Armand Colin, 2012, p.87 et svt., spéc. p.88) de la survenance des choses. L'auteur propose une gradation des marges de possibilité offertes par la règle : « *ce qui doit se produire, c'est ce qui ne peut pas ne pas se produire* » (*Ibid.* p. 88) ; « *ce qui ne peut pas se produire, c'est ce qui doit ne pas se produire* » (*Ibid.*) et enfin « *ce qui peut se produire, c'est ce qui peut ne pas se produire* » (*Ibidem*). La première modalité correspond à l'obligation.

[987] Obligation générale également, inscrite au titre des *principes* du RGPD (art. 5).

[988] M.-A. FRISON-ROCHE, « Les droits des personnes, Internet et la CNIL », *Dalloz - Etudiants*, 7 juillet 2016. Sans aller jusqu'à une affirmation aussi ferme A. DEBET relève que l'application des notions d'obligation de moyens ou de résultat n'était pas très claire : « *L'affirmation selon laquelle l'obligation de sécurité est une obligation de moyens montre seulement que la CNIL est consciente qu'elle ne peut pas exiger des responsables de traitement une infaillibilité informatique impossible à atteindre, pour le reste – et les responsables de traitement ne doivent pas s'y méprendre – ses exigences sont très fortes et elle sait toujours trouver des choses à leur reprocher !* » (A. DEBET, « Le responsable de traitement est tenu d'une obligation de résultat s'agissant de l'exactitude des données », *Com. comm. électr.* 2016, n°5, comm. 44).
L'affirmation selon laquelle l'obligation de sécurité est une obligation de moyens montre seulement que la CNIL est consciente qu'elle ne peut pas exiger des responsables de traitement une infaillibilité informatique impossible

ce qui distingue aussi l'objectif de sécurité posé par le RGPD du devoir de protéger les informations par la déontologie des professionnels de santé[989]. Ce que confirme encore l'identité des débiteurs de l'obligation de sécurité des traitements.

200. Les débiteurs de l'obligation de sécurité. Dans les premiers considérants du règlement, exprimant la *ratio legis*, le législateur européen justifie notamment son intervention[990] par la généralisation du traitement des données à caractère personnel : « *l 'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante* »[991]. Il est ainsi apparu nécessaire de garantir aux individus qui autorisaient le traitement de leurs données personnelles que seuls les individus auxquels ils avaient donné cette autorisation pouvaient effectivement les traiter, le traitement, consistant, au regard de la définition des opérations de traitement, aussi bien dans le fait de prendre connaissance des données que dans le fait de les stocker, de les utiliser ou de les diffuser. Jusqu'à l'entrée en vigueur du RGPD le droit national prévoyait que cette obligation incombait uniquement au responsable du traitement[992]. Depuis l'entrée en vigueur du RGPD le sous-traitant[993] est tenu à la même obligation tandis qu'il bénéficiait, sous l'empire de l'ancienne version de la loi informatique et libertés, d'une forme « *d'immunité* »[994]. Il faut noter que les conditions de la

---

à atteindre, pour le reste – et les responsables de traitement ne doivent pas s'y méprendre – ses exigences sont très fortes et elle sait toujours trouver des choses à leur reprocher !

[989] V. *supra* n°59.

[990] Sur la portée variable des considérants v. S. LEMAIRE, « Interrogations sur la portée juridique du préambule du règlement Rome I », *D.* 2008, p. 2157.

[991] Consid. 6 du RGPD.

[992] Selon la définition posée à l'article 4 7) du RGPD, le responsable de traitement est « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre* ».

[993] Le sous-traitant est défini à l'article 4 8) du RGPD comme : « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ». Dans le domaine de la santé l'exemple le plus évident est celui des hébergeurs de données de santé mais cela peut également concerner toutes structures ou entreprises avec lesquelles le responsable du traitement est lié par contrat aux fins de traiter les données telle qu'une société de maintenance informatique ou une entreprise spécialisée dans l'analyse des données.

[994] A. DEBET, J. MASSOT, N. METTALINOS, *Informatique et libertés*, coll. Les intégrales, Lextenso, 2015, n° 1337. V. notamment la décision TGI de Marseille, 6ème ch. corr., jugement du 7 juin 2017 dans laquelle le sous-traitant avait été relaxé du fait de manquement à l'obligation de sécurité sanctionné à l'article 226-17 du Code pénal pour ne pas avoir pris « *toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés, en l'espèce en créant un portail de saisie de données informatisées de santé concernant des enfants et des femmes hospitalisés dans l'unité de néonatalogie de l'hôpital Nord de l'AP-HM dans le cadre d'une prestation relative à*

sous-traitance doivent être régies par un contrat ou un autre instrument juridique[995] entre le responsable du traitement et le sous-traitant. L'article définissant les obligations du responsable du traitement précise que celui-ci doit choisir un sous-traitant qui présente des garanties suffisantes au regard des mesures de sécurité techniques et organisationnelles relatives aux traitements à effectuer et qui doit veiller au respect de ces mesures[996]. Le contrat liant le responsable du traitement et le sous-traitant doit en outre, prévoir une clause de confidentialité lorsque le sous-traitant n'est pas soumis à une « *obligation légale de confidentialité* »[997]. Cette remarque nous permet de souligner que la *confidentialité* ne recouvre pas la même signification selon le contexte. Ce n'est pas l'obligation légale de confidentialité ou le devoir de confidentialité comme mécanisme de protection des supports de l'information, qui sont ici visés. La clause de confidentialité est la source d'une obligation contractuelle[998] tandis que l'obligation légale à laquelle il est fait référence nous semble renvoyer au secret professionnel dans la mesure où *confidentialité* et *secret* sont souvent employés comme synonymes. La confidentialité corollaire de l'obligation de sécurité recouvre une définition encore différente.

B - La sécurité condition de la confidentialité

201. La sécurité et la confidentialité forme un « couple » **(1)** dont le respect le respect est contrôlé et sanctionné **(2)**.

---

un projet de réseau de santé pour des enfants nés prématurés, sans s'assurer de la sécurisation de ce portail », il est également relaxé du chef de divulgation commise par imprudence ou négligence des données à un tiers n'ayant pas les qualités pour les recevoir prévu à l'article 226-22 du Code pénal. Dans cette affaire le sous-traitant n'avait pas pris les précautions utiles et les données de santé relatives à des patients soignés dans un établissement public de Marseille avaient été divulguées sur internet ; c'est pourtant le responsable du traitement, un pédiatre, qui avait été condamné pour les faits reprochés.

[995] Selon les termes de l'article 27 du RGPD.

[996] Art. 28 §1 RGPD.

[997] *Ibid.* §3 b).

[998] L'obligation de confidentialité d'origine contractuelle constitue une obligation de se taire et donc une obligation de secret. v. C. CASEAU-ROCHE, « La clause de confidentialité », *AJCA* 2014, p. 119 ; O. LECLERC, « Sur la validité des clauses de confidentialité en droit du travail », *Dr. soc.* 2005, p. 173 ; « *Les clauses de confidentialité ont cet objet d'interdire contractuellement au débiteur de communiquer à des tiers certaines informations qui lui sont transmises, qu'elles soient commerciales, financières, stratégiques ou technologiques* » (A.-S. LUCAS-PUGET, « L'opportunité des clauses de confidentialité aujourd'hui, et demain ? », *LPA*, 14 nov. 2016, n° 119, v2, p. 50).

1 - Le couple sécurité/confidentialité

202. Contour de l'obligation de sécurité. En quoi consiste *l'obligation* de sécurité et quel est son rapport avec la confidentialité ? D'abord l'article 32 du RGPD consacrant l'obligation de sécurité précise qu'il s'agit, pour le responsable de traitement ou le sous-traitant, de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Les moyens visés doivent permettre « *de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* »[999]. De plus, l'appréciation du niveau de sécurité adapté doit prendre en compte les « *risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite* »[1000]. La sécurité apparaît donc comme le *moyen* de garantir la confidentialité, la première conditionnant la seconde. La confidentialité est donc, en quelque sorte, subsumée sous l'obligation générale de sécurité.

203. Ce que recouvre la notion de confidentialité. La confidentialité est traditionnellement rattachée à l'article 9 de Code civil en ce qu'elle constituerait un « droit-moyen » qui concourt à un « droit-fin »[1001]. Pourtant tout manquement à l'obligation de confidentialité des données n'entraine pas nécessairement une atteinte à la vie privée et, comme l'explique Madame Rochfeld : « *La* « charte des droits fondamentaux » *de l'Union Européenne, dans son article 8, protège d'ailleurs les données comme un droit fondamental, dissocié de la vie privée, mais lié à la personne* »[1002]. Quand bien même l'on adhérerait à l'idée selon laquelle l'article 9 du Code civil est la matrice des droits de la personnalité, un certain nombre d'objections viennent contredire cette position[1003]. Il n'est toutefois pas besoin de régler les questions de classification

---

[999] Art. 32 §1 b) RGPD.
[1000] *Ibid.* §2.
[1001] M. BENEJAT, « Les droits sur les données personnelles », *in* J.-C. SAINT-PAU (ss. la dir.), *Droits de la personnalité*, *op.cit.*, n° 940.
[1002] Entretient avec J. ROCHFELD, « Des données personnelles : Quels nouveaux droits ? », *Statistiques et Société*, Vol. 5, n° 1, 2017, p. 49.
[1003] Evoquant l'existence de normes formelles autonomes et de grandes différences de régimes tenant principalement à ce que la logique qui guide la protection des données n'est pas d'empêcher toute intrusion dans la vie privée des personnes mais d'organiser « *l'après-révélation, l'après-intrusion* » en reconnaissant des droits spécifiques aux individus (droit à l'oubli, droits d'accès, droit de rectification, droits à la portabilité) : M. BENEJAT, « Les droits sur les données personnelles », in J.-C. SAINT-PAU (ss. la dir.), *Droits de la personnalité*, op.cit., n° 940.

ou de lui trouver un fondement théorique pour en déterminer les contours. En acceptant, lorsque le traitement y est conditionné, que ces données à caractère personnel ou sensibles soit traitées, la personne concernée a accepté qu'un tiers utilise des éléments de sa personnalité[1004]. Dès lors, elle doit être en mesure de s'assurer qu'elles ne seront pas traitées par d'autres que ceux à qui elle a donné son consentement[1005]. L'accès étant une opération de traitement, l'on comprend qu'il s'agit de s'assurer que les données ne seront accessibles qu'aux personnes autorisées. Toute la question réside donc dans le fait de savoir ce que recouvre l'expression « *personnes autorisées* ». L'on perçoit immédiatement que le consentement doit être au centre du dispositif, ne seraient alors des personnes autorisées que celles auxquelles la personne concernée par les données a donné autorisation d'y accéder. La situation est plus complexe qu'il n'y parait et nous y reviendrons. Avant cela il nous faut encore évoquer le contrôle du respect de l'obligation de sécurité et donc du maintien de la confidentialité et les sanctions attachées à son manquement.

2 - Contrôle et sanctions du non-respect de l'obligation de sécurité

204. Contrôle de la CNIL. Le passage de la *régulation* à la *compliance* effectué par le Règlement n'est pas complet[1006] puisque la CNIL effectue encore, quoique de manière réduite,

---

[1004] En ce sens v. J. ROCHFELD, « Quelle politique européenne en matière de données personnelles ? », *op. cit.*, p. 15.

[1005] Pèse également sur le responsable de traitement et le sous-traitant, une obligation d'information, qui existe même lorsque le consentement n'est pas exigé comme c'est le cas pour le traitement des données à des fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal (art. 44 1° LIL) et les données à caractère personnel traitése dans le domaine de la santé pour une finalité d'intérêt public (section III, chapitre III, titre II de la LIL ; ancien chapitre IX). Cette obligation d'information impose – que les données aient été directement collectées auprès de la personne concernée ou non – que le responsable du traitement informe la personne des destinataires ou des catégories de destinataires des données collectées. Dans le domaine de la santé ce sont les acteurs du système de santé qui vont informer les personnes pour le compte du responsable de traitement qui peut-être une personne morale tel qu'un établissement de soins, une clinique, un laboratoire…etc.

[1006] Le RGPD organise davantage « *une forme de co-régulation entre les responsables de traitement et les autorités, consistant en la mise en place de programmes de conformité à l'intérieur des entreprises et de la supervision de ces mesures par les autorités de l'État* » (W. MAXWELL et S.TAÏEB, « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP/IT* 2016, p. 123 ; dans le même sens : « le Règlement renforce la co-régulation entre la CNIL et les responsables de traitement des données s'inscrivant dans le cadre du principe d'accountability » (K. FAVRO, « La démarche de compliance ou la mise en œuvre d'une approche inversée », *Legicom* 2017/2, n° 59, pp. 21 à 28).

un contrôle *en amont* du respect de ces obligations par le responsable de traitement. Cette fonction de contrôle de la CNIL s'analyse dans un ensemble plus vaste de transformations successives de l'action de l'Etat et de conception de l'Etat lui-même. Tandis que dans une conception classique l'Etat, par la règlementation, encadre les comportements en imposant une législation contraignante, l'*Etat régulateur* décrit « *une conception arbitrale du rôle de l'État* »[1007]. Ce rôle d'arbitre, qu'il tient d'abord dans la sphère économique, s'est ensuite étendu à d'autres secteurs qui ne constituaient pas, à l'origine, des marchés. Il en est ainsi du traitement des données à caractère personnel où la régulation tant à opérer un compromis entre progrès technique et libertés et droits des individus. Ce rôle d'arbitre, dans les secteurs régulés, est assuré par l'intermédiaire des autorités administratives indépendantes. S'agissant de la CNIL l'indépendance était d'autant plus nécessaire que la loi informatique et libertés avait pour objectif premier de garantir une protection de l'individu face au pouvoir étatique. Concernant le traitement des données à caractère personnel dans le domaine de la santé, couvertes par le secret professionnel en raison de leur source, le régime a longtemps été celui de l'autorisation. Il s'est assoupli au fur et à mesure jusqu'à ne plus concerner que les traitements de données à caractère personnel dans le domaine de la santé présentant une finalité d'intérêt public ou ayant pour finalité la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention. Par ailleurs, la CNIL opère également un contrôle en amont des mesures de sécurité que l'Etat prévoit de mettre en œuvre pour les traitements de données qu'il autorise par actes réglementaires[1008].

[1007] Monsieur Chevallier explique l'évolution complexe de la conception de l'Etat régulateur en quatre « temps ». Il évoque ainsi l'Etat régulateur comme « *principe de la cohésion sociale* », dans cette conception de la régulation « *l'État apparaît comme un principe d'ordre, dont l'intervention permet de faire tenir ensemble les divers éléments constitutifs de la société, en leur imposant la discipline d'un projet collectif* ». Cette conception de la régulation va accroitre « *la légitimité étatique : l'État apparaît plus que jamais comme le « centre » d'intégration et d'unification d'une société qui serait, sans son intermédiaire, vouée au désordre, à l'éclatement, à la dissolution ; c'est le catalyseur qui transforme les antagonismes sociaux en projet collectif, l'élément centripète indispensable pour contrebalancer les forces centrifuges, le facteur essentiel d'homogénéisation du tissu social. Cette valorisation de l'État conduit dès lors tout naturellement à l'ériger en clef de voûte du développement social : en tant que « régulateur », l'État devient la « providence » de la société* ». L'Etat régulateur renvoie alors à l'Etat providence, « *clef de voûte du développement social* » dont les critiques néo-libérales auront raison, signant le « retrait de l'Etat ». La régulation est alors conçue comme une forme d'arbitrage de l'Etat, mais c'est d'abord un arbitrage économique qu'il opère, dans les secteurs où il n'a plus le monopole et donc où il n'opère plus comme acteur direct. Il devient alors, selon les mots de Monsieur Chevallier « arbitre du jeu économique » (J. CHEVALLIER, « L'Etat régulateur », *RFAP*, 2004/3, n° 111, pp. 473-482).

[1008] C'est le cas des traitements de données utilisant le NIR mais s'agissant de l'utilisation du NIR dans le domaine de la santé les conditions d'utilisation du NIR ont fait l'objet d'un assouplissement (En ce sens v. L. CLUZEL-METAYER et E. DEBAETS, « Le droit de la protection des données personnelles : la loi du 18 juin 2018 », *RFDA*

205. Sanctions de la CNIL. L'action préventive de la CNIL se double d'un pouvoir de sanction. Le tournant pris par le Règlement européen vers la *compliance* ne signifie pas l'absence de sanction. Au contraire, et bien que la *compliance* suppose la confiance[1009], les sanctions à l'égard des responsables de traitement, qu'il s'agisse de personnes publiques ou de personnes privées[1010], sont importantes. La gradation de ces sanctions est prévue à l'article 45 de la loi informatique et libertés. Allant du rappel à l'ordre à l'amende administrative dont le montant maximum est de 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, la CNIL peut également demander au responsable de traitement de se mettre en conformité et assortir cette demande d'une astreinte journalière pouvant s'élever à 100 000 € par jour de retard. Ces sanctions peuvent évidemment porter sur la nécessité d'assurer la sécurité et la confidentialité des traitements. La faiblesse du contentieux civil en matière de protection des données à caractère personnel s'explique essentiellement par l'approche règlementaire de la loi de 1978 : « *En confiant à la CNIL le rôle de recevoir* « les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements de données à caractère personnel *» le législateur a fait le choix d'un traitement administratif des difficultés rencontrées par la personne concernée dans l'exercice de ses droits […]* »[1011].

2018, p. 1101) par la Loi n° 2016-41 du 26 janv. 2016 de modernisation de notre système de santé (instituant le NIR comme identifiant national de santé) et la Loi n° 2016-1321 du 7 oct. 2016 pour une République numérique (LRN) puis par la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. Enfin la Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé est encore venue modifier la loi informatique et libertés. Désormais, le cadre juridique des traitements de données comportant le NIR est inscrit à l'article 30 de la LIL. Cet article impose que ces traitements soit mis en œuvre par un décret pris en Conseil d'Etat, il pose également de nombreuses exceptions. Ainsi pour l'utilisation du NIR dans les traitements de données à caractère personnel dans le domaine de la santé ce sont les dispositions dédiées au traitements de données à caractère personnel dans le domaine de la santé qui s'appliquent (régime d'autorisation uniquement si le traitement n'est pas conforme à un référentiel type pris par la CNIL). Toutefois, un décret en Conseil d'Etat est encore exigé pour : les traitements de données à caractère personnel dans le domaine de la santé mis en œuvre par les organismes ou les services chargés d'une mission de service public figurant sur une liste fixée par arrêté des ministres chargés de la santé et de la sécurité sociale ayant pour seule finalité de répondre, en cas de situation d'urgence, à une alerte sanitaire et d'en gérer les suites (art. 67 LIL) et pour fixer les conditions d'utilisation du NIR comme identifiant national en santé (art. L. L1111-8-1 du CSP et art. 30 de la LIL).

[1009] K. FAVRO souligne la contradiction apparente entre la *compliance* qui suppose une discipline que l'opérateur s'impose à lui-même et les sanctions « surdimensionnées » que peut infliger la CNIL (*Ibid.* ; K. FAVRO, « La CNIL, une autorité à « l'âge de la maturité » », *Dalloz IP/IT* 2018, p.464).

[1010] Seul l'Etat ne peut être condamné à une amende pour les fichiers mis en œuvre par lui (art. 45 7° LIL).

[1011] C. BLOUD-REY, « Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? », *D.* 2013, p. 2795.

Les sanctions des autorités administratives en générale et de la CNIL en particulier vise à assurer l'effectivité des normes[1012].

206. Faiblesse du contentieux pénal. Outre le contrôle de la CNIL et les sanctions administratives prononcées par elle, le juge répressif peut également connaître des manquements à l'obligation de sécurité et de confidentialité à laquelle est soumis le responsable du traitement ou le sous-traitant. En effet, l'article 226-17 du Code pénal réprime le fait de procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi informatique et libertés, mesures qui consistent à assurer la sécurité et la confidentialité des données traitées. Surtout, l'infraction prévue à l'article 226-22 du Code pénal sanctionne spécifiquement la divulgation des données à des tiers non-autorisés. Le nombre de sanctions pénales prises sur ce fondement est néanmoins faible. Cette faiblesse du contentieux s'explique par l'efficacité des sanctions administratives de la CNIL comme le souligne notamment Madame Bloud-Rey « *La flexibilité, la variété, la rapidité des sanctions administratives, ainsi que l'absence d'une véritable politique pénale adaptée constitueraient une première série de facteurs. Les juges ne maîtriseraient guère les notions et principes de la loi de 1978 et hésiteraient à prononcer des sanctions adéquates, le quantum de la peine apparaissant comme excessif* »[1013]. Nous ne consacrerons donc qu'un court développement aux infractions pénales pour concentrer ensuite notre attention sur la doctrine de la CNIL, premier interprète des dispositions relatives à la protection des données[1014].

[1012] Sur les notions d'effectivité et d'efficacité v. Ph. CONTE, « « Effectivité », « inefficacité », « sous-effectivité », « surefficacité »…variations pour un droit pénal », *in Mélanges Catala*, Litec, 2001, p. 125. A propos des sanctions des autorités administratives v. aussi M. BENEJAT qui explique que « *Les sanctions qu'elles prononcent n'ont pas un objectif purement répressif mais visent avant tout le bon fonctionnement des systèmes qu'elles chapeautent* » (M. BENEJAT, *La responsabilité pénale professionnelle*, préf. J.-C. SAINT-PAU coll. nouvelle bibliothèque des thèses, Dalloz, vol. 111, 2012, n° 17). On peut encore rappeler que cette efficacité, ainsi que le niveau d'expertise important des AAI, constitue un des arguments sociologiques de leur création (En ce sens v. P. IDOUX, « L'argument sociologique et les autorités administratives indépendantes », *in* D. FENOUILLET (ss. la dir.), *L'argument sociologique en droit. Pluriel et singularité*, coll. Thèmes, actes et commentaires, Dalloz, 2015, p. 137, spéc. 139.

[1013] C. BLOUD-REY, « Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? *D.* 2013, p. 2795). V. également J. FRAYSSINET, « La régulation du respect de la loi informatique, fichiers et libertés par le droit pénal : une épée en bois », *Légicom* 2009, n° 42, p. 23.

[1014] « *Toute la doctrine de la CNIL consiste ainsi, au travers des délibérations qu'elle adopte, à interpréter les dispositions générales de la loi Informatique et Libertés à la lueur des dispositions spéciales qui s'appliquent à chaque cas d'espèce* » (G. DESGENS-PASANAU, « Le Conseil d'État censure la CNIL sur la question des contrôles sur place et des fichiers d'exclusion », *Dalloz IP/IT* 2016, p. 615) ; « *Forte de la concentration de ses pouvoirs, la Commission nationale informatiques et libertés (CNIL) occupe aujourd'hui une place primordiale dans le système mis en œuvre par la loi n° 78-17 du 6 janvier 1978 modifiée. Son action se traduit notamment par la construction d'un « corps de doctrine de la CNIL* » (C. BLOUD-REY, « Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? », *op. cit.*).

§ 2 - La violation de confidentialité des données, une infraction voisine de la violation du secret professionnel

207. L'infraction prohibant la violation de la confidentialité des données sanctionne, entre autre, la divulgation des données à caractère personnel à des tiers non-autorisés **(A)**. Elle peut donc être comparée à l'infraction sanctionnant la violation du secret professionnel **(B)**.

A - La divulgation à des tiers non-autorisés

208. Sanction de la divulgation de données à caractère personnel. Le juge répressif peut être amené à se prononcer en raison de la commission de certaines infractions portant atteinte aux droits de la personne résultant du traitement de leurs données personnelles. L'article 226-22 du Code pénal incrimine le fait « *pour toute personne* » qui a procédé à des opérations sur des données à caractère personnel « *dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir* ». Le second alinéa de l'article incrimine les mêmes faits lorsque la divulgation est commise par négligence ou imprudence. Cette infraction n'a pas fait l'objet de beaucoup de travaux spécifiques en doctrine[1015], les condamnations sur ce fondement étant par ailleurs assez rares[1016]. Matériellement l'infraction nécessite une révélation, volontaire ou non, à un tiers non autorisé à connaitre les données personnelles objet de la révélation. Cette infraction ne sanctionne pas uniquement un manquement à l'obligation de sécurité puisque l'infraction peut

---

[1015] Les principaux travaux portent néanmoins sur le rapport entre cette infraction et de celle sanctionnant la violation du secret professionnel : M. BENEJAT, « Les droits sur les données personnelles », *in* J.-C. SAINT-PAU (ss. la dir.), *Traités de droit de la personnalité,* LexisNexis, n° 1045 et plus ancien J. FRAYSSINET, « Un concurrent associé du secret professionnel : le droit de la confidentialité du traitement des données personnelles », *Revue Juridique de l'Ouest* 2000, n° spéc. *Les médecins libéraux face au secret médical*, pp. 23-46 ; J. FRAYSSINET, « La confidentialité sur l'Internet : du secret professionnel à la protection des données personnelles », *Gaz. Pal*., 26 mars 2002, n°85, p. 17 ; C. ZORN, *Données de santé et secret partagé pour un droit de la personne à la protection de ses données de santé partagées*, *op. cit.*, n° 39 et svt.

[1016] Le constat est identique pour toutes les infractions relatives à la loi informatique et libertés et déjà souligné de longue date par J. FRANCILLON, « Infractions relevant du droit de l'information et de la communication », *Rev. sc. crim.*, 1996, n°3, p. 676 ; A. LEPAGE « Loi du 6 août 2004. Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *Com. comm. électr.* 2005, n° 2, étude 9 ; G. BRAIBANT, *Données personnelles et société de l'Information*, Rapport au Premier ministre, *La Documentation française*, 1998, p. 119 ; J. FRAYSSINET, « La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée en bois », *Legicom* 2009/1, p. 23.

être commise par toute personne ayant effectué des opérations sur des données faisant l'objet d'un traitement. Tandis que l'obligation de sécurité n'incombe qu'au responsable de traitement et au sous-traitant, qui peuvent se voir infliger de sévères amendes par la CNIL, l'infraction prévue à l'article 226-22 du Code pénal n'est pas attitrée. Le personnel technique ou administratif d'une structure responsable de traitement peut donc être poursuivi sur ce fondement alors même qu'il n'est pas débiteur de l'obligation légale de sécurité du traitement. Ensuite, n'est punissable que la révélation qui « *aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée* »[1017]. L'utilisation du conditionnel démontre, selon un auteur, qu'il n'est nul besoin d'un tel résultat mais simplement d'un risque, dont l'appréciation sera fonction de la nature des données divulguées[1018]. Enfin, il faut que les données aient été révélées à des tiers non qualifiés pour en connaitre. Analysant la notion de « *tiers qui n'a pas qualité pour les recevoir* » Madame Bénéjat, propose une approche *a contrario* et affirme qu'une personne est qualifiée pour recevoir des données au regard de deux critères : **la nécessité et la confiance**[1019]. Ainsi une personne est qualifiée à recevoir des données lorsque « *l'exercice de ses fonctions requiert qu'elle dispose de l'information* » et lorsqu'elle « *présente des garanties suffisantes de confiance, notamment lorsqu'elle est astreinte au secret* ». L'infraction présente, en ce sens, des ressources complémentaires par rapport au secret professionnel.

209. La confidentialité et la notion de tiers : des notions extra-pénales. La notion de confidentialité est toujours définie par son objectif : elle consiste dans le fait de s'assurer que les données ne sont pas communiquées à des tiers non-autorisés. Le moyen pour s'en assurer consiste en des mesures de sécurité. La loi ne fixe alors qu'un objectif, laissant à la CNIL et la jurisprudence le soin de définir si les données sont effectivement accessibles à des tiers non-autorisés. Le point nodal de la définition réside donc dans la notion de tiers non-autorisés. Or, il s'agit d'une notion extérieure au droit pénal, il faut donc en rechercher la définition dans le RRGP et au travers des analyses de la CNIL.

[1017] Art. 226-22 CP.
[1018] En ce sens M. BENEJAT, « Les droits sur les données personnelles », *in* J.-C. SAINT-PAU, *Traités de droit de la personnalité*, LexisNexis, n° 1045.
[1019] *Ibid.*

Si le défaut de sécurité et donc de confidentialité est évident lorsque les données sont, par exemple, accessibles en ligne[1020], la CNIL a aussi pu décider de l'existence d'un manquement à l'obligation de sécurité, mettant en péril la confidentialité, en raison du manque de robustesse des mots de passe nécessaires pour accéder aux données[1021], ou de l'absence de limitation du nombre de tentatives infructueuses d'authentification[1022]. Ainsi, une sécurité adéquate est en quelque sorte la base de la confidentialité. Dans le cas de traitements de données à caractère personnel, le tiers est, au sens du RGPD : « *une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel* »[1023]. La définition est négative : sont des tiers tous ceux qui ne sont pas autorisés à traiter les données. La notion de tiers serait alors différente de celle de tiers non-autorisé.

210. Les destinataires, les tiers et les tiers autorisés. La notion de tiers non-autorisés se comprendrait donc *a contrario* des définitions des autres personnes qui sont autorisées à traiter les données. Afin de saisir qui sont les acteurs dont il est question il est nécessaire de procéder par exclusion[1024]. Le responsable du traitement, le sous-traitant et les personnes placées sous leur autorité ne sont pas des tiers selon la définition qui est donnée de ces derniers. Le RGPD définit également la catégorie des destinataires. Le destinataire est « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers* »[1025]. Ainsi, un premier cercle de personnes doit être retranché : la personne concernée, le responsable du traitement, les sous-traitants et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données

---

[1020] V. par exemple CNIL, délibération de la formation restreinte n° SAN-2018-010 du 6 septembre 2018 prononçant une sanction pécuniaire à l'encontre de l'association Alliance française paris Île-de-France ; délibération de la formation restreinte n° SAN-2018-002 du 7 mai 2018 prononçant une sanction pécuniaire à l'encontre de la société Optical Center CNIL, délib. n° 2014-238, 12 juin 2014.
[1021] CNIL, décision n°2016-083 du 26 septembre 2016.
[1022] CNIL, décision n° 2016-058 du 30 juin 2016 mettant en demeure la société Microsoft.
[1023] Art. 4 12) RGPD.
[1024] *Adde* A. DEBET, J. MASSOT, N. METALLINOS *et alii*, *Informatique et libertés*, coll. les intégrales, Lextenso Editions, 2015, n° 550.
[1025] Art. 4 9) RGPD.

ne sont pas des tiers[1026] mais peuvent être des destinataires. Ensuite, les destinataires ne sont pas responsables du traitement mais peuvent en avoir communication, notamment en raison des finalités du traitement[1027]. Ces destinataires sont des tiers au traitement dès lors qu'ils ne font pas partie de la première catégorie évoquée : ils ne sont pas les personnes originellement autorisées à traiter les données. Enfin, les tiers autorisés sont toutes les personnes qui ne sont pas autorisées à traiter les données mais ont la possibilité d'accéder où de se faire communiquer les données en vertu d'un texte légal ou règlementaire[1028]. Les destinataires qui ne sont pas des tiers constituent une catégorie de personnes qui peuvent avoir accès aux données en raison de l'activité, parfois technique, qu'elles ont à jouer dans la mise en œuvre du traitement. Elles ont un rôle secondaire[1029] : il s'agit notamment des services qui mettent en œuvre le traitement et qui sont, à ce titre, « *chargés de l'exploitation informatique des données* »[1030], ou encore « *les services fonctionnellement ou opérationnellement responsables de la mise en place du traitement* »[1031]. Enfin, il faut noter, s'agissant des personnes qui, en raison de leurs fonctions, sont chargées de traiter les données[1032] qu'il s'agit du personnel qui accède aux données « *pour les besoins de l'accomplissement de leurs tâches professionnelles, comme par exemple des opérateurs de saisie, des personnels d'un centre d'appel accédant au dossier du consommateur* »[1033]. Nous rejoignons sur ce point l'analyse de Madame Bénéjat qui suggère que ces personnes accèdent aux données en raison d'un critère de nécessité[1034].

211. Tiers non-autorisés. Au regard de ce qui vient d'être expliqué, il apparaît que les tiers non-autorisés sont donc tous ceux qui ne sont ni la personne concernée par les données ni celles autorisés à traiter les données, ni les destinataires – qui sont potentiellement des tiers dans la mesure où ce ne sont pas des personnes autorisées à traiter les données – , ni des tiers autorisés en vertu d'une autorisation légale ou règlementaire[1035]. Le lien entre secret professionnel et

---

[1026] A ce titre ne peuvent être considérés comme des tiers non autorisé les super administrateurs d'un logiciel dès lors qu'ils prennent connaissance des données à caractère personnel dans le cadre de leurs activités de maintenance du logiciel support du traitement des données (Crim., 3 juin 2008, n° 08-80.467 : *JCP E* 2009, 1674, n° 27, obs. M. VIVANT, N. MALLET-POUJOL et J.-M. BRUGUIERE).

[1027] La CNIL définit le destinataire comme une personne habilitée à recevoir les données en raison de ses fonctions. Il s'agit des fonctions au regard des finalités de traitement (<https://www.cnil.fr/fr/definition/destinataire>, dernière consultation le 14 oct. 2019).

[1028] *CNIL, Dix ans d'informatique et libertés*, Économica, 1988, p. 30.

[1029] A. DEBET, J. MASSOT, N. METALLINOS *et alii*, *Informatique et libertés*, *op. cit.*, n° 550.

[1030] *Ibid.* n° 552.

[1031] *Ibid*.

[1032] Et ne sont, à ce titre, ni des destinataires, ni des tiers, ni des tiers autorisés.

[1033] A. DEBET, J. MASSOT, N. METALLINOS *et alii*, *Informatique et libertés*, *op. cit.*, n° 553.

[1034] M. BENEJAT, « Les droits sur les données personnelles », *op. cit.*, n° 1045.

[1035] En ce sens v. J.-M. BRUGUIÈRE, N. MALLET-POUJOL, M. VIVANT, « Droit de l'informatique », *JCP E* 2002, n° 23, 888, p. 949, n°20.

confidentialité ne se dessine pas d'emblée, il relève en premier lieu d'une complémentarité entre l'infraction prévue à l'article 226-13 du Code pénal et celle de l'article 226-22 du même Code.

B - Cumul des qualifications et complémentarité

212. La moblisation des principes du droit pénal général permet d'envisager la possibilité d'un cumul des qualifications **(1)**, leurs champs d'application sont complémentaires **(2)**.

1 - Cumul des qualifications

213. Commission de l'infraction informatique par un professionnel soumis au secret professionnel. L'étude des qualifications de violation du secret professionnel et de divulgation de données à caractère personnel a été faite de longue date[1036]. Monsieur Frayssinet, à l'occasion de plusieurs articles, expose les ressources concurrentes et donc complémentaires des deux incriminations[1037]. Il faut d'abord rappeler que lorsqu'un traitement de données porte sur des données de santé issues d'une prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins, au sens de l'article L. 1110-4 du Code de la santé publique, les personnes appelées à procéder à des opérations sur les données peuvent également être soumises au secret professionnel. Ainsi, le professionnel qui, à l'occasion d'opérations sur des données à caractère personnel, lesquelles sont également des informations à caractère secret dont il a pris connaissance dans l'exercice de ses fonctions, divulgue volontairement celles-ci, commet l'infraction de violation du secret professionnel et celle de divulgation de données à caractère

---

[1036] A. LEPAGE « Loi du 6 août 2004. Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *Com. comm. électr.* 2005, n° 2, étude 9 ; J. FRAYSSINET, « La confidentialité sur internet : du secret professionnel à la protection des données personnelles », *Gaz. Pal.* 2002, doctr. n°85 ; J. PRADEL et M. DANTI-JUAN, *Droit pénal spécial*, coll. manuels Cujas, Cujas, 3e éd., n° 273.

[1037] J. FRAYSSINET, « La confidentialité sur internet : du secret professionnel à la protection des données personnelles », *op. cit.* ; , « Un concurrent associés du secret professionnel : le droit de la confidentialité du traitement des données personnelles », *Revue juridique de l'Ouest* 2000, n° spéc. « Les médecins libéraux face au secret médical », p. 23 ;

personnel. Le concours de qualifications se résoudrait alors par l'application du texte spécial[1038] c'est-à-dire l'incrimination de divulgation de données qui est également la plus haute qualification pénale[1039]. Dans la seule affaire ayant donné lieu à une condamnation à notre connaissance, le juge avait retenu les délits de violation du secret professionnel, de manquement à la sécurité informatique (226-17 du code pénal) et divulgation d'informations nominatives[1040]. Ce qui amène à considérer que les valeurs sociales protégées par ces infractions ne sont pas identiques et que les deux qualifications peuvent donc être retenues pour un même fait. Cela confirme leur complémentarité et abonde sans doute dans le sens de la thèse de Madame Bénéjat qui considère que le secret professionnel a vocation à protéger l'ordre public professionnel[1041] et non pas un intérêt privé, ce que l'auteur illustre par exemple, en évoquant le cumul des qualifications et les valeurs protégées, en prenant l'exemple du cumul des qualifications de violation du secret professionnel et de diffamation qui sanctionnent l'atteinte « *cumulative d'intérêts collectifs ou individuels distincts* »[1042]. Mais l'on peut également défendre l'idée que l'infraction sanctionnant la divulgation des données protègerait l'identité tandis que l'infraction de violation du secret professionnel protégerait la vie privée ou l'ordre public.

2 - Complémentarité des champs d'application

214. Complémentarité : caractère involontaire de la divulgation. Outre la question de la concurrence sur le plan de la qualification, les infractions méritent d'être comparées au regard de leur champs d'application. Le premier élément permettant d'affirmer une complémentarité des infractions tient à la sanction de la divulgation involontaire des données à caractère personnel. L'article 226-22 al. 2 du Code pénal sanctionne les divulgations par imprudence ou négligence là où la violation du secret professionnel doit être volontaire pour être caractérisée mais les deux infractions peuvent porter sur le même objet dès lors que les données à caractère

---

[1038] En ce sens. J. FRAYSSINET, « Un concurrent associés du secret professionnel : le droit de la confidentialité du traitement des données personnelles », *op. cit.*

[1039] M. BENEJAT, « Les droits sur les données personnelles », in J.-C. SAINT-PAU (ss. la dir.), Traités de droit de la personnalité, LexisNexis, n° 1045

[1040] CA Rennes, 13 janv. 1992 : *D.* 1993, somm. pr. 54, obs. M. VASSEUR ; *D.* 1994, somm. p. 287, obs. H. MAISL.

[1041] M. BENEJAT, *La responsabilité pénale professionnelle*, *op. cit.*, spéc. sur la définition donnée par l'auteur de l'ordre public professionnel v. n° 242 et svt.

[1042] Crim., 19 oct. 1982 : *Bull. crim.* n° 225 ; Commentant cette formulation : « Expression que l'on peut comprendre comme visant d'une part les intérêts privés – et d'autre part l'ordre public professionnel – pour le délit de violation du secret professionnel », *Ibid.* n° 252.

personnel, sensibles ou non, peuvent également être des informations secrètes. Le risque de confusion serait alors assez commun au profit de la seule violation du secret professionnel. Comme le constate un auteur : « *L'attitude habituelle consistant à lui attribuer un quasi-monopole de protection du secret, de la confidentialité, de la discrétion des informations relatives aux patients est une forme de réflexe qui frise aujourd'hui la paresse intellectuelle* »[1043]. La sanction de la divulgation involontaire de données à caractère personnel consiste pourtant en une véritable ressource complémentaire au secret professionnel, d'autant plus que, sur le plan pénal, l'élément moral de l'infraction a donné lieu à quelques désaccords doctrinaux.

L'infraction de violation du secret professionnel a effectivement pu servir d'exemple pour illustrer la question des difficultés à distinguer entre le concept de dol général et la faute purement matérielle. Tandis qu'Emile Garçon affirmait, lorsqu'il annotait le Code pénal, que le professionnel qui laissait à la vue de tous un document contenant des informations à caractère secret ne commettait pas l'infraction de violation de secret professionnel dans la mesure où celui-ci n'a pas, alors, la conscience et la volonté de commettre l'infraction[1044] (définition du dol général), Monsieur Dana affirmait que dans un tel exemple ce n'était pas l'intention qui faisait défaut mais l'élément matériel lui-même[1045]. Certains auteurs ont également considéré que certaines imprudences graves pouvaient donner lieu à sanction sur le fondement de l'article 226-13 du Code pénal[1046]. Enfin, Monsieur Couturier relevait sur ce point une confusion dans la jurisprudence et la doctrine entre imputabilité et culpabilité[1047]. Les différences de conception de l'élément moral de l'infraction de violation du secret professionnel, significatives d'une jurisprudence peu lisible[1048], souligne encore l'intérêt de l'infraction sanctionnant la révélation

---

[1043] J. FRAYSSINET, « Un concurrent associés du secret professionnel : le droit de la confidentialité du traitement des données personnelles », *op. cit.*

[1044] E. GARCON, *Code pénal annoté*, 2ème éd. par M. ROUSSELET, M. PATIN et M. ANCEL, Sirey, 1959, sous art. 378, n° 52. C'est l'opinion principalement partagée : v. par exemple J. PRADEL et M. DANTI-JUAN, *Droit pénal spécial*, *op. cit.*, n°308 ; E. DREYER, *Droit pénal spécial*, coll. Cours magistral, ellipses, 3e éd., 2016, n° 424.

[1045] A.-C. DANA, *Essai sur la notion d'infraction pénale*, Bibl. sc. crim., LGDJ., 1981, n° 468.

[1046] En ce sens v. M. DELMAS-MARTY et G. GUIDICELLI-DELAGE (ss. la dir.), *Droit pénal des affaires*, 4ème éd., P.U.F., Paris, 2000, p. 119 ; - *Adde*. J. LARGUIER et PH. CONTE, *Droit pénal des affaires*, 9ème éd., Armand Colin, Paris, 1998, n° 386 ; J. LARGUIER « Le secret de l'instruction et l'art. 11 du Code de procédure pénale », *Rev. sc. crim.* 1959, p. 313.

[1047] M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, th. dact., *op. cit.*, n° 237 et svt.

[1048] *Ibid.*

des données à caractère personnel. Cette infraction est en outre plus adaptée aux problématiques propres aux dispositifs techniques de l'information et de la communication puisque ce sont principalement les mésusages et les failles de sécurité de ces dispositifs qui présentent un frein à la confiance des individus dans les outils techniques. Il faut noter par ailleurs que lors de la rédaction du Code pénal de 1994 il avait été question de sanctionner également la révélation involontaire d'une information par un professionnel soumis au secret, ce qui avait finalement été abandonné[1049].

215. Complémentarité : des données recueillies à l'occasion d'une opération de traitement. La divulgation incriminée par l'article 226-22 du Code pénal porte sur des données recueillies à l'occasion d'une opération de traitement tandis que l'incrimination de violation du secret professionnel ne comprend aucun élément de nature technique. Sur ce point le champ d'application de la seconde infraction est plus large et celle-ci a vocation à s'appliquer aussi bien pour les données à caractère personnel traitées par un professionnel tenu au secret, dès lors qu'elles sont également des informations venues à la connaissance du professionnel, que pour toutes informations indépendamment de sa forme.

216. Complémentarité : la divulgation par « toute personne ». Si l'incrimination de violation du secret professionnel est une infraction *attitrée* dans la mesure où elle ne concerne que certaines personnes désignées par un texte légal ou règlementaire – dans le domaine de la santé l'article L. 1110-4 du Code de la santé publique – la divulgation prévue à l'article 226-22 du Code pénal concerne toute personne ayant procédé à des opérations sur les données. Le champ d'application de la seconde infraction, particulièrement large, permet de passer outre les difficultés liées à la question de savoir si telle ou telle personne est soumise au secret professionnel.

217. Complémentarité : l'objet de la révélation. Tandis que la violation du secret professionnel suppose la révélation d'une information à caractère secret, notion ayant donné lieu à de nombreux questionnements sur le point de savoir, notamment, si l'identité d'un client ou d'un patient constituait une telle information, la qualification de données à caractère personnel est plus évidente et suppose que les données puissent permettre d'identifier, directement ou non la personne concernée. Si toutes les informations à caractère secret sont nécessairement des données à caractère personnel, voire des données sensibles, ces

[1049] C. JOLIBOIS, Rapport au Sénat, n° 295, 1991, p. 154.

qualifications dépassent celle d'information à caractère secret. Les notions de données à caractère personnel ou de données sensibles étant clairement définies et attachées au critère d'identification de la personne, l'objet de l'infraction est donc plus aisé à définir. S'agissant de l'infraction de violation du secret professionnel, le critère de rattachement – la nature de l'information ou la profession du déposant – est toujours sujet à discussion.

218. Complémentarité : l'atteinte à la considération de l'intéressé ou à l'intimité de la vie privée. Si la majorité de la doctrine considère que l'effet préjudiciable de la révélation n'est pas une condition de la répression de la violation du secret professionnel[1050], la thèse inverse a pu être soutenue[1051]. De plus la Cour de cassation et les juridictions du fond ont pu souligner l'existence d'un préjudice sans pour autant affirmer qu'il s'agissait d'une condition de la répression[1052]. Cette question illustre toutes les difficultés relatives à l'infraction de violation du secret professionnel et cristallise celle de l'incertitude quant à son fondement[1053]. Il en va autrement du délit de divulgation prévu à l'article 226-22 du Code pénal qui suppose simplement l'exposition à un risque. L'appréciation du caractère dommageable de la divulgation est appréciée souverainement par les juges du fond[1054]. Il apparaît en outre que l'infraction prévue à l'article 226-22 du Code pénal est un délit privé puisque les poursuites

---

[1050] En ce sens v. par exemple : E. DREYER, *Droit pénal spécial*, *op. cit.*, n° 424 ; B. PY, *Rep. pén.*, v° « secret professionnel », fév. 2003 (mis à jour fév. 2017), n° 71 ; V. PELTIER, *Jcl. pénal code*, Fasc. 20 « Révélation d'une information à caractère secret. – Conditions d'existence de l'infraction. – Pénalités », n° 43.

[1051] V. par exemple : A. CHAVANNE, note sous CA Paris, 17 novembre 1953, R.-F. LE BRIS, note sous Civ. 1e, 26 mai 1964 ; *D*. 1965.109 ; M. DELMAS-MARTY « A propos du secret professionnel », *D*. 1982, chron. p. 267. Par ailleurs certains auteurs ont pu affirmer que seule la révélation d'une information préjudiciable à celui qui s'est confié permet de caractériser l'élément matériel de l'infraction. Ce n'est donc pas sur le terrain du résultat qu'ils se placent mais sur celui de l'élément matériel : J. PRADEL et M. DANTI-JUAN, *Droit pénal spécial*, 3ème éd., Cujas, Paris, 2004, n° 297, p. 257.

[1052] Pour une revue complète de la jurisprudence en ce sens v. M. COUTURIER, *Pour une analyse fonctionnelle du secret professionnel*, th. dact., *op. cit.*, n° 247 et svt.

[1053] Soit fondé sur un intérêt privé et sanctionnant une atteinte à la vie privée, soit fondé sur l'intérêt général et sanctionnant l'atteinte à la confiance dans certaines professions v. V. PELTIER, *Jcl. Pénal Code*, *op. cit.*, spéc. n° 5 et proposant de considérer la question sous l'angle d'une approche fonctionnelle et affirmant que la fonction exprimée du secret professionnel est la protection de la vie privée de celui qui se confie tandis que la fonction latente consiste dans la protection des professions soumises au secret v. M. COUTURIER, *Pour une analyse fonctionnelle du secret professionnel*, *op. cit.*

[1054] Il a ainsi été jugé que la révélation non intentionnelle du numéro de téléphone d'un particulier sur une messagerie rose constituait une telle atteinte (T. com. Briey, 15 sept. 1992 : *D.* 1994, somm. p. 289, obs. H. MAISL) ou encore s'agissant du directeur d'un établissement de crédit qui ayant communiqué à des commerçants une liste informatique de clients de l'établissement pouvant présenter des risques d'insolvabilité (CA Rennes, 13 janv. 1992 : *D.* 1993, somm. pr. 54, obs. M. VASSEUR ; *D.* 1994, somm. p. 287, obs. H. MAISL).

sont conditionnées à la plainte de la victime, tandis que le déclenchement des poursuites pour violation du secret professionnel reste à la discrétion du ministère public.

219. Place du consentement de la personne concernée. A l'instar du délit d'atteinte à la vie privée, incriminé à l'article 226-1 du Code pénal, le consentement est un élément constitutif de l'infraction de divulgation des données à caractère personnel[1055]. Il s'agit de la principale différence avec l'incrimination de violation du secret professionnel. Dès lors que la personne donnerait son consentement à la divulgation de ses données à caractère personnel, aucune poursuite ne pourrait être engagée sur le fondement de l'article 226-22 du Code pénal tandis que les poursuites resteraient envisageables sur le fondement de l'article 226-13 du Code pénal. Cette différence permet encore de comprendre que les valeurs sociales protégées par ces infractions ne sont pas identiques et incline à penser que le secret professionnel a surtout pour finalité la protection de la confiance publique.

220. La confidentialité, une forme de secret partagé ? La formulation du texte d'incrimination sanctionnant la révélation de données à caractère personnel n'est pas sans rappeler celle qui avait été envisagée, à l'époque de la rédaction du nouveau Code pénal, pour l'article 226-13 du Code pénal. La Commission de révision du Code pénal avait alors envisagé de consacrer un secret partagé général en incriminant uniquement la révélation faite « *à une personne non qualifiée pour en partager le secret* »[1056]. Suite à de nombreux débats[1057] la proposition avait été définitivement abandonnée. Les arguments qui avaient justifié l'abandon tenaient au fait que la référence à une personne non qualifiée était trop imprécise[1058] ainsi que la crainte que cela ne remette en cause l'existence même du secret professionnel de manière subreptice et « *que le verrou du secret ne finisse par sauter au profit d'organismes publics ou à des fins purement commerciales* »[1059]. Le secret partagé a finalement été érigé, dans le domaine de la santé, comme un fait justificatif de la violation du secret professionnel au travers

---

[1055] Ce dernier délit n'est toutefois pas un délit privé dans la mesure où, contrairement à l'infraction sanctionnant une atteinte à la vie privée par le moyen de dispositifs d'espionnage, l'action publique n'est pas conditionnée à une plainte de la victime (CP, art. 226-6).
[1056] G. ROUJOU DE BOUBEE, B. BOULOC, J. FRANCILLON, Y. MAYAUD, *Code pénal commenté*, Dalloz, 1996, p. 401.
[1057] *Ibid.* p. 401.
[1058] V. intervention C. Jolibois lors de la discussion du texte en seconde lecture, *JO* Sénat 4 oct. 1991, p. 2643, 2e col.
[1059] G. ROUJOU DE BOUBEE, B. BOULOC, J. FRANCILLON, Y. MAYAUD, *Code pénal commenté*, *op. cit.*, p. 402.

d'un texte dédié[1060] et non comme un élément de l'infraction. A l'inverse, l'article 226-22 du Code pénal laisse penser que la confidentialité consisterait en une forme de secret partagé qui ferait obstacle à la consommation de l'infraction[1061]. La question ne réside alors plus tant dans la distinction entre confidentialité et secret professionnel que dans l'étude de leurs rapports. C'est au stade de la mise en œuvre du traitement qu'il faut chercher les points de jonction. La doctrine de la CNIL constitue la matière première d'une telle entreprise.

Section 2 - Etude des rapports entre confidentialité et secret professionnel dans le domaine de la santé

221. Nous adhérons à l'idée que les critères de la confidentialité, c'est-à-dire les critères permettant de savoir qui a accès aux données sont : la confiance, que l'on peut placer en la personne qui accède aux données, et la nécessité qu'elle a d'accéder aux données pour que le traitement remplisse les finalités qui lui sont assignées. Sous l'angle de la vie privée la confiance est induite par le consentement de la personne concernée tandis que dans le domaine de la santé, la confiance est symbolisée par le secret professionnel. Aussi, la détermination des personnes qualifiées, et donc du contenu de la confidentialité, au regard de ce premier critère, varie-t-elle en fonction d'un élément extérieur. Quant au critère de la nécessité il implique également de recourir à des éléments extérieurs afin de déterminer si telle ou telle personne devrait avoir accès au traitement. Ce qui nous amène à étudier ces rapports sous deux angles. La détermination des personnes autorisées et donc le maintien de la confidentialité, qui est fonction de la soumission des personnes au secret professionnel **(paragraphe 1)**, constitue le

---

[1060] Dans le domaine de la santé c'est l'article L. 1110-4 du Code de la santé publique qui dispose des conditions du secret partagé mais la jurisprudence semble reconnaitre l'existence d'une telle justification dans d'autres domaine ce qui pose évidemment un problème du point de vue de la légalité criminelle : par exemple concernant la circulation, au sein d'un établissement bancaire, de la photocopie d'un chèque « *qui n'avait pas pour conséquence directe ou indirecte de faire connaître à un tiers un fait confidentiel en dehors de la « sphère bancaire »* » *(Crim. 18 oct. 2000, n° 99-85.563) ou encore que la communication, entre agents d'un même cabinet ministériel, d'un secret acquis dans l'exercice des fonctions, pour les besoins du service, ne constitue pas une révélation susceptible de tomber sous le coup de la loi pénale (CA Paris, 8 févr. 2001, Bull. inf. C. cass., no 538, 2001, no 727). Inversement, a été refusée pour non-préservation du secret professionnel entre associés la demande d'ouverture d'un cabinet secondaire d'avocats (CA Basse-Terre, 19 janv. 2000, Bull. info. C. cass., no 519, 2000, no 994)* » (B. PY, « Secret professionnel », *Rép. Pén. Dalloz* 2003 (act. Fév. 2017), n°160 et svt.).

[1061] En ce sens v. M. BENEJAT, « Les droits sur les données personnelles », *in* J.-C. SAINT-PAU (ss. la dir.), Traités de droit de la personnalité, *op. cit.*, n° 1045.

premier critère. La nécessité, second critère, est évaluée au regard de la finalité du traitement et de l'intérêt porté par cette finalité **(paragraphe 2**). Sur le plan de la méthode, nous nous appliquerons à souligner, ici encore, l'emploi de l'expression « secret médical » afin de parvenir, *in fine*, à démontrer que notre définition est également opérante dans le contexte de la protection des données et permet de déterminer la fonction de la confidentialité des données traitées dans le domaine de la santé.

§ 1 - L'assujettissement au secret professionnel, critère de la confidentialité

222. Nous proposons, au travers d'une analyse de la doctrine de la CNIL[1062] depuis sa création, de rendre compte de la place du secret professionnel comme déterminant de la mise

---

[1062] En raison des pouvoirs la CNIL est amenée, plus que le juge judiciaire, à interpréter les dispositions de la LIL en tenant compte des textes spéciaux qui participent à la protection des données « *le juge judiciaire occupe une place excessivement en retrait dans la mise en œuvre de la loi* » (C. BLOUD-REY, « Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? Analyse et perspectives », *D.* 2013, p. 2795). Le rôle de la CNIL n'est pas seulement de s'assurer du respect de la loi informatique et libertés mais de garantir l'application de toutes les dispositions relatives à la protection des données. A ce titre les dispositions, disséminées ça et là dans les textes de droit national et ayant vocation à protéger certaines informations en raison de leur nature ou de leur source sont interprétées par le CNIL tant lors de ses contrôles ex-ante qu'à l'occasion des sanctions qu'elle prononce (parmi la grande variété des pouvoirs octroyés aux autorités administratives indépendantes, dont la CNIL, il faut distinguer les pouvoirs règlementaires et, ceux qui correspondent à la possibilité d'édicter des normes de *droit souple* (Sur ce point v. B. LAVERGNE, *Recherche sur la soft law en droit public*, préf. N. JACQUINOT, coll. Thèses de l'IFR, PUT- LGDJ - Lextenso Editions, 2013 ; sur le droit souple v. *infra* n° 457. Les actes règlementaires peuvent ensuite être distingués selon qu'ils interviennent *en amont* ou *en aval* du traitement, le pouvoir d'autorisation relevant du premier type d'intervention et le pouvoir de sanction du second. A cet égard la Commission exerce son pouvoir de prendre des actes administratifs unilatéraux : Stéphane Gérry-Vernières, à l'occasion d'une analyse fonctionnelle des « petites » sources du droit, précise leur fonction de régulation, il explique que cette fonction est principalement remplie par ce type sources émanant des autorités administratives indépendantes (S. GERRY-VERNIERES, *Les « petites » sources du droit. A propos des sources étatiques non contraignantes*, coll. Recherches juridiques, Economica, 2012, n° 277 et svt). L'auteur s'emploie ensuite à distinguer les actes de régulation, les actes consultatifs et les actes décisoires (*Ibid.* n°291 et svt.). Il nous faut brièvement rappeler cette distinction car ces sources seront évoquées ultérieurement : Les actes de régulation constituant les « petites » sources du droit sont les instruments définis, en droit administratif, comme des « *actes juridiques, d'appellation et de formation diverses, qui ne comportent pas d'effet juridique obligatoire à l'égard des administrés destinataires, mais ont à leur égard un effet d'incitation, de conviction ou d'intimidation parfois plus efficace* » (Y. GAUDEMET, *Traité de droit administratif*, T. I, LGDJ, 16e éd., 2001, n° 1357). Les actes décisoires peuvent prendre la forme de décisions administratives individuelles faisant grief. C'est le cas des sanctions de la CNIL prévues à l'article 45 II et 46 de la LIL qui peuvent faire l'objet d'un recours devant le Conseil d'Etat en vertu de l'article R. 311-1 du Code de justice administrative (« *les sanctions pécuniaires prononcées par des autorités administratives constituent en réalité des sanctions de nature répressive dans la mesure où elles ont pour objet de punir un manquement à une obligation. Elles revêtent la forme d'une décisions administrative unilatérale* » (M. DOBKINE, « L'ordre répressif administratif », *D.* 1993, chron. p. 157). Les autres mesures prises par la CNIL qui ne sont pas des sanctions (c'est le cas des mises en demeure qui sont toutefois susceptibles de recours: CE, 9e et 10e ss-sect. réunies, 27 juill. 2012, n° 340026, Sté AIS2 : *Lebon* ; *JCP E*, 2012, n° 37, 1534, Pan. ; *JCP A*, 2012, n° 35, Act. 570, note C.-A. DUBREUIL ; *RSC* 2012, p.614, obs. J. FRANCILLON) sont parfois difficiles à qualifier et c'est au cas par cas que le Conseil d'Etat admet la recevabilité des recours (il en est par exemple ainsi du refus de la CNIL d'engager

en œuvre de la confidentialité des traitements de données dans le domaine de la santé. Cette entreprise est évidemment dépendante des évolutions du régime des traitements, le contrôle *ex ante* de la CNIL s'étant progressivement réduit. Pour mener à bien cette étude nous avons procédé à une recherche par mots-clefs, dans les rapports annuels de la CNIL ainsi que dans le moteur de recherche du site Légifrance. Nous avons retenu le terme général de *secret* pour effectuer notre recherche de sorte à pouvoir juger par nous-même les éléments qu'il importait de souligner. En outre, dans le discours de la CNIL l'expression « secret médical » est employée tantôt pour qualifier le secret professionnel médical, tantôt pour désigner l'état de secret, c'est-à-dire le « secret médical » objet de la protection juridique. Une recherche à partir du mot-clef « secret » nous permet donc également d'interpréter le sens dans lequel l'expression est utilisée. S'agissant de la recherche des délibérations sur Légifrance, la recherche par mots-clefs pouvant comporter d'important biais, nous avons procédé par années, en recherchant toutes les délibérations ayant trait au traitement des données de santé ou au traitement de données à caractère personnel mis en œuvre par une structure médicale, médico-sociale ou par des professionnels de santé. Partant nous avons pu constater que la confidentialité et donc la définition des personnes pouvant avoir accès aux données traitées dans le domaine de la santé est déterminée au regard de la soumission au secret professionnel **(A)**. D'autres mécanismes sont parfois plébiscités par la CNIL lorsque les personnes qui devraient pouvoir accéder aux données ne sont pas soumises au secret professionnel **(B)**.

A - L'assujettissement au secret professionnel un gage de confiance suffisant ?

223. Contextualisation. Jusqu'à l'entrée en vigueur de la loi du 4 mars 2002 aucun texte ne déterminait comment les informations devaient circuler. Seul le texte d'incrimination de l'article 226-13 du Code pénal[1063] servait de fondement au secret professionnel. C'est à partir

---

une procédure de sanction : CE, 21 juin 2018, n° 416505, *tables Rec. Lebon*). Enfin, les autorisations où les refus d'autorisation de traitement de données, dans les rares hypothèses où les formalités préalables ont été maintenues, consistent également en des actes administratifs décisoires présentés comme un pouvoir de police administrative (P. LIVET, *Autorisation administrative préalable et les libertés publiques*, LGDJ, 1974, p. 20, Pp. 186-188 ; E. PICARD, *La notion de police administrative*, LGDJ, 1984, p. 174 et svt.). En matière de traitement des données de santé le régime d'autorisation est maintenu pour les traitements de données à caractère personnel dans le domaine de la santé présentant un intérêt public, lorsque ces traitements ne sont pas conformes aux référentiels élaborés par la CNIL (art. 54 de la LIL) il en est de même pour ceux dont la finalité est ou devient la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention qui ne correspondent pas aux référentiels (art. 61 de la LIL).

[1063] Et l'ancien article 378 du Code pénal pour les décisions rendues avant 1994.

de la formulation de l'interdit que la CNIL a d'abord déterminé qui pouvait avoir accès à quelles données. Aussi, durant de nombreuse années la CNIL a porté, au visa de ses décisions, la mention de cet article. Le seul texte d'incrimination ne pouvant suffire à répondre à des problématiques relevant de la transmission d'informations ou de données par ou entre des personnes soumises au secret ou concernant l'accès à des données issues d'informations couvertes par le secret, la Commission s'est appuyée sur la jurisprudence et sur d'autres textes spéciaux pour rendre ses décisions. Son attention s'est portée sur le fait de savoir si les personnes auxquelles il était prévu de donner accès aux données, par transmission ou par accès direct, étaient soumises au secret professionnel. A titre informatif, il faut noter que les traitements sur lesquels l'autorité a eu à se prononcer étaient, dans les années 1980, principalement mis en œuvre par des établissements publics ou par l'Etat. Cela s'explique par le contexte technologique de l'époque et les finalités assignées à la loi informatique et libertés à cette époque. Enfin, une autre remarque doit être formulée quant à la méthode. Notre analyse sur ce point prend fin en 1994, date à laquelle la majorité des acteurs pour lesquels des doutes pouvaient subsister, sont astreints au secret professionnel par les textes ou parce que d'autres mécanismes ont permis de suppléer au secret professionnel. Autrement dit, au fil du temps, la CNIL a de moins en moins été amenée à se poser la question de savoir si certains acteurs intervenant dans le traitement des données issues de la relation de soins étaient ou non soumis au secret professionnel[1064].

224. Doctrine de la CNIL. Le premier traitement de données auquel nous nous sommes intéressés, qui est aussi une « affaire » dans la mesure où sa mise en œuvre avait provoqué de vives réactions[1065], est celui du fichier dit « GAMIN »[1066]. Indépendamment de l'aspect politique du fichier, la CNIL a eu à formuler son avis sur les personnes pouvant accéder à ce fichier, lequel contenait des données couvertes par le secret. Il s'agissait notamment des personnes intervenant dans le cadre de la protection maternelle et infantile. La commission relevait, sans que cela ne

[1064] Nous traiterons ultérieurement de la généralisation du secret professionnel, ce qui permettra de compléter les présents développements.
[1065] V. par exemple : C. HOFFSAES « Le système gamin : Erreur technocratique ou premier pas vers un fichage généralisé ? », *Esprit*, Mai 1982, n° 65, Pp. 22-42. Nous nous tiendrons, pour l'heure, éloignés des considérations d'ordre politique, que nous évoquerons ultérieurement.
[1066] Délibération n°81-74 du 16 juin 1981 : Il s'agissait du traitement automatisé des certificats de santé établis au huitième jour, neuvième et vingt-quatrième mois de la vie de l'enfant qui avait pour finalité la conduite de la protection maternelle et infantile.

soulève de contestation de sa part : « *Que les seuls destinataires des informations traitées sont le médecin chargé de la P.M.I., les personnes de son service ou des organismes ayant passé avec le département une convention sur la gestion d'un service de P.M.I.* ***tous agents tenus au secret professionnel*** » elle relevait également « […] *qu'une demande formulée par des personnes ou services extérieurs à la PMI ne peut recevoir satisfaction que dans la mesure où le demandeur est lui-même tenu au* ***secret médical*** »[1067].

Dans le rapport de la Commission pour l'année 1980-1981 et concernant le même traitement, l'on trouve encore un exemple de cette approche : « *Le secret dont l'article 378 du Code pénal sanctionne la violation lie non seulement les médecins, mais la plupart de leurs auxiliaires ; il ne s'étend pas aux informaticiens* »[1068]. Sans qu'elle n'explique la raison de cette mention, il n'est pas incohérent de soutenir qu'il s'agit d'une confirmation de ce que le secret professionnel est le critère premier de la détermination des tiers autorisés en même temps qu'une invitation à légiférer en ce sens afin de permettre l'accès des informaticiens aux données.

Durant l'année 1986 s'agissant d'un projet d'enquête épidémiologique dans le cadre de la recherche sur le Sida[1069], la CNIL précisait qu'il lui incombait de vérifier que les mesures prises par le responsable de l'étude permettait le respect du « secret médical » ainsi que de la loi informatique et libertés afin de s'assurer que ces mesures constituaient des garanties appropriées requises par l'article 6 de la Convention du Conseil de l'Europe[1070] au regard duquel « *les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées* ». Les références à la Convention sont nombreuses dans les rapports de la CNIL depuis sa ratification. Il faut noter, concernant spécifiquement l'article 6, que dans le cadre de la Convention, il n'est fait mention que des « *garanties appropriées* ». Le secret professionnel

---

[1067] *Ibid.* Le rapport de la CNIL est un peu plus précis : « *Que s'il peut communiquer certaines indications portées sur les certificats de santé aux membres de son équipe médicosociale, c'est uniquement en vue de la protection de la mère et de l'enfant ; qu'une demande formulée par des personnes ou services extérieurs à la PMI ne peut recevoir satisfaction que dans la mesure où le demandeur est lui-même tenu au secret médical* » (CNIL, *Rapport d'activité*, 1980-1981, p. 228). L'expression *secret médical* parait désigner le secret professionnel et sans doute plus précisément le secret professionnel des professionnels de santé.

[1068] CNIL, *Rapport d'activité*, 1980-1981, p. 27.

[1069] CNIL, *Rapport d'activité 1986*, p. 225.

[1070] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28. I.1981.

n'étant pas le seul moyen de protéger ses données particulières, la possibilité est laissée aux Etats de prévoir les modalités de cette protection, par des moyens juridiques ou techniques. Ainsi, le secret professionnel se présenterait comme un moyen de garantir la confidentialité au sens de ce premier instrument européen de protection des données.

En 1987, s'agissant de l'accès, par des professionnels de l'informatique, des données issues de la relation de soins, la CNIL formulait ce point de vue : « *Il paraît sans doute illusoire de vouloir réserver aux seules personnes astreintes au secret médical l'exploitation informatique de données médicales. L'informaticien est nécessairement appelé à participer à la gestion de ces systèmes* »[1071]. Outre le critère de la nécessité qui est déjà en question ici, il convient de remarquer que la question porte également sur la soumission au secret professionnel des informaticiens, l'expression « secret médical » visant ici le secret professionnel médical. En effet, la Commission relève ensuite que si les informaticiens fonctionnaires sont soumis au secret professionnel, une telle affirmation n'est pas possible pour les employés de la société en cause dans le traitement qui lui était soumis, ce qui empêche, *a priori*, d'admettre qu'ils puissent être des tiers autorisés[1072]. Ce raisonnement vient encore confirmer son approche : seuls les informaticiens qui ne sont pas fonctionnaires et donc non soumis au secret sont des tiers non-autorisés.

Dans son rapport de 1988, à propos de l'informatisation du secteur libéral de la santé, la CNIL constate un mouvement d'informatisation croissant et remarque des pratiques consistant par exemple à « *recourir à l'outil informatique et même aux réseaux télématiques pour transmettre leurs factures subrogatoires aux caisses de sécurité sociale, via parfois des organismes intermédiaires constitués à cet effet* […] »[1073]. En raison de ces pratiques, elle souligne, en faisant usage de la litote : « *Ces systèmes qui se proposent de favoriser la communication entre tous les acteurs du système de santé et de faciliter ainsi la disponibilité des informations médicales, ne sont pas sans soulever de sérieuses questions de fond tenant au*

[1071] CNIL, *Rapport d'activité 1987*, p. 98.
[1072] Elle procède, au passage, à une extension de l'article 13 de la loi informatique et libertés qui, dans sa version initiale, prévoyait que « *Les informaticiens appelés, soit à donner les renseignements à la commission, soit à témoigner devant elle, sont déliés en tant que de besoin de leur obligation de discrétion* » pour en déduire que les informaticiens sont soumis à une obligation générale de discrétion (*Ibid.*).
[1073] CNIL, *Rapport d'activité 1988*, p. 136.

respect d'un secret médical conçu ici de façon très élargie »[1074]. L'on constate toutefois qu'elle autorise ou prononce des avis favorables à l'égard de certains traitements de données couvertes par le secret professionnel dès lors que les personnes dont il est prévu qu'elles accèdent aux données sont soumises au secret professionnel[1075].

Enfin, il faut également remarquer qu'à partir de 1989 la Commission prend acte de la volonté des pouvoirs publics de développer l'informatique hospitalière. Elle rendra des avis sur certains traitements qui serviront de modèles types de traitement de données ayant pour finalité la gestion médicale et administrative des établissements publiques. Les établissements adoptant ces modèles bénéficieront d'un allègement des formalités préalables[1076]. Tous ces traitements sont donc soustraits à notre analyse à partir de cette période.

Au cours de l'année 1994 l'analyse d'un dossier a également attiré notre attention : il s'agissait de l'examen d'un traitement de données déclaré à la Commission et relatif à la mise en œuvre d'un dossier informatisé des patients hospitalisés à domicile. La coordination de la prise en charge par des intervenants professionnels de santé mais également assistants sociaux et aides ménagères été assurée par une association. Les informations saisies durant la journée par ces intervenants « *sont automatiquement* [transmises] *par le réseau téléphonique commuté au site central de l'association, lui permettant ainsi de gérer les temps de passage des intervenants, de mettre à jour les dossiers de soins, d'éditer les commandes, d'informer les surveillantes de nuit et le médecin coordinateur* »[1077]. Afin de s'assurer du respect du secret professionnel la Commission avait demandé que « *que chaque professionnel, administratif ou médical, acteur du système* »[1078] n'ait accès qu'aux données nécessaires à sa mission. Sans qu'elle précise davantage ce qu'elle entend par *acteurs du système* l'on se pose légitimement la

---

[1074] CNIL, *Rapport d'activité 1988*, p. 137.
[1075] CNIL, *Rapport d'activité 1988*, p. 423.
[1076] Délibération n° 89-51 du 13 juin 1989 portant avis sur le projet de décision du directeur du Centre hospitalier général de Mulhouse concernant la mise en œuvre d'un traitement relatif à la gestion des services médicaux ; Délibération n° 89-56 du 27 juin 1989 portant avis sur le projet de décision du directeur du Centre hospitalier régional de Dijon concernant la mise en œuvre d'un traitement relatif à la gestion administrative des malades (PAGE-MALADES) ; Délibération n° 89-05 du 24 janvier 1989 portant avis sur le projet de décision du directeur général du Centre hospitalier régional de Rennes concernant la mise en œuvre d'un traitement dont la finalité principale est la gestion des rendez-vous médicaux (GEREMI) et constituant un modèle type ; CNIL, *Rapport d'activité 1989*, p. 199 et svt. Ces traitements sont ensuite pris sur le fondement de l'ancien article 17 de la loi informatique et libertés et soumis à une déclaration de conformité.
[1077] CNIL, *Rapport d'activité 1994,* p. 321.
[1078] *Ibid.* p. 321.

question de savoir si les aides ménagères sont des acteurs du système susceptibles de recevoir des informations, et le cas échéant, la nature des informations dont elles peuvent être destinataires. Il nous semble ainsi qu'elle admette que ces différents acteurs sont soumis au secret professionnel.

225. Remarques. L'on constate au travers des quelques exemples sélectionnés que la CNIL a porté son attention sur le fait de savoir si les personnes qui étaient supposées avoir accès aux données étaient bien soumises au secret professionnel. L'on pressent à la lecture de nos développements qu'une question sous-jacente demeure en suspens, celle de la justification. En effet, qu'un tiers soit astreint au secret professionnel n'a jamais été une cause justificative de violation du secret professionnel, le seul critère qui devrait être pris en compte serait alors celui de l'existence d'un fait justificatif. Pourtant la jurisprudence de la Cour cassation confirme que la soumission au secret professionnel est un critère déterminant pour distinguer les personnes qualifiées pour recevoir les données des tiers non-autorisés[1079]. Elle a même parfois admis que la clause de confidentialité inscrite dans le contrat travail suffisait à considérer que la personne était qualifiée pour accéder aux données[1080]. La définition *a contrario* qui est désormais faite

---

[1079] Un arrêt rendu par la chambre criminelle de la Cour de cassation le 30 octobre 2001 (Crim., 30 Octobre 2001, n° 99-82136 ; *Gaz. Pal.* 2002, II, p. 1476 ; *Gaz. Pal.* 2002, n° 297, p. 40, *obs.* A. MOLE ET H. LEBON *; JCP E* 2002*,* n° 23, p. 888*, obs.* M. VIVANT ET N. MALET-POUJOL ; Comm. Com. élect. 2002, n° 11, comm. 14, note A. LEPAGE) vient étayer cette interprétation. Il pose, selon Madame Malet-Poujol et Monsieur Vivant « *la difficile question du secret partagé* » (M. VIVANT, N. MALET-POUJOL, « Droit de l'informatique », *JCP E 2002,* n° 23, p. 888. Cette remarque rejoint nos propos sur les travaux de la doctrine, les auteurs mentionnent *le secret partagé*, ce qui laisse supposer une unité entre l'exception au secret professionnel et la confidentialité telle que prévue par la loi informatique et libertés). Dans cette affaire, le président et le directeur d'un syndicat interprofessionnel de médecins du travail avaient fait procéder à l'informatisation des services. Les médecins y traitaient les données de leurs patients, sous forme de dossiers informatisés. Il était reproché à ces derniers un manquement à la sécurité et à la confidentialité des traitements sanctionné à l'article 226-17 du Code pénal et la violation du secret professionnel au motif que chacun des médecins utilisateurs et leurs secrétaires, mais aussi des personnels administratifs, pouvaient accéder aux fichiers créés par d'autres médecins. La Cour de cassation confirme que l'infraction de violation du secret professionnel n'est pas constituée dès lors qu'il ne s'agit pas de révélations volontaires. Il s'agissait ensuite de savoir si les médecins, leurs secrétaires et les personnels administratifs étaient des personnes non autorisées au sens de l'article 226-17 du Code pénal. La Cour de cassation valide le raisonnement des juges du fond selon lequel les médecins et leurs secrétaires, étant tous soumis au secret professionnel, ne peuvent être considérés comme des tiers non autorisés.

[1080] Crim., 3 juin 2008, n° 08-80.467 : *JCP E* 2009, 1674, n° 27, obs. M. VIVANT, N. MALLET-POUJOL et J.-M. BRUGUIERE : L'arrêt porte sur un pourvoi contre la décision d'une chambre de l'instruction de cour d'appel ayant prononcé un non-lieu du chef d'infraction à la législation informatique et libertés. Dans une plainte déposée par un syndicat interprofessionnel de médecine du travail[1080] contre personne non désignée, la partie civile arguait, entre autres, d'une violation de l'article 226-17 du Code pénal en ce que les informaticiens en charge de la maintenance du système avaient accès aux données de santé contenues dans les dossiers médicaux des patients. La Cour considère que c'est à bon droit que la chambre de l'instruction avait prononcé un non-lieu. Les informaticiens ne pouvant être regardés comme des tiers non autorisés dans la mesure où ils ont « *pu avoir accès*

des « tiers » dans le RGPD, c'est-à-dire toutes les personnes à l'exclusion, notamment, du responsable du traitement, du sous-traitant et des personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel, ne suffit pas à éclairer cette dernière question. Nous y reviendrons lorsque nous traiterons du critère de nécessité. Il convient, avant cela, de souligner qu'à l'occasion de certains contrôles la CNIL a parfois utilisé des mécanismes surprenants afin d'autoriser l'accès ou la transmission des données à des personnes intervenant dans le traitement des données issues de la prise en charge médicale, voire médico-sociale, des personnes tandis qu'elles n'étaient pas soumises au secret professionnel.

B - Les palliatifs au secret professionnel

226. Le secret professionnel, un critère suffisant mais non nécessaire. Nous avons constaté, à la lecture de décisions et avis de la CNIL dans les premiers temps de son existence, que le maintien de la confidentialité ne consistait pas uniquement à vérifier que les personnes pouvant avoir accès aux données étaient astreintes au secret professionnel. Dans certaines hypothèses, la CNIL a été pour le moins innovante dans la mesure où elle a cherché à générer la confiance en proposant la mise en œuvre de mécanismes qu'elle semble considérer comme équivalents au secret professionnel.

227. Des palliatifs contractuels. Parmi les autorisations de traitement rendues par la Commission concernant l'accès aux données issues de la prise en charge des personnes dans le système de santé, la Commission s'est notamment prononcée, en 1986 sur un traitement de données relatif à la gestion administrative et médicale des malades mis en œuvre par un centre hospitalier. A propos de l'intervention de techniciens d'une entreprise privée, et donc extérieure à l'établissement hospitalier, qui devaient se voir autoriser l'accès au traitement de données, la Commission autorise le traitement « *Considérant qu'une clause sur les sécurités doit être incluse dans le contrat conclu avec ce façonnier de manière à lui rappeler ses obligations de*

à des données protégées par le secret médical en leur qualité de super administrateur » et puisqu'ils ont « *agi dans le cadre de leur activité de consultant en informatique* » au titre de laquelle ils devaient assurer le fonctionnement du logiciel. L'arrêt précise en outre qu'ils se trouvaient liés à l'entreprise par un contrat de travail comportant une clause de confidentialité ce qui justifie qu'ils ne puissent être qualifiés de tiers non autorisés.

secret ainsi que les responsabilités encourues en cas de divulgation des informations qui lui sont confiées »[1081]. Pour la CNIL la clause de confidentialité incluse dans le contrat consiste en une garantie suffisante pour considérer que les techniciens sont autorisés à accéder aux données.

A propos des informaticiens, la Commission constate, à l'occasion de son rapport annuel de 1987, que si les informaticiens fonctionnaires sont soumis au secret professionnel, il est impossible de l'affirmer pour les informaticiens de sociétés privées[1082]. Afin de tout de même autoriser les traitements de données couvertes par le secret professionnel médical, elle explique que « *des garanties juridiques précises peuvent être instaurées afin de mieux responsabiliser les informaticiens* »[1083]. Elle propose que soit rédigé un « *engagement à l'obligation de discrétion et de sécurité* […] *précisant notamment que les données traitées étaient couvertes par le secret professionnel* »[1084]. Elle complète : « *Cet engagement devra être complété par la mention des sanctions pénales encourues au titre de l'art. 378 du Code pénal* »[1085]. La solution proposée par la CNIL est surprenante dans la mesure ou un contrat ne peut emporter désignation des personnes soumises au secret professionnel : cela reviendrait à nier le principe de légalité criminelle. L'on entrevoit là encore le critère de nécessité qui guide la démarche de la CNIL ; nous y reviendrons.

Durant l'année 1999 la Commission a eu à connaître de deux demandes de diffusion de données issues du PMSI à des fins d'études de l'activité hospitalière tant publique que privée par des organismes de presse. Il s'agissait de transmettre à ces organismes les résumés de sorties anonymes qui nourrissent le PMSI, et qui, malgré leur appellation, comportaient un risque de réidentification des personnes. Les données étaient donc considérées comme indirectement nominatives[1086]. Afin d'autoriser le traitement des données par ces entreprises privées, la

---

[1081] Délibération n° 86-112 du 25 novembre 1986 portant avis sur le projet de décision du directeur du Centre hospitalier général d'Auch, concernant la mise en œuvre d'un traitement relatif à la gestion administrative et médicale des malades (GAMMA - Filière PROFILS) Demande d'avis n° 104.209.

[1082] Elle procède, au passage, à une extension de l'article 13 de la loi informatique et libertés qui, dans sa version initiale, prévoyait que « *Les informaticiens appelés, soit à donner les renseignements à la commission, soit à témoigner devant elle, sont déliés en tant que de besoin de leur obligation de discrétion* » pour en déduire que les informaticiens sont soumis à une obligation générale de discrétion (*Ibid.*).

[1083] CNIL, *Rapport d'activité 1987*, p. 99.

[1084] *Ibid.* p. 100.

[1085] *Ibid.* p. 100.

[1086] « *les* « résumés de sortie anonymes *» comportent des données individuelles dont l'exploitation informatique ne permet pas, à elles seules, d'identifier les patients concernés ; que toutefois ces données sont susceptibles, dès lors qu'il serait procédé à leur rapprochement avec d'autres informations ou fichiers comportant l'identité de personnes hospitalisées, de déterminer, par recoupement, le motif d'hospitalisation de celles-ci* » (Délibération n°

Commission demanda la suppression de certaines mentions pouvant faciliter la réidentification des personnes concernées[1087]. Afin de s'assurer encore, que, même en cas de réidentification du fait d'informations que les personnes amenées à traiter les données détiendraient par ailleurs sur un individu, la Commission demanda au directeur de la rédaction de ces organes de presse de veiller « *à respecter et à faire respecter le secret des informations cédées par toutes les personnes susceptibles de travailler sur ces données, ces personnes étant astreintes par écrit au secret professionnel* »[1088]. La mention d'une soumission au secret *par écrit* est cette fois explicite. Cette solution que nous qualifions de *palliative* est ensuite utilisée à de nombreuses reprises dans le cadre de traitement autorisé par la Commission[1089].

228. Méthode du bricolage. Le terme de *bricolage*, tel que nous l'utilisons ici n'est pas péjoratif : il renvoie à la méthodologie développée par Claude Levy-Strauss dans *la pensée sauvage*[1090] : « *Le bricoleur est apte à exécuter un grand nombre de tâches diversifiées* ; […] *il ne subordonne pas chacune d'elles à l'obtention de matières premières et d'outils, conçus et procurés à la mesure de son projet : son univers instrumental est clos, et la règle de son jeu est*

99-061 du 21 décembre 1999 portant autorisation de mise en œuvre par la revue « Sciences et avenir » d'un traitement de données personnelles de santé à des fins d'analyse statistique des pratiques et des activités de soins).

[1087] A cette fin avait été supprimée à la fois la mention du mois de sortie de la personne concernée, ainsi que son âge précis, remplacé par une tranche d'âge (*Ibid.*).

[1088] Délibération n° 99-061 du 21 décembre 1999 portant autorisation de mise en œuvre par la revue « Sciences et avenir » d'un traitement de données personnelles de santé à des fins d'analyse statistique des pratiques et des activités de soins.

[1089] Où il encore question de soumettre contractuellement au secret professionnel afin d'accéder aux données : Délibération n° 00-001 du 13 janvier 2000 portant autorisation de mise en œuvre par le Comité médical paritaire local des médecins généralistes de Paris d'un traitement de données personnelles de santé ayant pour objet l'évaluation des pratiques médicales de prescription dans la rhino-pharyngite de l'enfant ; Délibération n° 00-002 du 13 janvier 2000 portant autorisation de mise en œuvre par l'Agence régionale de l'hospitalisation d'Île-de-France d'un traitement de données personnelles de santé à des fins d'évaluation des pratiques de soins en urgence face à un infarctus du myocarde ; Délibération n° 00-003 du 13 janvier 2000 portant autorisation de mise en œuvre par la Fédération des établissements hospitaliers et d'assistance privés à but non lucratif d'un traitement de données personnelles de santé à des fins d'analyse statistique des pratiques et des activités de soins). Voir encore : Délibération n° 00-001 du 13 janvier 2000 portant autorisation de mise en œuvre par le Comité médical paritaire local des médecins généralistes de Paris d'un traitement de données personnelles de santé ayant pour objet l'évaluation des pratiques médicales de prescription dans la rhino-pharyngite de l'enfant ; Délibération n° 00-002 du 13 janvier 2000 portant autorisation de mise en œuvre par l'Agence régionale de l'hospitalisation d'Île-de-France d'un traitement de données personnelles de santé à des fins d'évaluation des pratiques de soins en urgence face à un infarctus du myocarde. Délibération n° 00-003 du 13 janvier 2000 portant autorisation de mise en œuvre par la Fédération des établissements hospitaliers et d'assistance privés à but non lucratif d'un traitement de données personnelles de santé à des fins d'analyse statistique des pratiques et des activités de soins.

[1090] C. LEVY-STRAUSS, *La pensée sauvage*, Plon, 1962.

de toujours s'arranger avec les "moyens du bord" »[1091]. C'est pourquoi « *les éléments que collectionne et utilise le bricoleur sont "précontraints"* »[1092]. Et, « *parce que la composition de l'ensemble n'est pas en rapport avec le projet du moment* »[1093], les outils du bricoleur sont « *le résultat contingent de toutes les occasions qui se sont présentées de renouveler ou d'enrichir le stock, ou de l'entretenir avec les résidus de constructions et de destructions antérieures* »[1094]. Cela « *implique des capacités d'improvisation et d'adaptation qui permettent de faire face au caractère contingent de l'expérience et de ses défis* »[1095], surtout « u*ne certaine instrumentalité sert de contrainte première aux pratiques bricolantes* »[1096]. Sous les aspects du syllogisme juridique[1097], c'est bien à un *bricolage* que la CNIL procède parfois en utilisant les ressources disponibles au grès des espèces et des problématiques de terrain propres à chaque espèce. La méthode du *bricolage* n'est pas inconnue des réflexions sur le droit, c'est notamment celle – car c'est bien comme une méthode et non comme un chaos que Claude Levy-Strauss explique le bricolage[1098] – employée par Vincent Forray et Sébastien Pimont dans leur essai sur la décriture du droit[1099] et dont les auteurs affirment qu'elle permet « *des glissements et rapprochements, au lieu de recours exclusivement aux opérations de la logique juridique (inductions, déductions, inférences, pratiquées par les juristes dans le domaine doctrinal ou académique)* »[1100]. Il s'agit d'un *« mode alternatif de connaissance* »[1101] dans lequel « *la façon de coordonner les actions pour produire un savoir dépend du but que celui qui agit s'est fixé.*

[1091] *Ibid.* p. 27
[1092] *Ibid.* p. 29
[1093] *Ibid.* p. 29
[1094] *Ibid.* p. 29
[1095] D. MEUNIER, F. LAMBOTTE, S. CHOUKAH, « Du bricolage au rhizome : comment rendre compte de l'hétérogénéité de la pratique de recherche scientifique en sciences sociales ? », *Questions de communication* 2013, n° 23, p. 345-366, spéc. n° 9.
[1096] *Ibid.* n° 10
[1097] Nous pointons ici l'utilisation du visa, la mention de l'article du Code pénal sanctionnant la violation du secret professionnel étant inscrit au visa de toutes les délibérations relatives au traitement des données à caractère personnel ou de santé issues de la relation de soin avant la loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.
[1098] Claude Lévy-Strauss intitule le premier chapitre de son ouvrage « science du concret » (C. LEVY-STRAUSS, *La pensée sauvage*, Plon, 1962, p. 3). L'auteur oppose la méthode de *l'ingénieur* et du *bricoleur*, le premier se fondant « *sur l'ajustement des connaissances à un ordre rationnel (la manière moderne) ; l'autre sur la perception et l'imagination* » (V. FORRAY et S. PIMONT, *Décrire le droit...et le transformer. Essai sur la décriture du droit*, coll. Méthode du droit, Dalloz, 2017, p. 78).
[1099] V. FORRAY et S. PIMONT, *Décrire le droit…et le transformer. Essai sur la décriture du droit*, coll. Méthode du droit, Dalloz, 2017.
[1100] *Ibid.* p. 78 n° 91.
[1101] *Ibid.* p. 83, n° 97.

Ce qui diffère de l'idée selon laquelle elle dépendrait du but à atteindre, abstraitement fixé ou fixé a priori »[1102].

229. La méthode du bricolage n'est pas seulement mobilisable à des fins de connaissance du droit. Benoît Frydman, dans son *petit manuel pratique de droit global*[1103], évoque le bricolage pour décrire l'utilisation que les acteurs font des instruments juridiques dans un environnement global. Lorsqu'elle propose aux responsables de traitement la mise en œuvre de *garanties* destinées à pallier l'absence d'astreinte au secret professionnel et donc également propre à générer la confiance, la CNIL se saisit de tous les instruments disponibles pour parvenir au « juste équilibre » qui caractérise sa mission de régulation.

Si le *bricolage* comme méthode d'utilisation des matériaux juridiques renvoie, en miroir, à l'interprétation pragmatique ou réaliste des textes[1104], la CNIL se place comme acteur et non plus seulement comme interprète du droit. Elle élabore une stratégie avec les instruments juridiques à sa disposition[1105], mais également par la mise en œuvre d'instruments non juridiques.

[1102] *Ibid.* p.

[1103] B. FRYDMAN, *Petit manuel pratique de droit global*, L'économie de marché est-elle juste ? vol. 4, coll. L'académie en poche, Academie Royale de Belgique, 2014, p. 103 et svt.

[1104] V. FORRAY et S. PIMONT, *Décrire le droit...et le transformer. Essai sur la décriture du droit*, *op. cit.* p. 80, n° 93. Ce parallèle est notamment illustré par la présentation que Duncan Kennedy fait du « travail juridique de l'interprète » : « *Le travail présuppose la médiation d'un matériau que le travailleur façonne. Dans le cas du travail juridique, le matériau est l'ensemble des éléments juridiques qui sont considérés comme pertinents pour établir la signification de la norme en sorte qu'elle soit applicable aux faits de l'espèce* ». (D. KENNEDY, « Une alternative phénoménologique de gauche à la théorie de l'interprétation juridique Hart / Kelsen », *Jurisprudence – Revue critique* 2010, Université de Savoie, Lextenso éditions, p. 24 – *Adde* V. FORRAY et S. PIMONT, *Décrire le droit…et le transformer. Essai sur la décriture du droit, op. cit.*, p. 81). Le parallèle est également opéré par Véronique Champeil-Desplats lorsqu'elle évoque les difficultés de traiter des méthodes et méthodologies de la connaissance en droit. L'auteur cite l'ancien juge à la Cour suprême Benjamin Nathan Cardozo qui explique que si le juge dispose « *d'outils (ici la méthode philosophique, ou logique ; la méthode historique ou évolutionniste ; le recours à la tradition ou à la coutume ; la méthode sociologique, ou téléologique)* […]*, ni le choix de l'instrument, ni la manière de l'utiliser, ne s'imposent mécaniquement* » (B. N. CARDOZO, *La nature de la décision judiciaire (1921)*, Dalloz, 2011, p. 27). Véronique Champeil-Desplats utilise cette illustration pour souligner que le discours savant sur le droit (méta-métadiscours) procède également d'une part de « *d'intuition, d'imprévu, de hasard, d'arrangement, d'ajustement ou encore de savoir-faire singulier qui peut s'y glisser* » et fait référence au *bricolage* de Claude Levy-Strauss (V. CHAMPEIL-DESPLATS, *Méthodologies du droit et des sciences du droit*, coll. méthode du droit, 2e éd., Dalloz, 2016, n° 9-10).

[1105] Lorsqu'elle affirme par exemple que des « *garanties juridiques peuvent être trouvées* » pour permettre à des informaticiens d'accéder aux données couvertes par le secret professionnel médical afin d'en assurer la soutraitance et qu'elle procède alors en *passant en revue* tous les instruments permettant de faire peser sur eux une obligation *équivalente* au secret professionnel (CNIL, *Rapport d'activité 1987*, p. 99). Elle procède par rapprochement entre obligation de discrétion et secret professionnel. Rapprochement d'autant plus intuitif qu'il découle de la proximité sémantique entre discrétion et secret.

L'analyse que nous venons de proposer ne peut être complète sans considération du second critère permettant de déterminer qui sont les personnes qualifiées pour connaitre des données : la nécessité. C'est à partir de ce dernier élément que notre étude prendra sens car il permettra de mettre en perspective l'interprétation de la Commission. Si la confiance est un critère de détermination des personnes qualifiées pour prendre connaissance des données (par le biais d'un accès ou d'une transmission), la circulation des informations ou des données couvertes par le secret professionnel ne peut en principe être justifiée qu'en vertu d'une autorisation ou d'une obligation de la loi.

§ 2 - La nécessité de l'accès aux données : évolution légale et interprétation extensive de la CNIL

230. Le critère de nécessité a longtemps permis à la CNIL de déterminer en amont de la mise en œuvre des traitements, les cas dans lesquels la liste des destinataires contenait des tiers non-autorisés, qu'il s'agisse de leur donner accès aux données traitées ou d'autoriser que celles-ci leurs soient transmises. La CNIL opérait et opère encore, dans une moindre mesure, par le biais de son intervention *ex ante*, un contrôle de cette nécessité. Or, il convient de rappeler que la nécessité ne se définit que par rapport à une finalité, un but ou une situation. S'agissant du traitement des données à caractère personnel dans le domaine de la santé, ces données étant couvertes par le secret, la nécessité semble devoir s'apprécier au regard des faits justifiant la violation du secret professionnel. En ce sens, une personne ne serait qualifiée pour accéder aux données que parce que la loi ou le règlement autorise ou oblige la révélation et permet donc l'échange ou le partage des informations d'une personne soumise au secret déterminée vers une autre. Dans ce cas le législateur a d'ores et déjà déterminé quelles étaient les personnes dont les fonctions requéraient qu'elles aient accès aux informations ou aux données, et posé les conditions d'une révélation faisant ainsi obstacle à la consommation de l'infraction. L'on constate à la lecture de la doctrine développée par la CNIL au fil des ans qu'elle s'est attachée à vérifier l'existence de textes justifiant la révélation afin d'autoriser certains traitements de données **(A)**. Il apparaît toutefois que la CNIL a parfois apprécié la nécessité pour certaines personnes d'accéder aux données traitées en tenant compte des besoins du traitement au regard de sa finalité **(B)**.

A - Le contrôle par la CNIL de l'existence de faits justificatifs

231. Remarques préalables. Depuis les débuts de son existence la CNIL s'est placée en défenseur des droits et libertés des personnes dont les données sont traitées. Lorsque le régime attaché à la mise en œuvre des traitements de données était majoritairement celui des formalités préalables et, dans le domaine de la santé, celui de l'autorisation, la Commission a eu à examiner, notamment au travers des avis qu'elle a pu rendre, de nombreux projets de traitement. Elle s'est appliquée à vérifier l'existence de faits justificatifs permettant de justifier que certaines personnes soient inscrites sur la liste des destinataires. Notre analyse étant diachronique, la doctrine de la CNIL telle que nous l'avons exposée souligne des interprétations liées au droit positif – et parfois au contexte politique – en vigueur à chaque époque. Nous en préciserons par conséquent le contexte chaque fois que cela nous semblera nécessaire au regard de notre démarche. Le but de notre démonstration est de mettre en exergue un mouvement général, qui se vérifie indépendamment des époques et des changements législatifs et non de donner une vision exhaustive du droit positif de chaque époque.

232. Doctrine de la CNIL. Dans son rapport pour les années 1983-1984 la CNIL rappelle avec force l'absence de *secret partagé* entre les administrations en l'absence de tout fait justificatif. Elle affirme par ailleurs que les normes simplifiées qu'elle prend tiennent compte de cet interdit[1106]. Une question particulière a attiré l'attention de la Commission durant les années 1986 et 1987 à propos de la consultation par l'administration fiscale des *données médicales*[1107] détenues par les organismes de sécurité sociale. Il s'agissait de savoir si, en vertu de l'article, toujours en vigueur, L. 83 du Livre des procédures fiscales, il était possible de les compter parmi les destinataires de ces données. Elle s'appuie, pour donner sa position sur la

[1106] CNIL, *Rapport d'activité 1983-1984*, pp. 122-123.
[1107] C'est le terme employé alors. Il n'est nul besoin d'en cerner les contours, il convient simplement de souligner que ces données étaient issues de la relation de soins et donc couvertes par le secret.

question, sur un arrêt du Conseil d'Etat[1108] et une décision de tribunal administratif[1109], lesquels avaient décidé que la communication des copies des feuilles de maladie des clients d'un contribuable constituait une violation du secret professionnel. La CNIL raisonne alors par analogie et affirme que « *cette solution conduit à admettre que la consultation par un agent des services fiscaux d'un fichier d'un organisme de sécurité sociale, comprenant l'intégralité des renseignements portés sur les feuilles de maladie, contreviendrait aux dispositions de l'art. 378 précité* »[1110]. Selon cette interprétation les agents du fisc ne peuvent être des destinataires des données, pas plus qu'ils ne constituent des tiers autorisés. La solution s'explique, il nous semble, par la circonstance que le contrôle fiscal puisse être effectué sans que les agents de l'administration fiscale ne prennent connaissance des informations relatives aux patients d'un professionnel de santé[1111]. C'est à la lumière de la jurisprudence que la CNIL interprète la portée de l'article du livre des procédures fiscales.

Il faut ensuite souligner la position adoptée par la CNIL dans son rapport de 1989. Celle-ci est clairement critique à l'égard du décideur politique[1112]. Dans ce rapport, la

---

[1108] CE Ass. 12 mars 1982, *Conseil national de l'Ordre des médecins*, n° 11413, 11414,11466, 11099, 11100, 11451, *Rec. Lebon* 169 : « *Les dispositions de l'article 378 du code pénal s'opposent à ce que les membres des professions auxquelles elles s'appliquent fassent connaître à des tiers le nom des personnes qui ont eu recours à leurs services ou à leurs soins. En l'absence de toute disposition législative expresse il ne saurait être dérogé en faveur des agents des services fiscaux, bien qu'ils soient eux-mêmes tenus au secret professionnel, à la règle édictée par l'article 378* ».

[1109] TA Rennes, du 16 janvier 1985.

[1110] CNIL, *Rapport d'activité 1986*, p. 39 ; CNIL, *Rapport d'activité 1987*, p. 76.

[1111] Cette position du Conseil d'Etat s'étendait au nom des patients du médecin (CE 27 juill. 1984, req. n° 18281, *RJF* 11/1984, n° 693 ; CE 10 févr. 1988, req. n° 67016 , *RJF* 4/1988, n° 491) avant d'être assouplie et qu'il admette que les agents de l'administration fiscale pouvaient se faire communiquer des documents comprenant le nom des patients à condition qu'aucune autre mention ne figure sur les documents (CE 7 juill. 2004, req. n° 253711 , RJF 2004, n° 102).

[1112] Il faut noter quant au positionnement politique de la CNIL que celle-ci, entre 1979 et 1983, était présidée par Jacques Thyraud, tandis qu'à partir de 1984 la présidence sera assurée par Jacques Chauvet. Cela nous paraît devoir être relevé en raison de l'orientation politique de ces deux Présidents. Il nous semble en effet qu'il faille mentionner que J. THYRAUD, avocat de profession, avait notamment été un soutien de la loi Peyrefitte renforçant la sécurité et protégeant la liberté des personnes (Loi n° 81-82 du 2 février 1980 ; sur le soutien de J. THYRAUD à cette loi v. <http://www.senat.fr/senateur/thyraud_jacques59248p.html> dernière consultation le 14 oct. 2019) au sujet de laquelle A. PEYREFITTE avait affirmé « *La sécurité est la première des libertés* ». Cet élément de discours qui fera florès et à propos duquel M. DELMAS-MARTY souligne : « *En affirmant que la sécurité est la «* première des libertés *» le discours politique, largement relayé par les medias et les réseaux sociaux, dévalorise, voire ridiculise, les grands textes qui consacraient les libertés individuelles* » (M. DELMAS-MARTY, « Face au terrorisme global, la distinction entre guerre et paix a-t-elle encore un sens ? », *Constitutions* 2018, n° 3, p. 353). J. FAUVET est quant à lui journaliste de profession et directeur du journal *Le Monde* de 1969 à 1982 et notamment auteur de cinq articles relatifs à la magistrature pour lesquels il est inculpé en 1980 à la demande du Garde des Sceaux, A. PEYREFITTE. Ces précisions, ordinairement peu prises en compte par le juriste revêtent néanmoins un intérêt dès lors que l'on adopte une conception instrumentale du droit, conception dont l'aspect politique ne

commission consacre un développement assez long au « secret médical », intitulé « *un secret médical malmené* »[1113]. C'est la première fois, en dehors des quelques affirmations de « respect du secret médical », que la Commission prend une position ferme sur la question et même dénonce ce qu'elle considère être une dérive. Pour remédier au frein que constitue le secret professionnel médical au partage des données issues de la relation de soins avec les organismes en charge des statistiques publiques le législateur prévoyait, selon la CNIL « *une transmission de données médicales à l'INSEE qui fait perdre toute substance à la notion de secret médical* »[1114] et un consentement présumé du malade à l'utilisation de ces données pour des finalités de recherche et de statistiques, finalités éloignées de la prise en charge médicale pour lesquelles les données étaient collectées[1115]. A l'égard de ces modifications, la CNIL s'est prononcée pour que tout partage de données issues de la relation médicale avec d'autres professionnels que ceux prenant en charge le malade fasse l'objet d'une intervention législative propre à instaurer un fait justificatif en ce sens[1116].

Durant les années 1990 et 1991 la CNIL a été sollicitée pour se prononcer sur un projet de réforme relatif à la codification des actes de biologie médicale[1117] ainsi qu'à propos de la

---

peut être évacué. Une telle vision « […] *reflète* […] *une perspective particulièrement politique du droit. En effet, celui-ci devient le moyen qui permet par excellence de trancher, à l'arrière-plan, les conflits de valeurs, en faisant prévaloir les unes sur les autres dans la solution de questions particulières. Elle met donc en exergue l'insuffisance du point de vue purement interne du droit pour expliquer les phénomènes juridiques* » (D. RESTREPO AMARILES, « Conclusion », *in* B. FRYDMAN et C. BRICTEUX (ss. la dir.), *Le droit global*, coll. Penser le droit, Bruylant, 2017, 253-254). De la même manière F. OST souligne : « *Le droit si éminent soit-il, reste « lettre morte », s'il n'est réapproprié par ses destinataires, dans une démarche à caractère intrinsèquement politique – où l'on commence à entrevoir non seulement l'inéluctabilité du mélange des sphères, mais même leur évidente nécessité.* […] *cette lutte politique serait sans appui si elle ne pouvait se référer à un texte que chacun des protagonistes a dit vouloir respecter* » (F. OST, *A quoi sert le droit ? Usages, fonctions finalités*, coll. Penser le droit, Bruylant, 2016, spéc. p. 77).

[1113] CNIL, *Rapport d'activité 1989*, p. 14 et svt. Où il est notamment précisé *« Cette communication à une équipe de recherche qui, elle, ne concourt pas à la thérapeutique du patient et n'est pas couverte par le concept de secret médical partagé ».* Cette affirmation est remarquable dans la mesure où le secret partagé n'avait pas été conceptualisé à cette période, s'il était implicitement reconnu et admis par le juge civil et administratif ses contours restaient particulièrement incertains.

[1114] CNIL, *Rapport d'activité 1989*, p. 16.

[1115] *Ibid.* p. 16. Il faut souligner que la commission rappelle à cette occasion que le consentement n'est pas un fait justificatif de la violation du secret professionnel : « *La constitution de ces registres soulève en effet deux difficultés au regard respectivement du secret médical et des dispositions de la loi de 1978. La règle du secret médical pénalement sanctionnée par l'article 378 du Code pénal, est d'une application stricte, la Cour de cassation n'admettant pas la transmission de données médicales même avec l'accord des intéressés* […] ».

[1116]CNIL, *Rapport d'activité 1989*, p. 174.

[1117] Délibération n° 90-104 du 2 octobre 1990 relative au codage des actes de biologie médicale.

généralisation du projet de médicalisation des systèmes d'informations (PMSI)[1118]. Elle rappelle dans le premier cas qu'il n'existe pas de justification à une communication des informations envers les agents des caisses de sécurité sociale, autres que ceux chargés du contrôle médical[1119]. A propos du second elle rappelle qu'il n'existe pas de possibilité d'échange de données ou d'informations entre les professionnels de santé prenant en charge les patients et les médecins chargés de coder les actes : « *Elle a estimé que des transmissions de données médicales nominatives à des médecins ne participant pas au traitement thérapeutique des patients, ne peuvent être envisagées sans que de nouvelles dispositions législatives interviennent afin de compléter et modifier sur ce point* […] *l'article 378 du code pénal relatif au secret professionnel* »[1120]. Par ailleurs et de manière plus anecdotique au regard de l'aspect général des autres fichiers évoqués, la CNIL s'est opposée à la mise en œuvre d'un traitement de données ayant pour finalité la prévention des impayés des soins dentaires[1121]. Le traitement devait consister en un fichier au sein duquel chaque praticien pourrait inscrire le nom, le prénom, le lieu et la date de naissance des patients à l'égard desquels ils ont une créance. Les praticiens abonnés pourraient ensuite, en tapant le nom d'un client, savoir s'il était inscrit au fichier et donc s'il était débiteur à l'égard d'un autre professionnel. La CNIL avait estimé qu'un tel partage d'informations relevait d'une violation du secret professionnel puisque rien n'autorisait les professionnels à partager de ces informations.

Notons encore qu'en 1993 est expérimentée pour la première fois la carte SESAME-Vitale permettant notamment à un professionnel de santé d'avoir accès à l'historique des remboursements et donc de connaitre les traitements antérieurs reçus par le patient. La Commission affirme à ce sujet : « *La carte à mémoire ne peut se concevoir en effet que dans le cadre d'une notion renouvelée d'un secret médical partagé permettant, sous le contrôle du patient porteur de la carte, à tout médecin habilité de consulter le contenu entier de la carte, alors que traditionnellement, le praticien qui sollicite un avis ou oriente un patient vers un spécialiste, ne lui communique à cet effet qu'un nombre limité d'informations* ». Il faut souligner qu'à cette période le partage des informations entre professionnels de santé ne faisait l'objet

---

[1118] CNIL, *Rapport d'activité 1991*, p. 248 et svt.
[1119] Délibération n° 90-104 du 2 octobre 1990 relative au codage des actes de biologie médicale.
[1120] CNIL, *Rapport d'activité 1991*, p. 249.
[1121] Délibération n° 91-014 du 12 février 1991 portant sur la mise en œuvre d'un fichier de prévention de la multiplication des impayés dans la profession dentaire par la société APLITEL

que d'une reconnaissance implicite[1122]. De plus, il était encore admis que le médecin pouvait cacher certaines informations au malade[1123], ce qui explique cette conception du secret professionnel mais souligne au moins l'attachement de la CNIL au respect du régime attaché au secret professionnel médical.

A la même époque la CNIL a eu à se prononcer, suite de l'affaire du sang contaminé[1124], sur le traitement des données relatives à la traçabilité des produits sanguins[1125]. Cette période s'inscrivait dans les premières années de la mise en place de procédures de vigilance sur les produits sanguins et les médicaments[1126]. Obligation est alors faite aux professionnels de signaler les évènements indésirables engendrés par les transfusions sanguines[1127]. Toutes les personnes ayant à connaitre de ces informations sont soumises au secret professionnel[1128], et la CNIL s'est appliquée à vérifier que les fiches d'incident ne soient accessibles qu'aux

---

[1122] Longtemps la violation du secret professionnel ne connaissait aucune justification légale permettant aux professionnels de santé de partager ou d'échanger des informations en raison des nécessités de la prise en charge du malade. La jurisprudence avait néanmoins pu l'admettre dans le secteur hospitalier, car comme le remarque un auteur : « *En matière de médecine hospitalière, par exemple, le secret doit être considéré comme ayant par principe un caractère collectif, l'information étant d'emblée réputée confiée au service hospitalier et non à un praticien particulier* » (M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel, op.cit.*, n° 174. Dès 1972 le Conseil d'Etat affirme que « *le malade qui s'adresse à un organisme qui pratique la médecine collective s'adresse nécessairement à l'ensemble du personnel médical de cet organisme* » (CE, 11 fév. 1972, *Crochette* : Rec. p. 138 ; *R.D. publ.* 1972, p. 959, concl. G. GUILLAUME ; *Dr. social* 1972, p. 404 ; *D.* 1972.426, note M. LE ROY). La relation de soins étant conçue, dans ce cadre précis, comme liant l'établissement et le malade (S. PECHILLON, « L'adaptation du secret médical à l'hôpital : du silence à l'information médicale », in De l'hôpital à l'établissement public de santé, M.-L. MOQUET-ANGER (dir.), l'Harmattan, Paris, 1998, p. 317).

[1123] Il s'agissait de l'ancienne rédaction de l'article 42 du Code de déontologie de 1955 et de l'article 42 du Code de 1979 (sur ce point v. D. THOUVENIN, *Le secret médical et l'information du malade*, PUL, 1982, p. 58 et svt.).

[1124] Pour un rappel exhaustif de l'affaire : v. C. BYK, « Chapitre 4. *La jurisprudence française relative à la contamination des produits sanguins : une clarification de la perception juridique du sang humain* » *in La médecine en Procès*, *Journal International de bioéthique*, p. 49 ; B. KRIEGEL, « Chapitre 5. La responsabilité politique et pénale dans l'affaire du sang contaminé », *in La médecine en Procès*, op. cit., p. 59.

[1125] Sur le mise en œuvre d'un traitement de données des fiches d'incident transfusionnel (Délibération n° 96-014 du 12 mars 1996 relative à un projet d'acte réglementaire présenté par l'Agence française du sang concernant un traitement automatisé d'informations indirectement nominatives ayant pour finalité la gestion des fiches d'incident transfusionnel « GIFIT ») et sur un traitement permettant le suivi des produits sanguins labiles (Délibération n° 96-054 du 18 juin 1996 relative à un projet d'acte réglementaire présenté par l'Agence française du sang concernant un traitement automatisé d'informations nominatives ayant pour finalité l'expérimentation de la traçabilité des produits sanguins labiles).

[1126] Loi 93-5 du 4 janvier 1993 relative à la sécurité en matière de transfusion sanguine et de médicament ; Sur ce point v. notamment D. TABUTEAU, « La sécurité sanitaire, réforme institutionnelle ou résurgence des politiques de santé publique ? », *Les tribunes de la santé*, 2007/3, p. 87.

[1127] CSP, art. L. 666-12, ancien

[1128] *Ibid.*

professionnels prenant part à la procédure d'alerte[1129]. L'on peut encore citer quelques-unes des déclarations de la CNIL qui semblent attester qu'elle prête une attention particulière à l'existence de faits justificatifs pour déterminer les personnes qualifiées pour accéder aux données. Elle affirme, dans son rapport annuel pour 1998 que « *si des informations sont protégées par le secret professionnel ou par un secret particulier (médical, bancaire, fiscal, statistique), l'échange d'informations, c'est-à-dire leur divulgation à un organisme tiers, ne peut intervenir que si ce secret est préalablement levé par la loi* »[1130], et précise encore « *Quel serait le crédit d'un État qui assurerait que certaines informations sont protégées par le secret, si ce secret était en pratique et automatiquement éventé par le biais d'interconnexions entre organismes différents ? Quel serait d'ailleurs le crédit des dépositaires de ces secrets — médecins, banquiers, institut national de la statistique — si, hormis les cas prévus par la loi, des liaisons informatiques permettaient de révéler ce que la loi a entendu protéger du sceau du secret ?* »[1131].

Bien que ces exemples montrent l'attachement de la CNIL à vérifier que les données issues de la relation de soins ne soient transmises qu'à des personnes auxquelles les professionnels de santé peuvent, en raison d'une autorisation ou d'une obligation de la loi, transmettre les données, la majorité de notre analyse révèle qu'elle s'est parfois montrée favorable à ce que certaines catégories de personnes aient accès à ces données indépendamment de disposition légale. Il apparaît qu'elle se livre alors à une interprétation téléologique des textes[1132], ce qui, nous le verrons, n'est pas sans conséquence.

B - La CNIL, moteur des évolutions législatives ?

233. Porter un regard d'ensemble sur la doctrine de la CNIL nous amène à remarquer qu'elle ne s'est pas toujours positionnée dans le strict respect de la loi. Suivant la logique du compromis qui caractérise la loi informatique et libertés, elle a pris en compte la nécessité des traitements. Elle a notamment autorisé la transmission de données couvertes par le secret à des fins de

---

[1129] Dans sa délibération la CNIL rappelle cette procédure qui va de la transmission de la fiche d'incident transfusionnel au correspondant régional d'hémovigilance par le professionnel de santé jusqu'à sa transmission à l'Agence française du sang. Au cours de cette procédure, seule les personnes désignées pour participer au processus de traçabilité peuvent accéder aux données (Délibération n° 96-014 du 12 mars 1996 relative à un projet d'acte réglementaire présenté par l'Agence française du sang concernant un traitement automatisé d'informations indirectement nominatives ayant pour finalité la gestion des fiches d'incident transfusionnel « GIFIT »).
[1130] CNIL, *Rapport d'activité 1998*, p. 40.
[1131] CNIL, *Rapport d'activité 1998*, p. 41.
[1132] L. BOY, « Réflexions sur « le droit de la régulation », *D.* 2001, p. 303. Sur ce point v.

recherches médicales bien avant que le législateur n'intervienne **(1)**. S'agissant du partage des données entre professionnels de santé et entre les professionnels du secteur médical et médico-social ou social, elle semble toujours, si l'on peut dire, avoir un temps d'avance sur le législateur, diminuant les conséquences de son interprétation extensive des dispositions législatives par le biais de mesures techniques **(2)**.

1 - L'exemple de la recherche médicale

234. Il nous semble que l'exemple le plus édifiant de ce que la CNIL a parfois tenu des positions *contra legem* – nous usons de la litote lorsque nous évoquons des *invitations à* légiférer – concerne la recherche médicale. La Commission a soulevé le problème dès 1985 à propos des registres du cancer. Elle constate à l'occasion de son rapport annuel qu'une douzaine de registres ont été mis en œuvre à travers le territoire, ils « *permettent de recenser, dans une zone géographique déterminée, les cas de cancer à partir de données nominatives couvertes par le secret médical, transmises volontairement à l'organisme de recherche par les médecins et autres professionnels de santé concernés* »[1133]. La CNIL relève l'illicéité de ces transmissions de manière timorée : « *Il semble que, sur ce dernier point* [la transmission à autrui des informations recueillies par le médecin auprès de son malade], *les registres du cancer, dans la mesure où ils donnent lieu à la transmission d'informations nominatives à des tiers, sont d'une légalité discutable* »[1134]. Afin de remédier à ce problème et en l'absence de texte autorisant une telle transmission, elle adopte une recommandation[1135] à l'occasion de laquelle elle autorise ces transmissions sous réserve du consentement du patient. Par cette recommandation elle ne fait pas autre chose que poser un fait justificatif, ce qui relève évidemment de la compétence du seul législateur. L'argument principal de la CNIL tient au consensus entre le corps médical et du Comité national d'éthique, celui-ci étant guidé par l'intérêt que présente le développement de la recherche médicale par l'informatique. La nécessité est donc tirée de ce que la recherche médicale est d'intérêt général. C'est bien à une interprétation téléologique que se livre la CNIL. Elle propose un compromis et se place en législateur. Les registres du cancer ne sont pas le seul exemple de ce type : la recommandation

---

[1133] CNIL, *Rapport d'activité 1985*, p. 87.
[1134] *Ibid.* p. 88.
[1135] CNIL, Délibération n°85-07 du 19 février 1985 portant adoption d'une recommandation sur les traitements automatisés d'informations médicales nominatives utilisés à des fins de recherche médicale.

de la CNIL a longtemps permis d'avaliser des pratiques illicites. La solution sera finalement entérinée par le législateur en 1994, soit dix ans plus tard. Sur ce point, l'on peut affirmer que la CNIL a sans doute incité le législateur à réagir, ce qu'il a fait tardivement. Cet exemple, désormais ancien, révèle que le critère de la nécessité guide l'interprétation que la CNIL fait des textes, ce critère lui permettant de faire respecter la confidentialité des données au sens de la loi informatique et libertés tout en faisant fi du régime attaché au secret professionnel. Son interprétation extensive du *secret partagé* au fil des décennies en témoigne encore.

2 - L'interprétation extensive du secret partagé et la référence aux mesures techniques comme palliatif

235. Porter un regard sur l'interprétation que la CNIL fait des dispositions relatives au partage de l'information dans le domaine de la santé pose un problème de méthode. La reconnaissance légale d'un *secret partagé* n'est intervenue qu'à partir de la loi du 4 mars 2002. Les textes précisant les conditions d'échange et de partage sont ensuite intervenus de manière successive, l'article L. 1110-4 du Code de la santé publique qui dispose de l'autorisation de révéler ayant fait l'objet de multiples modifications. Au risque d'alourdir notre analyse, il nous paraît essentiel d'expliquer ces évolutions de manière exhaustive **(a)**. Elles permettront ensuite de replacer la doctrine de la CNIL au regard du droit positif en vigueur à un moment donné **(b)**.

a - Le partage des informations dans le système de santé : évolutions

236. Les origines du secret partagé, la reconnaissance légale. Longtemps la violation du secret professionnel ne connaissait aucune justification légale permettant aux professionnels de santé de partager ou d'échanger des informations en raison des nécessités de la prise en charge du malade. La jurisprudence avait néanmoins pu l'admettre dans le secteur hospitalier, car, comme le remarque un auteur : « *En matière de médecine hospitalière, par exemple, le secret doit être considéré comme ayant par principe un caractère collectif, l'information étant d'emblée réputée confiée au service hospitalier et non à un praticien particulier* »[1136]. La relation de soins étant conçue, dans ce cadre précis, comme liant l'établissement et le

[1136] M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel, op.cit.*, n° 174. Dès 1972 le Conseil d'Etat affirme, dès 1972, que « *le malade qui s'adresse à un organisme qui pratique la medecine collective c'est nécessairement à l'ensemble du personnel médical de cet organisme* » (CE, 11 fév. 1972, *Crochette* : Rec. p. 138 ; *R.D. publ.* 1972, p. 959, concl. G. GUILLAUME ; *Dr. social* 1972, p. 404 ; *D.* 1972.426, note M. LE ROY).

malade[1137]. A l'occasion de la loi du 4 mars 2002[1138] le législateur a consacré la pratique et l'a étendue à la médecine de ville. L'article L. 1110-4 du Code de la santé publique, dans sa rédaction originelle prévoyait que « *Deux ou plusieurs professionnels de santé peuvent toutefois, sauf opposition de la personne dûment avertie, échanger des informations relatives à une même personne prise en charge, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible. Lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe* »[1139]. Seuls les professionnels de santé pouvaient alors échanger des informations relatives au patient. Le *secret partagé* est traditionnellement présenté comme un fait justificatif de la violation du secret professionnel qui serait une autorisation dont dispose, s'agissant du secret partagé en matière de santé, une loi prise en matière civile[1140].

237. Une extension légale du partage avec les professionnels du secteur social et médico-social, une logique de système. L'extension du partage de l'information entre professionnels s'est accompagnée d'une généralisation du secret professionnel, d'abord à l'occasion de la loi du 4 mars 2002, puis de la loi du 26 janvier 2016[1141]. La logique sous-jacente consistait à rapprocher la prise en charge sanitaire et la prise en charge sociale et médico-sociale afin d'assurer la pérennité du système de santé[1142] et de garantir la mise en œuvre du « *parcours de santé* »[1143] des malades. Cette stratégie d'amélioration de la prise en charge était menée par le

---

[1137] S. PECHILLON, « L'adaptation du secret médical à l'hôpital : du silence à l'information médicale », in *De l'hôpital à l'établissement public de santé*, M.-L. MOQUET-ANGER (dir.), l'Harmattan, Paris, 1998, p. 317.
[1138] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.
[1139] CSP, art. L. 1110-4, al. 3, ancien.
[1140] M. BENEJAT, *La responsabilité pénale professionnelle*, *op. cit.*, n° 67.
[1141] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé. Spécifiquement sur les modifications induites par la loi v. F. VIALLA, « Le secret partagé », *RDS*, n° 2, 2016 (v. numérique 2018), pp. 52-64.
[1142] Sur le secret partagé et l'évolution du système de santé et notamment l'émergence de la médecine prédictive, des vigilances sanitaires, de la maîtrise des dépenses de santé v. D. TABUTEAU, « Le secret médical et l'évolution du système de santé », *D.* 2009, p. 2629.
[1143] Sur le parcours de santé et les évolutions en matière d'accès aux soins v. B. APOLLIS, « L'accès aux soins et la loi du 26 janvier 2016 », *RDSS* 2016, p. 673 ; Sur la coordination du parcours du malade et le secret partagé v. F. EON, « Hôpital public et données personnelles des patients », *RDSS* 2015, p. 85 ; sous l'angle des politiques de santé et de la stratégie nationale de santé (2018-2022) v. M. BORGETTO, « La stratégie nationale de santé », *RDSS* 2018, p. 387.

gouvernement depuis la loi « HPST »[1144], mais sa mise en œuvre se trouvait réduite du fait de l'absence de permission de partager et d'échanger des informations entre les professionnels des différents secteurs. En effet, alors que le texte de l'article L. 1110-4 du Code de la santé publique prévoyait la soumission au secret de tous les professionnels intervenant dans le système de santé[1145], le partage de l'information recélait une certaine évidence. Il faudra

---

[1144] Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

[1145] La question de la soumission au secret professionnel des professionnels de l'action sociale et médico-sociale parait complexe en raison de la dissémination des textes de désignation. En l'absence d'un texte général dans ce domaine le doute persiste sur le fait que certains intervenants soient soumis au secret professionnel (sur ce point v. C. RAHALI, *Le secret professionnel et l'action médico-sociale*, thèse dact., ss. la dir. de B. PY, soutenue le 20 décembre 2014, Université de Lorraine, *spéc.* n° 80 et svt et n°99 et svt.). Ce problème trouve toutefois une solution partielle dans la force d'attraction de la notion, non définie, de système de santé. En soumettant au secret professionnel toutes les personnes intervenant dans le système de santé l'article L. 1110-4 du Code de la santé publique vise également les intervenants de l'action sociale et médico-sociale. La notion de système de santé n'est pas définie pourtant, comme le souligne J. SAISON, le discours politique s'est approprié le vocable depuis quelques années. L'auteur souligne à ce propos « *La recherche de performance, à la fois technique mais aussi économique, a guidé et guide encore aujourd'hui l'ensemble des politiques de restructuration du champ sanitaire, social et médico-social. Il s'agit de constituer un véritable* « système » *entendu* « comme un ensemble d'éléments en interaction dynamique organisés en fonction d'un but » » (J. SAISON, « Service public hospitalier ou service public de santé ? À la recherche d'unité pour le système de santé... », *RDSS* 2017, p.634. Le fonctionnement en « système » suppose une unité (« L'une des caractéristiques communes à tous les systèmes consiste dans l'unité requise » A. –J. ARNAUD *et alii*, Dictionnaire encyclopédique de théorie et de sociologie du droit, 2ème éd., 1993, LGDJ, V° « Système ») qui est d'autant moins évidente que l'organisation de la santé en France s'est « « *Bâtie de façon empirique et par empilement, autour des structures d'offre de services, l'organisation doit être repensée au plus près des usagers, de la personne malade ou en situation de perte d'autonomie* » (A. Cordier (ss. la dir.), Un projet global pour la stratégie nationale de santé, *19 recommandations du comité des « sages »*, juin 2013, p. 6.). Ainsi, des efforts de coordination et de coopération médicale, sociale et médico-sociale ont émergés et se sont renforcés au niveau régional, sous la gouvernance des ARS. A ce propos J. SAISON souligne : *« Ses différentes formes de coopération sont complétées par des mécanismes de coordination gradués des actions menées par les acteurs du système de santé. Au premier niveau, on trouve l'équipe de soins primaires, constituée d'au moins un médecin généraliste et d'un professionnel paramédical. La communauté professionnelle territoriale de santé forme le deuxième niveau de la coordination en élargissant sa composition à l'ensemble des acteurs souhaitant se coordonner sur un territoire. Enfin, la plateforme territoriale d'appui aux situations complexes, troisième degré de la coordination, doit permettre de coordonner les parcours de santé en assurant l'information et l'orientation des professionnels vers les ressources sanitaires, sociales et médico-sociales du territoire. Elle offre un appui à l'organisation des parcours complexes par l'évaluation sanitaire et sociale de la situation et des besoins du patient, l'organisation de la concertation pluri-professionnelle, la planification de la prise en charge et du suivi et la coordination des actions autour du patient. Elle constitue également un soutien aux pratiques et initiatives professionnelles en matière d'organisation et de sécurité des parcours, d'accès aux soins et de coordination.* » (J. SAISON, « Service public hospitalier ou service public de santé ? À la recherche d'unité pour le système de santé... », *op. cit.*). La question de la soumission au secret professionnel ne se pose donc plus en termes de professionnel mais bien au regard des missions des différents intervenants dans un système de santé en constante évolution. Cette évolution étant liée à la capacité du système à étendre la prise en charge du malade de la santé vers le bien-être, notons sur ce point que l'article R. L. 1110-2 du Code de la santé publique qui liste les personnes pouvant échanger ou partager des informations relatives à la personne prise en charge mentionne les particuliers accueillant des personnes âgées ou handicapées mentionnées au titre IV et du livre IV du Code de l'action sociale et des familles ». Accueillant familial n'est pas une profession bien que l'activité soit rémunérée, ces derniers ne sont soumis explicitement au secret professionnel par aucun texte mais dès lors qu'ils sont considérés comme participant à la prise en charge des personnes il nous semble qu'ils sont astreints au secret professionnel en vertu de l'article L. 1110-4 du Code de la santé publique.

néanmoins attendre la loi du 26 janvier 2016 pour que le législateur affirme la possibilité d'un partage et d'un échange entre les professionnels de santé et les professionnels du secteur sanitaire et médico-social[1146], le texte prévoyant désormais : « *Un professionnel peut échanger avec un ou plusieurs professionnels identifiés des informations relatives à une même personne prise en charge, à condition qu'ils participent tous à sa prise en charge et que ces informations soient strictement nécessaires à la coordination ou à la continuité des soins, à la prévention ou à son suivi médico-social et social* »[1147]. Ce partage est strictement encadré et le même article distingue entre deux types de prise en charge : en équipe de soins[1148] où hors équipe de soins. Dans la première situation, les informations peuvent être échangées ou partagées sans que le consentement de la personne concernée ne soit sollicité, tandis que dans l'hypothèse où les professionnels prenant en charge la personne ne forment pas une équipe de soins, le partage est conditionné au consentement de la personne concernée par les informations. Cette distinction recèle quelques subtilités qu'il convient d'analyser.

238. Cadre général de l'échange et du partage : définitions. La première remarque qu'il convient de formuler est d'ordre sémantique mais engendre des conséquences pratiques : tandis que le professionnel peut *échanger* des informations en vertu du II de l'article L. 1110-4 du Code de la santé publique, le III du même article précise que les professionnels *partagent* également des informations. L'échange « *consiste à communiquer des informations à un ou plusieurs destinataires clairement identifiés par un émetteur connu, dans les conditions prévues au présent code* »[1149]. Le partage « *consiste à mettre à disposition de catégories de*

[1146] La logique de système impose ensuite le partage de l'information : « *La réussite de ces dispositifs de coordination repose notamment sur un partage de l'information* » (J. SAISON, « Service public hospitalier ou service public de santé ? À la recherche d'unité pour le système de santé... », op. cit.).

[1147] CSP, art. L. 1110-4 II.

[1148] Les frontières du secret partagé, dans la Loi du 4 mars 2002, se définissait dans le cadre de la structure de prise en charge (« Lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé » CSP, art. L. 1110-4) tandis que la Loi du 26 janvier 2016 fixe le périmètre de l'équipe de soins indépendamment de la structure de prise en charge. L'article L. 1110-12 du Code de la santé publique prévoit que outre le fait d'exercer au sein d'une même structure, constitue également une équipe de soins *« les personnes qui se sont vu reconnaitre la qualité de membre de l'équipe par le patient qui s'adresse à eux pour la réalisation des consultations et des actes prescrits par un médecin auquel il a confié sa prise en charge* » et celles « *exercent dans un ensemble, comprenant au moins un professionnel de santé, présentant une organisation formalisée et des pratiques conformes à un cahier des charges fixé par un arrêté du ministre chargé de la santé* » (CSP, art. L. 1110-12).

[1149] Arrêté du 25 novembre 2016 fixant le cahier des charges de définition de l'équipe de soins visée au 3° de l'article L. 1110-12 du code de la santé publique, Annexe, *JORF* n°0280 du 2 décembre 2016.

professionnels fondés à en connaître des informations dans les conditions prévues au présent code, respectant les conditions de confidentialité et de sécurité »[1150].

239. Cadre général de l'échange et du partage. L'article L. 1110-4 du Code de la santé publique prévoit d'abord le cadre de l'échange et du partage. Les dispositions générales relatives à ces deux hypothèses dans lesquelles l'information circule sont définies par des actes règlementaires : l'échange comme le partage doivent concerner des informations strictement nécessaires à la prise en charge du malade et dans le périmètre des missions dévolues à la personne qui reçoit l'information[1151]. Ensuite l'échange et le partage peuvent se faire entre tous les professionnels inscrits à la liste de l'article R. 1110-2 du Code de la santé publique[1152]. Cette

---

[1150] *Ibid.*

[1151] Il ne s'agit plus seulement des informations relatives au malade mais des informations relatives à la personne. L'article R. 1110-1 du Code de la santé publique issu du décret du 20 juillet 2016 (Décret n° 2016-996 du 20 juill. 2016 relatif à la liste des structures de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale dans lesquelles peuvent exercer les membres d'une équipe de soins) précise que les informations relatives à la personne prise en charge peuvent être échangées dans la double limite : « *1° Des seules informations strictement nécessaires à la coordination ou à la continuité des soins, à la prévention, ou au suivi médico-social et social de ladite personne ; 2° Du périmètre de leurs missions* ». Cette formule indique que la nature des informations échangées ou partagées n'est plus seulement médicale : elles peuvent également concerner « *les difficultés sociales de la personne prise en charge, ses conditions d'hébergement, ou son entourage familial* » (L. MORLET-HAÏDARA, « Le nouveau cadre légal de l'équipe de soins et du partage des données du patient », *RDSS* 2016, p. 1103). Le critère du partage et de l'échange n'est plus la nature de l'information mais les besoins de la prise en charge en fonction de la mission des professionnels intervenant dans celle-ci.

[1152] Soc. 20 avr. 2017, n° 15-27927 et n°15-27955, *D.* 2017, IR, p.920 « CHSCT (hôpital) : limitation de la mission de l'expert en raison du secret médical », *D. actu.*, 5 mai 2017, *comm.* J. SIRO, « Opposabilité du secret médical à l'expert du CHSCT » ; F. CANUT, « Le secret est opposable à l'expert CHSCT », *Les cahiers sociaux*, n° 297, p 302 ; C. BERLAUD, « L'expert du CHSCT d'un hôpital et le secret médical », *Gaz. Pal.*, n° 19, p. 41 ; P. VERON, « Opposabilité du secret à l'expert mandaté par le CHSCT d'un établissement de santé », 6 sept. 2017, n° 177-178, p. 16) semble confirmer une vision restrictive de la portée de l'article L. 1110-4 du Code de la santé publique. En l'espèce, le CHSCT d'un centre hospitalier procède à une expertise sur le fondement de l'article L. 4614-12 du Code de la santé publique. Lors de cette expertise le directeur du centre hospitalier refuse à l'expert l'accès aux blocs opératoires durant les périodes d'intervention ainsi qu'aux réunions quotidiennes des équipes de santé. Le directeur invoque, à l'appui de ce refus, le secret professionnel médical. La cour d'appel ayant considéré que l'expert de la CHSCT n'était pas soumis au « secret médical », l'expert et le CHSCT s'étaient pourvus en cassation. Le pourvoi est rejeté par la Cour de cassation au motif que c'est à bon droit que la cour d'appel a jugé que l'expert du CHSCT n'était pas soumis au « secret médical » dès lors qu'il « *n'est pas en relation avec l'établissement ni n'intervient dans le système de santé pour les besoins de la prise en charge des personnes* ». Il parait évident que l'expert du CHSCT n'est pas soumis à un secret dont le régime serait identique à celui des personnes intervenant dans le système de santé. Il n'est toutefois pas possible de déduire de cet arrêt que les experts du CHSCT qui révèleraient une information relative à un patient identifié et apprise lors de l'expertise ne pourrait être condamnés sur le fondement de l'article 226-13 du Code pénal, dès lors qu'ils sont soumis au secret en application de l'article L. 4614-13 du Code du travail. La question qui se posait ici était de savoir si les experts du CHSCT font partie, au regard de l'article L. 1110-4 du Code de la santé publique, des professionnels avec lesquels l'information peut être partagée. La Cour d'appel avait répondu négativement, ce que confirme la Cour de cassation. La Cour répond ici aux moyens invoqués par les parties, c'est-à-dire sur la question de savoir si les membres de CHSCT peuvent être regardés comme des professionnels intervenant dans le système la réponse est négative mais elle emporte comme conséquence principale leur exclusion du cercle des partageant au regard de l'article L. 1110-4 et R. 1110-2 du Code de la santé publique.

liste, qui a fait l'objet de critiques[1153], distingue les professionnels susceptibles d'échanger ou de partager des informations relatives au malade. L'article distingue la catégorie des professionnels de santé (dont les professions sont encadrées par le Code de la santé publique) et ceux relevant des sous-catégories comprenant les professionnels de l'action sociale et médico-sociale (dont l'activité est régie par le Code de l'action sociale et des familles) et certaines professions ne figurant dans aucun de ces deux codes : les ostéopathes, chiropracteurs, psychologues et psychothérapeutes[1154]. Partant, l'échange et le partage ne sont possibles qu'entre ces seules personnes et à condition que les informations échangées ou partagées concernent strictement la prise en charge et soient ciblées en fonction des missions de chacun des acteurs. Il faut à présent s'intéresser aux cadres respectifs de l'échange et du partage.

240. Dispositions spécifiques à l'échange. Au regard de la définition précédemment évoquée, l'échange d'informations peut être bilatéral ou non : il s'agit d'une communication et donc d'une action positive. L'échange prévu au II de l'article L. 1110-4 du Code de la santé publique est possible indépendamment de la référence à un cadre d'équipe de soins, contrairement au partage. N'importe quel professionnel de la liste prévue à l'article R. 1110-2 du Code de la santé publique peut communiquer, volontairement, une information relative à un patient dès lors que le professionnel à l'origine de l'échange « *informe préalablement la personne concernée, d'une part, de la nature des informations devant faire l'objet de l'échange, et d'autre part, soit de l'identité du destinataire et de la catégorie dont il relève, soit de sa qualité au sein d'une structure précisément définie* »[1155]. Le patient peut évidemment s'opposer à cet échange en vertu de l'article L. 1110-4 IV du Code de la santé publique, cette disposition s'appliquant en effet dans toutes les hypothèses où le consentement de la personne n'est pas exigé.

241. Dispositions spécifiques au partage. Le partage de l'information relative à un malade dans le cadre de sa prise en charge, ne correspond plus à une action occasionnelle : il s'agit

---

[1153] Notamment en ce qu'elle n'inclue par les aidants et la famille v. E. BUCKI, G. CASANOVAS, S. LANGARD, « Les règles d'échange et de partage d'informations : aux limites de la démarche empirique », *RDS*, n° 79, 2017, p. 658 ; Egalement sur le fait que cette liste inclut les particuliers accueillant des personnes âgées ou handicapées v. L. MORLET-HAÏDARA, « Le nouveau cadre de l'équipe de soins et du partage des données du patient », *op. cit.*

[1154] Il s'agit de professions qui ne sont pas règlementées.

[1155] CSP art. R. 1110-3 I.

d'une mise en commun ainsi que le confirme l'arrêté du 25 novembre 2016[1156] qui évoque une « *mise à disposition* »[1157]. La mise à disposition des informations devant permettre un accès constant aux informations concernées, il paraît évident que le cadre du partage doit être plus strict que celui de l'échange. Il faut ainsi distinguer le partage au sein d'une même équipe de soins et le partage hors équipe de soins. L'équipe de soins est définie à l'article L. 1110-12 du Code de la santé publique. Il s'agit des professionnels qui : « *Soit exercent dans le même établissement de santé, au sein du service de santé des armées, dans le même établissement ou service social ou médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles ou dans le cadre d'une structure de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale figurant sur une liste fixée par décret ; soit se sont vu reconnaître la qualité de membre de l'équipe de soins par le patient qui s'adresse à eux pour la réalisation des consultations et des actes prescrits par un médecin auquel il a confié sa prise en charge ; soit exercent dans un ensemble, comprenant au moins un professionnel de santé, présentant une organisation formalisée et des pratiques conformes à un cahier des charges fixé par un arrêté du ministre chargé de la santé* »[1158]. Dans le cas où la mise à disposition s'effectue dans le cadre d'une équipe de soins alors le consentement de la personne n'est pas exigé mais il pèse sur les professionnels une obligation d'information, il en est de même pour l'échange dans le cadre de l'équipe de soins, qui ne diffère pas du cadre général de l'échange[1159]. S'agissant du partage des informations hors équipe de soins, la pratique est nécessairement plus encadrée puisqu'il s'agit de mettre à disposition constante des informations hors du cadre d'une équipe définie ou d'autoriser un professionnel ne faisant pas partie de l'équipe à accéder aux informations. Aussi ne s'agira-t-il plus seulement d'informer la personne mais d'obtenir son consentement au partage (mais non à l'échange qui répond au cadre général). Ces modalités sont inscrites aux articles D. 1110-3-1 et suivants du Code de la santé publique.

[1156] Arrêté du 25 novembre 2016 fixant le cahier des charges de définition de l'équipe de soins visée au 3° de l'article L. 1110-12 du code de la santé publique, *JORF* n°0280 du 2 décembre 2016.

[1157] « Le partage de ces données consiste à mettre à disposition de catégories de professionnels fondés à en connaître des informations dans le respect des dispositions du présent code » (Annexe du cahier des charges du décret du 25 novembre 2016, *op. cit.*).

[1158] CSP, art. L. 1110-12.

[1159] A propos des modalités d'information v. Arrêté du 25 novembre 2016 fixant le cahier des charges de définition de l'équipe de soins visée au 3° de l'article L. 1110-12 du code de la santé publique, Annexe, *op. cit.*

Au regard de l'évolution du cadre légal de l'autorisation de partager et d'échanger des informations et des données couvertes par le secret, il est désormais possible de poser un regard averti sur la doctrine de la CNIL.

b - Doctrine de la CNIL

242. A propos du fichier GAMIN, mis en œuvre par l'Etat en 1981, outre le fait que la CNIL recherche si tous les destinataires sont astreints au secret professionnel, elle affirme par exemple « […] *qu'une demande formulée par des personnes ou services extérieurs à la PMI ne peut recevoir satisfaction que dans la mesure où le demandeur est lui-même tenu au secret médical* »[1160]. Bien qu'à cette période l'existence d'un *secret partagé* n'était qu'implicitement reconnue, la Commission détermina elle-même les conditions qui permettaient, dans le cadre de ce fichier, de transmettre des données à l'extérieur des services de la protection maternelle et infantile. L'on trouve encore une illustration de sa démarche téléologique dans son rapport de l'année suivante, lorsqu'elle affirme que son rôle est « *beaucoup moins de protéger des données nominatives déjà couvertes par le secret médical, que de replacer le dossier médical dans le processus qui va de la saisie à l'utilisation finale, de l'examen du malade au diagnostic, aux soins, à l'expérimentation, à la statistique, à la recherche génératrice de découvertes et de meilleurs soins. C'est à la totalité du circuit, à tous les maillons de la chaîne que s'applique la vigilance de la Commission, chargée par la loi de concilier le respect de l'individu et l'intérêt de tous* »[1161].

[1160] *Ibid.* Le rapport de la CNIL est un peu plus précis : « *Que s'il peut communiquer certaines indications portées sur les certificats de santé aux membres de son équipe médicosociale, c'est uniquement en vue de la protection de la mère et de l'enfant ; qu'une demande formulée par des personnes ou services extérieurs à la PMI ne peut recevoir satisfaction que dans la mesure où le demandeur est lui-même tenu au secret médical* » (CNIL, *Rapport d'activité*, 1980-1981, p. 228).

[1161] (CNIL, *Rapport d'activité* 1981-1982, p. 21). La CNIL admet, à notre sens, que l'idée de conciliation l'invite à envisager la circulation de l'information comme une « chaine » d'acteurs ayant intérêt à accéder aux données. La circulation des données, même sensibles, implique qu'elle opère la balance entre l'intérêt individuel des malades et l'intérêt général servi par les traitements au regard de leurs finalités.

L'on peut également mentionner, durant la même décennie, le traitement GIPSY destiné à la surveillance des mouvements des malades mentaux[1162]. La Commission avait concentré son analyse sur le fait de savoir si les autorités administratives chargées de la police des malades mentaux, ainsi que les autorités judiciaires devaient être considérées comme des destinataires du traitement mis œuvre par l'hôpital psychiatrique d'Epinay-sur-Orge. Ces autorités étaient alors habilitées à effectuer des contrôles en application des dispositions de l'article L. 332 du Code de la santé publique[1163]. Or, le traitement contenait des informations relatives aux hospitalisations précédentes ainsi que des informations d'ordre médical[1164]. La CNIL avait fait ici une interprétation extensive de la possibilité de contrôle des établissements par les autorités en déduisant de celle-ci la possibilité d'accéder aux informations couvertes par le secret professionnel. Elle justifiait alors son interprétation par la mention de deux arrêts du Conseil d'Etat[1165] par lesquels la haute juridiction avait confirmé qu'il revenait « *aux autorités chargées de la police des malades mentaux de recueillir toutes les informations utiles sur les personnes dont l'état mental risqu[ait] de menacer l'ordre public et plus particulièrement sur celles qui [avaient] fait l'objet de placements d'office à la suite d'actes de violences* »[1166]. Cette possibilité, admise par le Conseil d'Etat relevait d'un pouvoir de contrôle qui ne devait porter que sur les malades susceptibles de menacer l'ordre public et les malades violents[1167]. En admettant que

---

[1162] Délibération n°84-32 du 25 septembre 1984 portant avis sur un traitement automatisé d'informations nominatives dénommé "GIPSY" relatif à la gestion administrative des malades mentaux, mis en œuvre par le Centre Hospitalier spécialisé de Vaucluse (Epinay-sur-Orge).

[1163] CSP, art. L. 332, ancien « *Le préfet et les personnes spécialement déléguées à cet effet par lui ou par le ministre de la Santé publique et de la Population, le président du tribunal, le procureur de la République, le juge du tribunal d'instance, le maire de la commune, sont chargés de visiter les établissements publics et privés consacrés aux aliénés ou accueillant des malades soignés pour troubles mentaux. Ils recevront les réclamations des personnes qui y sont placées, et prendront, à leur égard, tous renseignements propres à faire connaître leur position. Les établissements visés au premier alinéa sont visités, à des jours indéterminés, une fois au moins chaque trimestre, par le procureur de la République. En outre, ces établissements sont visités, une fois par année, par les autres autorités visées au même alinéa. Il en est rendu compte aux autorités compétentes.* »

[1164] Ce qui avait engendré une vive opposition de la part des syndicats de psychiatres (CNIL, *Rapport d'activité* 1983-1984, p. 92). La CNIL admet d'ailleurs que « *La fonction de suivi des hospitalisations antérieures des malades pouvait apparaître comme une tentative d'extension médico-administrative d'un système initialement conçu pour assurer une simple gestion administrative de facturation des frais de séjour. Or cette fonction était susceptible de poser problème, au regard notamment du respect des règles du secret médical. En effet, elle prévoyait la transmission par l'administration de renseignements de type médico-social à des tiers extérieurs à l'hôpital* » (*ibid*. 92).

[1165] CE 5 / 3 SSR, 26 janvier 1979, n° 99910 Inédit au recueil Lebon et CE, 26 janvier 1979, n° 99511. CNIL, *Rapport d'activité* 1983-1984, p. 93.

[1166] CE, 26 janvier 1979, n° 99511.

[1167] Sur ce point v. notamment B. PY, « Ficher les fous. Au sujet du traitement automatisé de données à caractère personnel dénommé « Redex » (répertoire des expertises) », *RDS* 2018, n° 84, p. 611.

les autorités publiques soient destinataires des données concernant tant les personnes ayant fait l'objet d'un placement d'office que libre il nous semble que la CNIL admettait une forme de *secret partagé*, qu'elle déduisait de « *l'habilitation* »[1168] des autorités précitées. Les arrêts évoqués par la CNIL ainsi que les textes, à cette période, prévoyaient la *possibilité* pour les autorités publiques de recueillir les informations. Les deux arrêts du Conseil d'Etat ne précisent en aucun cas les modalités de ce recueil, et ni le Code de la santé publique ni le Code pénal ne posaient pour le professionnel une obligation de révéler. En somme, être destinataire des données signifie que ce sont les autorités qui reçoivent communication des données, là où le recueil des informations nécessitait un *contrôle circonstancié*. La permanence de la communication et son extension relèvent davantage d'un partage d'informations. Cet exemple témoigne, à notre sens, de la logique de compromis qui a amené la CNIL à créer, sans le formuler explicitement, des hypothèses de partage d'informations.

S'agissant du fait de savoir si les informaticiens devaient être considérés comme des personnes qualifiées pour recevoir les données couvertes par le secret, nos remarques relatives aux tentatives de la CNIL consistant à trouver des succédanés au secret professionnel, révèlent également que la possibilité d'accéder aux données est guidée par la nécessité, notamment lorsqu'elle affirme que « *L'informaticien est nécessairement appelé à participer à la gestion de ces systèmes* »[1169]. La nécessité, qui est au cœur de la confidentialité telle qu'entendue par la loi informatique et libertés permet à la CNIL de déterminer elle-même les hypothèses dans lesquelles les données doivent être amenées à circuler.

Un projet d'acte règlementaire – en raison de la sensibilité des données traitées – présenté par l'INSERM[1170] portant sur un traitement de données ayant pour finalité une étude sur le vieillissement cognitif a été soumis à l'examen de la Commission au cours de l'année 1992. L'étude consistait à suivre les patients pendant trois ans afin de mieux décrire l'évolution au cours du vieillissement des déficits des fonctions cognitives, dans le but permettre un

---

[1168] CNIL, *Rapport d'activité* 1983-1984, p. 93. En principe le secret professionnel pouvait être opposé à l'administration, bien que la question fût longtemps discutée (v. E. GARCON, *Code pénal annoté,* Nouvelle édition refondue et mise à jour par M. ROUSSELET, M. PANTIN et M. ANCEL, T. II, Sirey, 1956) et quand bien même il aurait existé une obligation de révéler pour le professionnel de santé mentionné à l'article 378 du Code pénal, les informations demandées portaient sur des personnes préalablement identifiées.
[1169] CNIL, *Rapport d'activité 1987*, p. 98.
[1170] Institut national de la santé et de la recherche médicale.

meilleur suivi médical et social des personnes âgées. Les données traitées étaient issues de questionnaires et de tests interactifs réalisés par une cohorte de six-cent-cinquante personnes. Il s'agissait de mesurer l'attention visuelle et auditive, la mémoire et l'habileté manuelle mais également de poser des questions relatives aux qualités de vie des individus. Les enquêtes étaient effectuées par des psychologues tandis que les résultats étaient analysés des médecins. Parmi les données servant à ces analyses, certaines devaient être transmises par les médecins traitants des personnes participant à l'étude. La CNIL relève à propos de la participation des psychologues et de l'échange d'informations : « *Il s'agira strictement d'une enquête d'observation, sans visée diagnostique ni objectif thérapeutique direct, ce qui n'empêchera pas un échange éventuel d'informations entre le médecin traitant et le responsable de l'étude, dans l'intérêt du malade.* […] *pour ce qui est de la transmission d'informations par le médecin traitant, on peut considérer qu'elle entre dans le cadre du « secret partagé »* »[1171]. Cette dernière formule de la CNIL est d'autant plus significative qu'elle insiste, dans son rapport, sur l'appui apporté à cette recherche par l'OMS et sur son intérêt pour l'évolution de la recherche médicale. C'est l'intérêt supposé de la recherche qui justifie une vision très extensive du *secret partagé*, en l'absence de tout fait justificatif posé par le législateur.

A propos, par exemple, de l'examen d'un traitement de données déclaré à la Commission et relatif à la mise en œuvre d'un dossier informatisé des patients hospitalisés à domicile, la CNIL avait porté son attention sur la coordination de la prise en charge des personnes par des intervenants professionnels de santé mais également des assistants sociaux et des aides ménagères employées par une association. Les informations saisies durant la journée par ces intervenants étaient « *automatiquement* [transmises] *par le réseau téléphonique commuté au site central de l'association, lui permettant ainsi de gérer les temps de passage des intervenants, de mettre à jour les dossiers de soins, d'éditer les commandes, d'informer les surveillantes de nuit et le médecin coordinateur* »[1172]. Afin de s'assurer du respect du secret professionnel la Commission avait demandé que « *que chaque professionnel, administratif ou médical, acteur du système* »[1173] n'ait accès qu'aux données nécessaires à sa mission. Sans qu'elle précise davantage ce qu'elle entend par *acteurs du système* l'on se pose légitimement la question de savoir si les aides ménagères sont des acteurs du système susceptibles de recevoir

[1171] Délibération n° 92-041 du 7 avril 1992 portant avis sur le projet d'acte réglementaire présenté par l'INSERM concernant un traitement relatif à une étude épidémiologique du vieillissement cognitif.
[1172] CNIL, *Rapport d'activité 1994,* p. 321.
[1173] *Ibid.* p. 321.

des informations, et le cas échéant, l'on s'interroge sur la nature des informations dont elles pourraient être destinataires. Ensuite, la Commission avait également demandé, s'agissant des informations transmises au site de l'association, qu'elles ne fassent pas mention du nom de la personne concernée. Or le nom n'est qu'un élément identifiant parmi d'autres. Il nous semble ainsi qu'elle admettait, à cette occasion, un partage d'informations entre ces différents acteurs. Pour le justifier, elle s'appuyait sur l'ancien article L. 711-5 du Code de la santé publique prévoyant la possibilité pour des établissements privés de participer au service public hospitalier « *en collaboration avec les médecins traitants et avec les services sociaux et médico-sociaux, à l'organisation de soins coordonnés au domicile du malade* »[1174]. La Commission en déduit l'existence d'un secret partagé entre les intervenants de tout ordre.

Durant l'année 2002 l'attention de la Commission s'est portée sur « *la circulation des données de santé* »[1175]. Cela s'explique notamment par le fait que le secret professionnel se présente de moins en moins comme une limitation à la disponibilité des données[1176]. L'article L. 1110-4 du Code de la santé publique, dans sa rédaction initiale, érige en effet le *secret partagé* comme une possibilité de révéler, fait justificatif propre au système de santé[1177]. Cette possibilité, au regard de la lettre de l'article ne concerne que les professionnels de santé prenant en charge un même patient. L'information est par ailleurs réputée confiée à l'ensemble de l'équipe de soins lorsque la personne est prise en charge par un établissement public.

243. Changement de politique de communication. Dès 2004 et en raison des transformations induites par la transposition de la directive de 1995, les rapports de la CNIL s'appauvrissent[1178]. Le rapport d'activité de 2004 ne contient que trois pages portant sur la

---

[1174] CSP, art. L. 711-5, ancien
[1175] CNIL, *Rapport d'activité 2002*, p. 121 et svt.
[1176] Le rapport de la CNIL, qui consacre un chapitre à la circulation des données, en introduction de celui-ci, pose cette question : « Demain que restera-t-il du secret médical ? » (*Ibid.*).
[1177] CSP, art. L. 1110-4, dans sa version antérieure.
[1178] La rédaction d'un rapport annuel par l'autorité administrative est une obligation prévue par l'article 8 de la LIL au regard duquel elle rend compte de ses activités, chaque année, au Président de la République et au Premier ministre, cette obligation figure également à l'article 11 de la loi portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes (Loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes). Pourtant les textes ne précisent en rien leur contenu. Une évolution est intervenue dans leur rédaction depuis la création de la CNIL, se dont rend compte Madame Debet. A l'occasion d'une présentation critique du rapport annuel 2017 de l'autorité

question du « *partage des données médicales personnelles* »[1179], retraçant les conditions de mise en œuvre du *Dossier médical partagé*. A cette occasion elle se contente de rappeler que le dossier doit être tenu dans le respect du *secret médical*[1180]. Elle évoque par ailleurs la possibilité de transmettre des données anonymisées aux organismes d'assurance complémentaire[1181]. Il en est de même pour les rapports de 2005 et 2006 qui posent un état des lieux de l'avancement de la mise en œuvre du dossier médical.

244. Réseaux de santé. Le jeu combiné des articles de la loi informatique et libertés et des dispositions relatives aux réseaux de santé - originellement dénommés réseaux de soin[1182] - implique que la CNIL a notamment eu à se prononcer sur des traitements de données permettant une prise en charge coordonnée des personnes « *adaptée aux besoins de la personne tant sur le plan de l'éducation à la santé, de la prévention, du diagnostic que des soins* »[1183]. Il faut noter que les conditions d'échange d'informations entre les personnes intervenant au sein de ces réseaux étaient alors prévues à l'article D. 766-1-4 du Code de la santé publique, devenu l'article D. 6321-4 du même Code, mais dont le contenu est resté inchangé. Il prévoit qu'une

---

de régulation l'auteur s'interroge sur la fonction de cet écrit (A. DEBET, « À la veille de l'entrée en vigueur du RGPD, la CNIL publie son rapport annuel 2017 », *JCP G* 2018, n° 19-20, 537, p. 916) et remarque que « *l'article 23 de la loi du 6 janvier 1978 d'origine prévoyait que celui-ci décrirait notamment les procédures et méthodes de travail suivies par la commission et contiendrait en annexe toutes informations sur l'organisation de la commission et de ses services, propres à faciliter les relations du public avec celle-ci* » (*Ibid.*). L'auteur relève ainsi qu'à l'origine le rapport annuel était gage de transparence et tendait à expliquer les méthodes de l'autorité et, partant, d'expliciter les interprétations qu'elle fait des dispositions relatives à la protection des données et ses prises de position concernant des sujets qui avait marqué son activité durant l'année : « *Ces rapports apportaient de la sécurité juridique pour les responsables de traitement qui connaissaient les positions de la CNIL et les raisons d'éventuelles évolutions de celles-ci. Les rapports annuels permettaient donc à cette source non négligeable du droit qu'est la doctrine de cette AAI d'être publique et prévisible, caractéristiques indispensables de toutes les sources du droit pour garantir la sécurité juridique des citoyens* » (*Ibid.*). A partir de 2005 les rapports de la CNIL vont peu à peu perdre leur caractère explicatif et exhaustif, d'une centaine de pages il sont progressivement devenus des « *plaquette de communication […] et non plus un document de référence pour les juristes spécialistes du secteur* » (*Ibid.*).

[1179] CNIL, *Rapport d'activité 2004*, sommaire p. 4.

[1180] *Ibid.* p. 53.

[1181] *Ibid.* p. 55. Délibération n°2004-081 du 09 novembre 2004 portant autorisation d'une expérimentation présentée par la Fédération Nationale de la Mutualité Française ayant pour finalité d'accéder, sous forme anonymisée, aux données de santé figurant sur les feuilles de soins électroniques ; Délibération n°2005-018 du 03 février 2005 portant autorisation d'une expérimentation présentée par la société Axa France ayant pour finalité d'accéder, sous forme anonymisée, aux données de santé figurant sur les feuilles de soins électroniques.

[1182] Les réseaux de soins, devenu réseaux de santé, font l'objet d'une définition à l'article L. 6321-1 CSP, ils : « *ont pour objet de favoriser l'accès aux soins, la coordination, la continuité ou l'interdisciplinarité des prises en charge sanitaires, notamment de celles qui sont spécifiques à certaines populations, pathologies ou activités sanitaires* » et sont « *constitués entre les professionnels de santé libéraux, les médecins du travail, des établissements de santé, des centres de santé, des institutions sociales ou médico-sociales et des organisations à vocation sanitaire ou sociale, ainsi qu'avec des représentants des usagers* ».

[1183] *Ibid.*

« charte réseau » prise par les acteurs – aussi bien professionnels que bénévoles – de celui-ci précise « *les modalités de partage de l'information dans le respect du secret professionnel et des règles déontologiques propres à chacun des acteurs* »[1184]. Soulignons que de 2002 à 2016, l'article L. 1110-4 fixant les limites de l'échange d'informations dans le domaine de la santé prévoyait que seuls les professionnels de santé pouvaient échanger des informations, sauf oppositions de la personne. Dans le cadre d'une équipe de soins *en établissement de santé* les informations étaient réputées confiées à l'ensemble de l'équipe. Les décisions rendues par la CNIL à partir de 2004 et disponibles sur *Légifrance* concernent principalement la mise en œuvre de dossiers partagés et de systèmes de partage d'informations en réseau pour des finalités d'intérêt public[1185]. Dans cette hypothèse la Commission ne porte pas l'article L. 1110-4 du Code de la santé publique au visa de ses décisions, seul le décret du 17 mars 2002 créant les réseaux de soins. Si dans les cas qui ne soulèvent pas de discussion la CNIL relève systématiquement que les destinataires des données sont les professionnels de santé participant au réseau ou au dispositif pour les informations relatives à leurs patients[1186], il faut noter que,

---

[1184] CSP, art. 766-1-7.

[1185] C'est le cas de toutes les décisions que nous reproduiront ci-après.

[1186] Liste non exhaustive d'autorisations : Délibération n°2005-048 du 22 mars 2005 portant autorisation de mise en œuvre par l'association de gestion du réseau e-santé Bas-normand d'une plate-forme régionale d'information de santé ; Délibération n°2005-025 du 17 février 2005 portant autorisation de mise en œuvre par l'association Onco Pays de la Loire d'un dossier médical partagé ; Délibération n°2005-027 du 17 février 2005 autorisant le service médical de la région Ile-de-France à mettre en œuvre une étude sur les ententes préalables en matière de chirurgie plastique et reconstructrice et de vérifier les conditions techniques de réalisation de ces actes ; Délibération n°2005-026 du 17 février 2005 portant autorisation de mise en œuvre par le GIE Télémédecine océan indien d'un dossier médical partagé en cancérologie. Délibération n°2005-024 du 17 février 2005 portant autorisation de mise en œuvre par l'association réseau de soins sur l'hypertension artérielle en Guadeloupe d'un dossier médical partagé ; Délibération n°2005-214 du 11 octobre 2005 portant autorisation de mise en œuvre par l'association Carédiab d'un dossier médical partagé dans le cadre d'un réseau de santé en Champagne Ardenne ; Délibération n°2005-303 du 08 décembre 2005 portant autorisation de mise en œuvre par l'association du réseau de prise en charge de l'insuffisance cardiaque au sein de l'Isère, d'un traitement automatisé de données à caractère personnel ayant pour finalité la saisie et le partage sécurisés d'informations médicales et paramédicales "patients" entre les professionnels de santé du réseau RESIC 38 ; Délibération n°2005-316 du 20 décembre 2005 portant autorisation de mise en œuvre par l'association pour le développement du dossier médical informatisé DDMI) d'un traitement automatisé de données à caractère personnel ayant pour finalité la création d'un dossier médical informatisé en réseau pour des patients traités en cancérologie dans l'ouest parisien ; Délibération n°2005-230 du 11 octobre 2005 portant autorisation de mise en œuvre par l'association Franc-Comtoise du Diabète - Réseau de santé Gentiane, d'un dossier médical partagé ; Délibération n°2005-229 du 11 octobre 2005 portant autorisation de mise en œuvre par l'Union Régionale des Médecins Libéraux de Picardie RMLP- Réseau Diabète Picardie d'un dossier médical partagé ; Délibération n°2005-216 du 11 octobre 2005 portant autorisation de mise en œuvre par le réseau de cancérologie de l'Arc Alpin d'un traitement automatisé de données à caractère personnel ayant pour finalité la création d'un réseau de cancérologie destiné aux professionnels de santé prenant en charge des patients atteints de cancer ; Délibération n°2005-107 du 19 mai 2005 portant autorisation de mise en œuvre par l'association réseau

concernant certains dossiers partagés la Commission autorise l'échange des données entre professionnels de santé et assistants sociaux. Concernant par exemple un dossier partagé en gérontologie autorisé par la CNIL et contenant des informations essentiellement médicales[1187], les destinataires sont « *dans la limite de leurs attributions respectives, les professionnels de santé et les assistants sociaux dûment habilités intervenant auprès d'un bénéficiaire* »[1188]. Dans une autre décision elle autorise un traitement de données à caractère personnel ayant pour finalité la prise en charge en réseau de patients en soins palliatifs à domicile. Les membres du réseau sont médecins, infirmiers, psychologues et assistantes sociales, tous destinataires des données en raison de leurs attributions[1189]. Elle a pu, par ailleurs, autoriser la communication de données de santé à des personnes qui n'étaient pas des professionnels de santé et qui n'intervenaient dans la prise en charge, à des fins épidémiologiques, les données n'étant pas anonymisées mais simplement non nominatives[1190]. En 2006, la Commission relève, dans un cas, que les professionnels de santé et les assistants sociaux sont destinataires des données dans la limite de leurs attributions[1191]. Dans une seconde décision elle autorise « *un dossier minimum partagé entre les professionnels de santé et les assistants sociaux dûment habilités* »[1192]. Il apparaît donc clairement dans cet exemple que les assistants sociaux ont accès à certaines

---

25 d'un traitement automatisé de données à caractère personnel ayant pour finalité la création d'un dossier médical partagé dans le domaine des conduites addictives ; Délibération n°2005-070 du 20 avril 2005 portant autorisation de mise en œuvre par la direction de la santé de Polynésie française d'un réseau de santé. Délibération n°2006-029 du 02 février 2006 portant autorisation de mise en œuvre par le CHU de Grenoble d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'un système d'information hospitalier destiné à permettre le partage de l'information "patient" entre les professionnels de l'établissement chargés de sa prise en charge et permettant la communication et l'échange de données vers et depuis la plateforme régionale de santé Rhône-Alpes.

[1187] « *relatives à l'identité du patient, son mode de logement, à la personne référente, à l'organisation du soutien à domicile, aux antécédents médico-chirurgicaux, aux maladies actuelles, aux évolutions gérontologiques, au plan de soins infirmiers, à la grille AGGIR, au plan de soins kinésithérapique et ergothérapique, aux prescriptions, aux observations pharmaceutiques, au plan d'aide domicile et à la coopération des soins* » (Délibération n°2005-030 du 17 février 2005 portant autorisation de mise en œuvre d'un dossier médical partagé par le réseau de santé de gérontologie dénommé visage).

[1188] *Ibid.*

[1189] Délibération n°2005-287 du 22 novembre 2005 portant autorisation de mise en œuvre par le GIP réseau douleur soins palliatifs de Hautes-Pyrénées, ARCADE d'un traitement automatisé de données à caractère personnel ayant pour finalité la prise en charge coordonnée de patients en soins palliatifs.

[1190] Délibération n°2005-152 du 14 juin 2005 portant autorisation de mise en œuvre par la société Kappa Santé et le centre de mémoire de ressources et de recherche de la région Provence-Alpes-Côte d'Azur d'un réseau de données épidémiologiques standardisées sur la maladie d'Alzheimer.

[1191] Délibération n°2006-030 du 2 février 2006 portant autorisation de mise en œuvre par le réseau de l'association MGADDOC d'un traitement de données à caractère personnel ayant pour finalité la prise en charge médico-psycho-sociale des patients en difficulté avec des substances psycho-actives sur le département du Loir-et-Cher.

[1192] Délibération n°2006-203 du 14 septembre 2006 portant autorisation de mise en œuvre par l'Association "Le cheval bleu" d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'un dossier minimum partagé dans le cadre d'un réseau santé mentale précarité.

informations couvertes par le secret professionnel médical. A d'autres occasions elle a pu autoriser des traitements pour lesquels figuraient à la liste des destinataires les psychologues[1193], les assistants sociaux[1194] et plus largement les *professionnels médico-sociaux*[1195]. Nous pouvons également faire mention d'une décision dans laquelle les éducateurs médico-sportifs sont destinataires des données contenues dans un système d'échange de données de santé[1196]. L'on en trouve encore des exemples dans les autorisations données par la Commission en 2007 pour des traitements dans lesquels les psychologues[1197], tabacologues, sophrologues, et professeurs d'éducation physique adaptée étaient destinataires des données de santé nécessaires à leurs fonctions[1198]. Encore, en 2009 sont autorisés des traitements dont la liste des destinataires des données de santé comptait : les auxiliaires de vie, les aides à domicile, les institutionnels publics et privés et les services sociaux[1199]. Le même constat est valable pour l'année 2010, la Commission admet que les acteurs sociaux, notamment les auxiliaires de vie,

---

[1193] Dans une décision la Commission classe d'ailleurs les psychologues dans la catégorie des auxiliaires médicaux libéraux : Délibération n°2007-069 du 25 avril 2007 autorisant la mise en œuvre par l'Association GERONTO ASSISTANCE d'un dossier médical informatisé et partagé dans le cadre d'un réseau de santé.

[1194] Délibération n°2007-066 du 25 avril 2007 autorisant la mise en œuvre par ACCOMIP-REPOP d'un système d'échange de données de santé dans le cadre d'un réseau de santé ville-hôpital de prévention et de prise en charge - de l'obésité pédiatrique en Midi-Pyrénées ; Délibération n°2007-071 du 25 avril 2007 autorisant de mise en œuvre par le Centre hospitalier universitaire de Besançon d'un dossier médical informatisé et partagé en cancérologie dans le cadre du réseau régional de cancérologie ONCOLIE ; Délibération n°2007-068 du 25 avril 2007 autorisant la mise en œuvre par l'Association VIE L'AGE d'un dossier médical informatisé et partagé dans le cadre d'un réseau de santé ; Délibération n°2007-235 du 13 septembre 2007 autorisant la mise en œuvre par l'Association « soins de suite » 45 d'un dossier médical partagé afin d'améliorer l'orientation des patients dans le système de soins.

[1195] Délibération n°2007-063 du 25 avril 2007 autorisant la mise en œuvre par le réseau HANDIDENT d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'un dossier odontologique partagé.

[1196] Délibération n°2007-074 du 25 avril 2007 autorisant la mise en œuvre par RÉUCARE d'un système d'échange de données de santé dans le cadre de comités de concertation pluridisciplinaires.

[1197] Délibération n°2008-213 du 17 juillet 2008 autorisant la mise en œuvre par l'Association de Soins Palliatifs du Littoral d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins palliatifs à domicile ;

[1198] Délibération n°2008-100 du 10 avril 2008 n°2008-100 du 10 avril 2008 autorisant la mise en œuvre par l'association pour le développement de la réhabilitation respiratoire (ADRRES) d'un traitement automatisé de données à caractère personnel ayant pour finalité le partage de données de santé entre des professionnels de santé dans le cadre d'un réseau de santé.

[1199] Délibération n°2009-074 du 29 janvier 2009 autorisant la mise en œuvre par le réseau d'accompagnement et de soins palliatifs de l'Allier d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins palliatifs à domicile. Mentionnant, outre des professionnels de santé, les auxiliaires de vie et les aides à domicile : Délibération n°2009-308 du 7 mai 2009 autorisant la mise en œuvre par le réseau d'accompagnement et de soins palliatifs de l'Alsace Nord (ASPAN) d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins palliatifs à domicile ; Délibération n°2009-415 du 2 juillet 2009 autorisant la mise en œuvre par le réseau de soins palliatifs 72 – RSP d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins palliatifs à domicile

les aides à domicile libéraux, sont destinataires des données, toujours dans la limite de ce qui est nécessaire à leur mission[1200] - ils figurent même parfois dans la liste des *professionnels paramédicaux*[1201] - ainsi que les éducateurs ou encore dans certains cas les professeurs

[1200] Délibération n°2010-010 du 28 janvier 2010 autorisant la mise en œuvre par le réseau de santé gérontologique CARMAD d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins à domicile ; Délibération n°2010-090 du 8 avril 2010 autorisant la mise en œuvre par le Réseau Gérontologique GERONTONORD d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins aux personnes âgées prises en charge à domicile ; Délibération n°2010-092 du 8 avril 2010 autorisant la mise en œuvre par le Réseau Gérontologique du Pays Messin d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins aux personnes âgées prises en charge à domicile ; Délibération n°2010-129 du 20 mai 2010 autorisant la mise en œuvre par l'Association Réseau Gérontologique « Gaves et Bidouze », d'un traitement automatisé de données à caractère personnel ayant pour finalité la coordination des soins aux personnes âgées prises en charge à domicile ; Délibération n°2010-260 du 24 juin 2010 autorisant la mise en œuvre par l'Association Réseau Gérontologique « Les cantons d'Aliénor » d'un traitement automatisé de données à caractère personnel ayant pour finalité la coordination des soins aux personnes âgées prises en charge à domicile ; Délibération n°2010-289 du 15 juillet 2010 autorisant la mise en œuvre par le Réseau Gérontologique Aloise d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins aux personnes âgées prises en charge à domicile ; Délibération n°2010-287 du 15 juillet 2010 autorisant la mise en œuvre par le réseau de Soins Continus du Compiégnois (ARSCC) d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins palliatifs à domicile ; Délibération n°2010-288 du 15 juillet 2010 autorisant la mise en œuvre par le réseau de Soins palliatifs de l'Association de coordination sanitaire et sociale de l'Oise (PALLI-ACSSO) d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins palliatifs à domicile ; Délibération n°2010-285 du 15 juillet 2010 autorisant la mise en œuvre par le réseau d'accompagnement et de soins palliatifs de la Somme (PALPI80) d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins palliatifs à domicile ; Délibération n°2010-286 du 15 juillet 2010 autorisant la mise en œuvre par le réseau d'accompagnement et de soins palliatifs du Soissonnais (CECILIA) d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins palliatifs à domicile ; Délibération n°2010-284 du 15 juillet 2010 autorisant la mise en œuvre par le réseau de Soins de Proximité de Haute Picardie (RSPHP) d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins palliatifs à domicile ; Délibération n°2010-318 du 22 juillet 2010 autorisant la mise en œuvre par le Réseau Gérontologique du Compiégnois (60) d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins aux personnes âgées prises en charge à domicile ; Délibération n°2010-317 du 22 juillet 2010 autorisant la mise en œuvre par le Réseau Oncageoise (60) d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'un réseau de soins palliatifs ; Délibération n°2010-320 du 22 juillet 2010 autorisant la mise en œuvre par le Réseau de Santé Personnes Agées du Noyonnais-Ressontois (60) d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins aux personnes âgées prises en charge à domicile; Délibération n°2010-319 du 22 juillet 2010 autorisant la mise en œuvre par le Réseau Gérontologique Vimeux Baie de Somme (60) d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins aux personnes âgées prises en charge à domicile ; Délibération n°2010-359 du 30 septembre 2010 portant autorisation de la mise en œuvre par le Réseau NEPHROLOR (54) d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dossier médical partagé en réseau pour la prise en charge des patients souffrant d'insuffisance rénale chronique dans la région nancéienne (autorisation n°1356686) ; Délibération n°2011-328 du 18 octobre 2011 autorisant la mise en œuvre par le Réseau de coordination des soins de l'insuffisant cardiaque CARDIAUVERGNE d'un système d'échange de données de santé dans le cadre d'un réseau de santé ville-hopital.

[1201] Délibération n°2010-362 du 30 septembre 2010 portant autorisation de la mise en œuvre par le cabinet infirmier PRUDENTE (92) d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dossier médical partagé en réseau pour la prise en charge des patients souffrant de cancer (autorisation n°14033161) ; Délibération n°2011-006 du 13 janvier 2011 autorisant la mise en œuvre par l'Association Réseaux de Santé addictions, précarité et diabète de Champagne-Ardennes d'un traitement de données à caractère personnel ayant pour finalité la prise en charge coordonnée des patients ; Délibération n°2011-002 du 13 janvier 2011 autorisant la mise en œuvre par l'Association Réseau régional de cancérologie du Ponant d'un dossier médical

d'éducation physique adaptée[1202]. Deux remarques peuvent être formulées suite à l'analyse de l'ensemble de ces traitements de données de santé : la CNIL adopte une **conception très large du secret partagé** bien avant l'intervention du législateur. Elle opère la balance des intérêts au regard de la nécessité du traitement et des finalités d'intérêt public de celui-ci. Il nous semble encore que la distinction entre échange et partage issue de la loi du 26 janvier 2016[1203] est inspirée de la méthode que la Commission mettait déjà en œuvre avant l'entrée en vigueur de la loi. L'on peut citer l'exemple d'un traitement autorisé par la CNIL et mis en œuvre par une association et ayant pour finalité l'accompagnement des adolescents accueillis dans le cadre d'une *Maison des adolescents* départementale. Les données de santé traitées concernaient les antécédents médicaux, les traitements antérieurs et en cours. La liste des destinataires comportait aussi bien des professionnels de santé, à l'origine des données, que des intervenants sociaux ou éducatifs ainsi que des agents de certaines administrations[1204]. Il est précisé que « *la Commission prend acte que l'habilitation à consulter des données de santé ne peut être attribuée qu'à des personnes soumises au secret professionnel* »[1205] tandis qu'au sein de la liste des destinataires sont distingués ceux qui peuvent *accéder* aux données et ceux qui peuvent se voire *transmettre* les données. L'accès répondrait donc à des conditions plus strictes – celles du partage – que la transmission – échange.

---

informatisé et partagé en cancérologie ; Délibération n°2011-044 du 10 février 2011 autorisant la mise en œuvre par l'Association du réseau périnatal de Champagne-Ardennes d'un traitement de données à caractère personnel ayant pour finalité la mise en œuvre d'un dossier médical informatisé et partagé en périnatalité ; Délibération n°2011-049 du 17 février 2011 autorisant la mise en œuvre par la société « Santé, Autonomie, Services » d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'une plateforme de téléassistance médicalisée assortie de la constitution d'un dossier médico-social informatisé et partagé ; Délibération n°2011-100 du 14 avril 2011 autorisant l'Association du réseau gériatrique de Champagne-Ardennes (RéGéCA) à mettre en œuvre un traitement de données à caractère personnel ayant pour finalité la prise en charge coordonnée et pluridisciplinaire de personnes âgées à travers un dossier médical informatisé et partagé.

[1202] Délibération n°2010-108 du 22 avril 2010 autorisant la mise en œuvre par le Réseau de Réhabilitation Respiratoire de Ville du Pays Basque et des Landes (R3VPBL), d'un traitement automatisé de données à caractère personnel ayant pour finalité le partage de données de santé entre des professionnels de santé dans le cadre d'un réseau de santé.

[1203] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

[1204] « *Les données sont accessibles en interne, selon les problèmes rencontrés par la personne concernée, par le médecin, le psychologue, l'assistante sociale, l'éducateur ou l'enseignant spécialisé, dûment habilités. Les données peuvent également être transmises aux personnels dûment habilités de la Maison Départementale des Personnes Handicapées, la Maison Départementale de l'Enfance et de la Famille, la Protection Judiciaire de la Jeunesse, le Juge des enfants, le médecin traitant, les hôpitaux, les paramédicaux libéraux, les institutions médico-éducatives, ainsi que l'inspection académique* » (Délibération n°2012-036 du 2 février 2012 autorisant l'association pour la Maison des adolescents du Calvados (PASSADO 14) à mettre en œuvre un traitement de données à caractère personnel ayant pour finalité l'accompagnement des adolescents accueillis dans le cadre de la Maison des adolescents du Calvados (Autorisation n°1503607)).

[1205] *Ibid.*

245. Conclusion du second chapitre. Sur le plan du droit pénal spécial, le secret professionnel et la confidentialité ont des champs d'application complémentaires. L'infraction sanctionnant la divulgation de données personnelles peut être commise par toute personne, tandis que celle sanctionnant la violation du secret professionnel vise des catégories de personnes au regard de leur état, profession, mission ou fonction. L'infraction sanctionnant la divulgation de données est, quant à elle, une infraction privée, tandis que l'infraction de violation du secret professionnel est considérée par une partie de la doctrine comme étant fondée sur l'ordre public. S'agissant de l'infraction prévue à l'article 226-22 du Code pénal, elle sanctionne également les divulgations commises par imprudence ou négligence. Enfin, la détermination de l'objet de l'infraction est plus aisée pour la divulgation de données à caractère personnel. Cette complémentarité des champs d'application a une vertu explicative. C'est toutefois au stade de la mise en œuvre de la confidentialité que se situe le véritable apport de la recherche.

La confidentialité est un cadre, elle ne détermine pas qui a accès aux informations, mais indique comment l'information circule en posant des critères dont le contenu lui est extérieur. Concernant les données issues de la prise en charge des personnes dans le système de santé, la mise en œuvre de la confidentialité paraît devoir être déterminée au regard des textes légaux et règlementaires prévoyant les contours du « secret partagé ». Cette idée ne résiste toutefois pas à l'analyse. Pour déterminer qui a accès à quelles données, il faut, de surcroît, rechercher qui sont les tiers autorisés par un texte. L'examen de la doctrine de la CNIL nous apprend également que les critères de nécessité et de confiance sont, en partie, indéterminés. Lorsque la nécessité le dictait, la CNIL a proposé des instruments alternatifs au secret professionnel. .

246. Conclusion du second titre. Le champ d'application des dispositions relatives à la protection des données à caractère personnel se déploie autour de deux notions clés : **les données à caractère personnel** et **le traitement**. Les informations issues de la prise en charge des personnes par un professionnel intervenant dans le système de santé sont des données à caractère personnel sensibles. Ces informations revêtent donc deux qualifications : secrètes en raison du contexte dans lequel elles sont apprises ; à caractère personnel et sensibles en raison de leur nature. La notion de traitement se définit au travers des opérations de traitement. L'étude de ces opérations révèle les antinomies susceptibles d'exister entre le traitement des données et le secret professionnel. Traiter les données ne consiste pas seulement à les mettre en mémoire informatisée mais renvoie aussi à des opérations ayant pour but de faire circuler les données. Tandis que le secret professionnel est une technique de préservation – statique – de

l'information, le traitement des données suppose, plus encore que leur communication – supposant d'en comprendre le sens –, leur circulation.

247. Par ailleurs, un régime spécifique est prévu pour le traitement des données de santé à caractère personnel issues de la prise en charge des personnes dans le système de santé. Les données issues d'informations couvertes par le secret ne sont pas des données de santé ordinaires. On le constate, tant au regard de la moindre place accordée au consentement des personnes concernées qu'au regard des conditions de traitement. Les personnes concernées n'ont pas la maîtrise complète des données les concernant : le législateur a posé des interdictions d'accès au DMP et à l'espace numérique de santé en dépit du consentement, de même qu'il existe une interdiction générale de cession de ces données à titre onéreux. L'on remarque encore que l'assujettissement au secret professionnel est à la fois une condition du traitement de ces données et une conséquence de l'accès. Il convenait, dès lors, d'analyser les conditions de circulation des données.

La protection des données s'organise autour de la notion clef de sécurité. Les responsables de traitement et les sous-traitants ont l'obligation de mettre en œuvre la sécurité de leur traitement. La sécurité des traitements conditionne en partie la confidentialité en ce qu'elle doit empêcher les intrusions des tiers dans les systèmes qui soutiennent les traitements de données. En outre, la confidentialité doit être mise en œuvre de manière positive, elle suppose de déterminer comment les données circulent en posant les critères de nécessité et de confiance. Ces critères sont des contenants et non des contenus. En ce sens, la confidentialité « organise » la protection du « secret médical » plus qu'elle ne protège. C'est en ce sens qu'il convient, selon nous, d'interpréter les propos que la CNIL formulait en 1982 selon lesquels il s'agit « *beaucoup moins de protéger des données nominatives déjà couvertes par le secret médical, que de replacer le dossier médical dans le processus qui va de la saisie à l'utilisation finale, de l'examen du malade au diagnostic, aux soins, à l'expérimentation, à la statistique, à la recherche génératrice de découvertes et de meilleurs soins* »[1206].

[1206] (CNIL, *Rapport d'activité* 1981-1982, p. 21). La CNIL admet, à notre sens, que l'idée de conciliation l'invite à envisager la circulation de l'information comme une « chaine » d'acteurs ayant intérêt à accéder aux données. La circulation des données, même sensibles, implique qu'elle opère la balance entre l'intérêt individuel des malades et l'intérêt général servi par les traitements au regard de leurs finalités.

CONCLUSION DE LA PREMIERE PARTIE

248. Le premier temps de notre étude a été l'occasion de comprendre comment s'organisait la protection du « secret médical » dans le contexte des technologies de l'information et de la communication au travers de l'étude du droit commun. Partant du « secret médical » objet juridiquement protégé, il a été déterminé que l'expression désignait, en premier lieu, des informations. En droit commun, ces dernières sont protégées tant au regard de leur nature que de leur source. Au prisme de la première fonction des dispositifs techniques de l'information, les implications de la représentation des informations ont été mises en lumière. Dès lors que l'information est représentée sur un support, le syntagme « secret médical » désigne un état de secret. Le respect de cet état vis-à-vis des tiers ne dépend plus seulement de l'attitude des personnes. Le « secret médical » ne peut être protégé que par la protection du support qui incarne l'information secrète. L'adaptation du droit commun aux évolutions des technologies de l'information et de la communication permet, en outre, de sanctionner l'appropriation de l'information lorsque celle-ci peut être dissociée de son support.

Le « secret médical », compris comme une situation, est, de surcroît, juridiquement protégé des intrusions réalisées au moyen de dispositifs techniques de l'information et de la communication. Il sanctionne par ailleurs les révélations accomplies à l'aide des dispositifs techniques de la communication.

Les ressources du droit commun offrent une protection multipolaire du « secret médical », prenant en compte tant la fonction d'information des dispositifs techniques que leur fonction de communication.

249. L'étude de la protection du « secret médical » ne pouvait être complète sans une étude du droit de la protection des données à caractère personnel. Le traitement des informations couvertes par le secret étant nécessaire au fonctionnement du système de santé, il convenait de comprendre comment s'articulait la protection accordée au « secret médical » – l'état de secret et l'information secrète – en droit commun avec les dispositions relatives à la protection des données à caractère personnel. Cette entreprise nous a, entre autres, permis de relever que les informations issues de la relation de soin bénéficiaient d'un régime de protection dérogatoire au droit commun de la protection des données à caractère personnel. Leur traitement est notamment conditionné à l'assujettissement au secret professionnel. Certaines dispositions

prévoient, au contraire, que sont soumis au secret professionnel toutes les personnes qui accèdent aux données. Cette spécificité nous a conduit à nous intéresser aux conditions dans lesquelles les données sont rendues accessibles et circulent. Au terme de cette analyse, il est apparu que la confidentialité des données n'avait pas pour objet de protéger le « secret médical » mais d'agencer les secrets « moyens ». Ce que nous avons nommé des « palliatifs », notamment contractuels, en sont un exemple. La première partie de notre étude nous permet de considérer que la protection de l'objet « secret médical » est largement étendue. Les adaptations des mécanismes de protection juridique aux évolutions techniques permettent une protection de l'information et de ses supports et, partant, une protection de l'état de secret.

PARTIE II - LE SECRET COMME MOYEN

250. Le secret est un moyen de préservation des informations. A propos de la protection des créations de l'esprit, Monsieur Vivant affirmait que le secret était même le premier moyen de réservation des informations : « *Quel meilleur moyen de conserver pour soi une idée, une technique, une information que de ne pas la communiquer !* »[1207]. Ainsi que nous l'avons expliqué en introduction de cette étude, les énoncés normatifs et la doctrine – lorsqu'elle adopte une posture dogmatique et reproduit le contenu du discours-objet – utilisent le syntagme « secret médical » pour désigner le secret professionnel « médical »[1208]. Le secret professionnel est la norme « qui protège », c'est un secret « moyen ». Afin de mener à bien notre étude, il importe donc de traiter des rapports entre la norme instituant le secret professionnel, moyen de réservation de l'information, et les technologies de l'information et de la communication. C'est, dès lors, sous un prisme différent de notre étude du secret « objet » qu'il faut se saisir de cette question.

251. Le traitement des données est dynamique, il suppose la circulation. Il est, par ailleurs, possible d'observer que la confidentialité est un moyen d'organiser et de construire le « parcours » des données issues de la relation de soin. Ces éléments laissent entrevoir une contradiction entre les finalités assignées aux traitements des données et la finalité première du secret professionnel qui est de préserver les informations à caractère secret. Cette contradiction devient visible en adoptant un angle de vue auquel nous sommes, jusqu'alors, resté aveugle : les traitements de données de santé à caractère personnel issues de la relation de soin sont généralement mis en œuvre pour des finalités d'intérêt public. Or, le moyen juridique de préservation de l'information que constitue le secret professionnel souffre de la dualité de ses fondements. Lorsqu'il s'agit d'en affaiblir la portée, afin d'obliger le professionnel à réveler certaines informations, le fondement d'ordre privé sera mis en balance avec d'autres intérêts[1209]. Ainsi, dans le domaine de la santé et de manière plus générale, la doctrine a constaté

[1207] M. VIVANT, « La privatisation de l'information par la propriété intellectuelle », *Revue internationale de droit économique* 2006/4, t. XX, pp. 361 à 388, spéc. p. 365.
[1208] V. *supra* n° 5.
[1209] J.- D. SARCELET, « La confidentialité des informations de santé peut-elle tenir face à la protection d'autres intérêts légitimes ? – Le rôle du juge dans la confrontation des intérêts légitimes en présence », *D.* 2008, p. 1921 ;

un double mouvement de généralisation du secret professionnel et de multiplication des permissions et obligations de révéler[1210]. Sous le prisme étatique, les traitements de données sont des instruments au service de l'intérêt public. Cette donnée d'ordre factuel qui doit être au centre de l'étude des rapports entre les technologies de l'information et de la communication et secret professionnel. Plus précisément, c'est le traitement des données qui nous intéresse. Le fonctionnement de nombreux dispositifs visant la sécurité publique, la maîtrise des dépenses, la continuité et l'accès au soin, la qualité des soins, la recherche dans le domaine de la santé, dépendent de la mise en œuvre du traitement des données issues de la relation de soin. Le secret professionnel se présente alors comme un obstacle à l'utilisation efficace des dispositifs nécessitant le traitement des données, en ce qu'il est un frein à la circulation des données. Nous procèderons donc à une évaluation de la portée du secret professionnel, comme secret « moyen », eu égard aux finalités assignées aux traitements des données issues de la prise en charge des personnes par le système de santé **(Titre 1)**.

252. En outre, il est possible d'observer, au travers de la doctrine de la CNIL, que le secret professionnel est envisagé comme un moyen parmi d'autres de protéger les données issues de la prise en charge des personnes dans le système de santé. La CNIL a ainsi proposé aux acteurs de mettre en œuvre d'autres instruments imposant de ne pas communiquer les données. S'ils peuvent être juridiques – citons les clauses de confidentialité –, certains sont extérieurs au droit. Ce recours aux moyens techniques comme « secret » moyen mérite d'être approfondi. Nous avons souligné, en introduction de cette étude[1211], que les dispositifs techniques étaient des moyens de régulation des conduites. Or, ils constituent également des secrets « moyens » en ce qu'ils peuvent préserver les données des intrusions et des révélations **(Titre 2)**.

C. BERGOIGNAN-ESPER, « La confidentialité des informations de santé peut-elle tenir face à la protection d'autres intérêts légitimes ? », *D.* 2008, p. 1918.

[1210] Par exemple : M. BENEJAT-GUERLIN, « Que reste-t-il de la protection pénale du secret médical ? », *AJ pénal* 2017, p. 368 ; M.-A. FRISON-ROCHE, « Critère des intérêts et secret professionnel », *in Les entretiens du Palais*, *Gaz. Pal.*, 18 févr. 2005, pp. 78-81 ; B. PY, « Le secret professionnel : le syndrôme des assignats ? », *AJ pénal* 2004, p. 133 ; M. COUTURIER, « Que reste-t-il du secret médical ? », *in Mélanges en l'honneur de Gérard Mémeteau. Droit médical et éthique médicale : regards contemporains*, LEH Édition, 2015, pp. 351-360.

[1211] V. *supra,* n° 13.

TITRE I. Le secret comme moyen en droit

253. Le secret professionnel est à la fois une condition du traitement des données issues de la relation de soin et une conséquence de la réutilisation ou de l'accès à ces données. Nous avons utilisé l'image du phénomène de recursivité pour expliquer ce mouvement. Ainsi, le secret professionnel se présente comme l'une des principales conditions au traitement, à l'accès et à la réutilisation des données. La CNIL a d'ailleurs parfois incité le législateur à soumettre au secret professionnel certaines catégories de personnes.

La doctrine a dégagé les critères de soumission au secret professionnel, ces derniers ayant été, depuis lors, régulièrement remis en cause[1212]. Certains affirment, au regard du mouvement de généralisation du secret professionnel, que le critère de l'assujettissement au secret professionnel dans le domaine de la santé tiendrait désormais à la nature des informations. Nous synthériserons les approches des auteurs et analyserons notamment cette question sous l'angle de l'accès et de la réutilisation des données. Les critères de soumission au secret professionnel étant intimement liés à la portée de la norme, cette étude nous permettra de porter un premier regard sur les conséquences de l'utilisation des technologies de l'information et de la communication sur le secret professionnel, « secret médical » moyen **(Chapitre 1)**. Ce regard ne peut porter suffisamment s'il n'est pas procédé à un examen des faits justificatifs et des possibilités, pour les professionnels qui y sont soumis, d'opposer le secret. La multiplication des premiers et la restriction des secondes entraîne une dilution du secret professionnel **(Chapitre 2)**.

[1212] M. BENEJAT, *La responsabilité pénale professionnelle*, préf. J.-C. SAINT-PAU, coll. Nouvelle bibliothèque de thèses, vol. 111, Dalloz, 2012 ; M. CONTIS, *Secret médical et évolutions du système de santé*, préf. C. NEIRINCK, coll. Thèses, LEH Editions, 2010.

Chapitre 1 - La généralisation du secret professionnel

254. « *Est punissable, la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire* »[1213]. Si les termes du texte d'incrimination paraissent clairs, la question des critères de soumission au secret professionnel a connu, à l'instar de toutes les interrogations àu propos de cette règle juridique, des réponses jurisprudentielles disparates. La doctrine a souvent essayé de systématiser ces réponses, sans jamais y parvenir tout à fait. Notre objectif n'est pas de renouveler encore l'approche générale de ce problème. Il s'agit de montrer que cette inflation, au moins dans le domaine de la santé, est liée à l'utilisation des dispositifs techniques de l'information et de la communication et plus particulièrement au traitement des données à caractère personnel dans le domaine de la santé. Il nous importe également de révéler le rôle joué par le CNIL. Pour ce faire, nous reviendrons, de la manière la plus synthétique possible, sur les critères posés par le législateur et sur ceux dégagés par la doctrine (**section 1**), avant de proposer notre analyse. Il en ressort qu'un critère unique conditionne l'assujettissement au secret professionnnel s'agissant du traitement des données à caractère personnel issues de la prise en charge des personnes dans le système de santé **(section 2)**.

Section 1 - Une pluralité de critères

255. Si, par simplification, il est présenté une « mutation » des critères de désignation, il s'agit toujours de constructions doctrinales qui se sont succédées en fonction de l'évolution des textes et de la jurisprudence. Nous présenterons donc ces critères tels qu'ils ont été mis en exergue (**paragraphe 1**). Par ailleurs, l'on constate qu'il existe, au sein du Code de la santé publique, plusieurs secrets professionnels en ce sens qu'ils n'ont pas tous la même portée. (**paragraphe 2**)

[1213] CP, art. 226-13.

§ 1 - La mutation des critères de désignation

256. Sont soumises au secret, les personnes qui sont dépositaires d'une information à caractère secret « *soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire* »[1214]. La condition préalable de l'infraction en tant qu'elle décrit une situation juridique qui représente la valeur sociale juridiquement protégée doit être qualifiée au regard d'une définition extra-pénale[1215]. L'une des difficultés de l'étude de l'infraction de violation du secret professionnel consiste dans le fait que la profession, la fonction, l'état ou la mission temporaire sont des notions polysémiques, la doctrine s'est donc attachée a dégager des critères permettant de distinguer entre les professions, les fonctions ou les missions pouvant « *rationnellement être parées du secret* »[1216]. Il convient donc de présenter l'évolution des constructions doctrinales **(A)** avant d'en envisager les conséquences **(B)**.

A - Présentation de la mutation

257. Le critère de la profession a fait l'objet de nombreuses réflexions, il s'est révélé insuffisant à systématiser les réponses jurisprudentielles **(1)**. Les autres critères dégagés par la doctrine ont également été relativisés au fil des évolutions législatives **(2)**.

1 - La profession un critère insuffisant

258. Le mode désignation des personnes soumises au secret a comme particularité de ne pas mentionner les professions, les missions, les fonctions et les états qui sont visés **(a)**. Afin de systématiser l'approche du secret professionnel, la docrine a cherché à asseoir la désignation sur le critère de la profession, puisqu'il s'agit bien d'un « secret professionnel ». L'évolution de la jurisprudence et la multiplication des textes de désignation ont conduit les commentateurs à admettre que ce critère était dépassé **(b)**.

[1214] CP, art. 226-13.
[1215] B. THELLIER DE PONCHEVILLE, *La condition préalable de l'infraction*, préf. A. VARINARD, PUAM, 2010, n° 23 *;* L. ROUSVOAL, *L'infraction composite : essai sur la complexité en droit pénal*, th. dact. ss. la dir. de P. MORVAN, soutenue en 2011, Université Rennes I, n° 26.
[1216] A. LEPAGE et H. MATSOPOULOU, *Droit pénal spécial*, coll. Thémis droit, PUF, 2015, n° 541.

a - La recherche des critères, une nécessité liée au mode de désignation

259. A propos de l'ancien texte d'incrimination. L'incrimination définie à l'article 226-13 du Code pénal sanctionne la révélation d'une information à caractère secret. Celle-ci n'est punissable que lorsque l'acte de révélation émane d'une personne « *qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire* »[1217]. Alors que l'ancien texte punissant la violation du secret professionnel[1218], dressait la liste des personnes qui y étaient soumises et ne visait expressément que les professions médicales[1219], la jurisprudence a amplement contribué à en accroître le nombre. Lors de la refonte du Code pénal en 1994, le législateur a pris acte de presque deux siècles de jurisprudence et d'études doctrinales[1220]. Préférant une définition générique des personnes astreintes au secret professionnel, « *la loi s'est contentée de poser le principe du secret. Elle n'a pas eu pour objet de remettre en cause la dualité de fondements que lui reconnait la doctrine. Reposant sur l'idée de confiance, et destiné, dans un intérêt général et d'ordre public, à garantir la sécurité des confidences liées à l'exercice de certaines professions, le secret professionnel revêt à l'évidence un aspect social, parfois prédominant ; mais il dérive aussi de l'intérêt privé et sa force varie selon la diversité des situations* »[1221].

260. L'absence de désignation par le texte d'incrimination actuel. Lors des travaux préparatoires de la loi n° 92-684 du 22 juillet 1992 portant réforme des dispositions du Code pénal[1222] relatives à la répression des crimes et délits contre les personnes[1223], la complexité de la législation relative au secret professionnel avait été soulignée et la critique portait

---

[1217] CP, art. 226-13.
[1218] Ancien CP, art. 378.
[1219] « *Les médecins, chirurgiens et autres officiers de santé, ainsi que les pharmaciens, les sages-femmes* » (Ancien CP, art. 378).
[1220] B. BOULOC, J. FRANCILLON, Y. MAYAUD, G. ROUJOU DE BOUBÉE, *Code pénal annoté. Article par article Livres I à IV*, Dalloz, 1996, p. 398.
[1221] *Ibid.*
[1222] Résultant d'une succession de lois : Loi n° 92-683 du 22 juillet 1992 portant réforme des dispositions générales du code pénal ; Loi n° 92-684 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes ; Loi n° 92-685 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les biens ; Loi n° 92-686 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre la nation, l'État et la paix publique.
[1223] Loi n° 92-684 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes (*JORF* n° 169, 23 juill. 1992 p. 9875).

principalement sur l'existence de « *dispositions spécifiques, réparties dans l'ensemble de notre droit, ayant imposé un* ***secret voisin****, à certaines professions. Par ailleurs, on relève, dispersées dans la législation française, diverses règles de confidentialité,* ***encore différentes, mais renvoyant aux peines prévues à l'article 378*** »[1224]. A la lecture des travaux préparatoires de la loi du 22 juillet 1992, on constate que la volonté du législateur a été de « *synthétiser* » le texte et surtout de *« **renoncer à la distinction** faite dans les termes entre « les médecins, chirurgiens et autres officiers de santé, ainsi que les pharmaciens, les sages-femmes » et les « autres professions »* »[1225]. Si l'objectif de simplification semble atteint, il est souvent déploré un manque de clarté et de précision du texte[1226]. Cette rédaction de l'incrimination n'a pas mis fin aux incertitudes, certains auteurs ne manquant pas de souligner la labilité des conditions préalables du délit[1227]. Pour déterminer de manière pédagogique les personnes astreintes au secret professionnel, la majorité des manuels consacrés au droit pénal général procèdent en distinguant les méthodes de désignation.

261. Méthodes de désignation de personnes tenues au secret professionnel. La formule retenue par le législateur lors de la rédaction de l'article 226-13 du Code pénal a pu être qualifiée de « *clause de style* »[1228]. Elle permet d'éviter de dresser, au sein du texte d'incrimination, la liste trop mouvante des personnes soumises au secret par un texte spécifique. Par ailleurs, l'absence de désignation permet d'étendre le champ d'application dès lors que le législateur a également entendu laisser au juge répressif le soin d'interpréter le texte afin de

---

[1224] C. JOLIBOIS, Rapport législatif n° 295, p. 150. Nous soulignons.
[1225] C. JOLIBOIS, Rapport législatif n° 295, p. 153. Nous soulignons.
[1226] Une question prioritaire de constitutionnalité a d'ailleurs été posée à propos de l'article 226-13 du Code pénal au motif que ce texte porterait atteinte au principe de légalité des délits et des peines et concernerait spécifiquement la définition de la notion « *d'information à caractère secret* ». La Cour de cassation a refusé de la transmettre. Selon elle « *la question posée ne présente pas, à l'évidence, un caractère sérieux dès lors que l'interprétation de l'article 226-13 du Code pénal, qui définit de manière suffisamment claire et précise le délit de violation du secret professionnel, entre dans l'office du juge pénal* » (Crim., 5 sept. 2012, n° 12-90045 ; *Comm. com. électr*. 2012, comm. 127, obs. A. LEPAGE).
[1227] L'imprécision des éléments de l'infraction du secret professionnel a été mise en exergue par Monsieur Couturier. Après une analyse de la jurisprudence, l'auteur conclut la première partie de sa thèse consacrée à l'étude substantielle du secret professionnel par ces mots « *on ne parvient pas à comprendre pleinement les particularités de la notion de secret professionnel en se livrant simplement à l'analyse des éléments constitutifs du délit qui sanctionne sa violation. En effet, on a constaté qu'il apparaît complexe voire impossible d'établir d'une façon suffisamment certaine et définitive le contenu, la substance de chacun d'eux* » (M. COUTURIER, *Pour une analyse fonctionnelle du secret professionnel*, th. dact. ss. la dir. d'A. PROTHAIS, soutenue le 17 déc. 2004, Université de Lille II, n° 265).
[1228] P. CONTE, *Droit pénal spécial*, 5ème éd., LexisNexis, 2016, n° 495 ; M.-L. RASSAT, *Droit pénal spécial. Infractions du Code pénal*, 8ème éd., coll. Précis, Dalloz, 2018, n° 502.

déterminer au cas par cas les personnes qui doivent être tenues au secret[1229]. Il existe donc une méthode de désignation légale ou réglementaire et une méthode de désignation jurisprudentielle[1230]. Le juge répressif semble avoir toujours fait un usage modéré de son pouvoir d'interprétation, aussi les désignations jurisprudentielles n'ont-elles pas connu d'inflation particulière sous l'empire de l'article 226-13 du Code pénal[1231]. Il n'en est pas de

---

[1229] L'appréciation laissée aux juridictions pénales a fait l'objet de critiques, notamment par un auteur qui estime que « *La jurisprudence ne devrait* […] *normalement avoir aucun rôle dans ce processus puisqu'il ne lui appartient pas – à défaut de légitimité pour cela – de décider qui doit être soumis à l'article 226-13 du Code pénal et qui ne l'est pas* ». (V. PELTIER, *JCl. Pénal Code,* Art. 226-13 et 226-14, Fasc. 20 : « Révélation d'une information à caractère secret – Conditions d'existence de l'infraction – Pénalités », mai 2015 (mise à jour sept. 2016), n° 18).

[1230] Cette distinction des méthodes de désignation est reprise dans la majorité des ouvrages de droit pénal spécial. Il faut toutefois mentionner que, outre le fait que la désignation jurisprudentielle heurte le principe de légalité criminelle (V. PELTIER, « Révélation d'une information à caractère secret – Conditions d'existence de l'infraction – Pénalités », *op. cit.*, n° 18), la technique du renvoi interroge également. Certains auteurs considèrent que l'infraction de violation du secret professionnel est une infraction « *ouverte* » (E. DREYER, *Droit pénal spécial*, 3ème éd., coll. Cours magistral, Ellipses, 2016, n° 418) ou de « *renvoi implicite* » selon Madame Bénéjat, qui analyse : « *Le renvoi est surtout utilisé dans les matières techniques. Il suppose, par principe, que la norme d'incrimination soit dissociée de la norme de comportement. Or, tel n'est pas tout à fait le cas de l'article 226-13 du Code pénal qui ne précise pas seulement les peines encourues mais également l'ensemble des éléments constitutifs, à la seule exclusion de la qualité de l'agent.* » (M. BENEJAT, *La responsabilité pénale professionnelle,* préf. J.-C. SAINT-PAU, coll. Nouvelle bibliothèque de thèses, vol. 111, Dalloz, 2012, note 260, n° 28). Dans le même sens, Madame Peltier remarque que la « *logique particulière du secret professionnel* » consiste dans le fait que l'article « *renvoie implicitement à d'autres textes qui, eux, ont la charge de désigner expressément les personnes tenues à cette obligation spéciale de se taire* » (V. PELTIER, « Révélation d'une information à caractère secret – Conditions d'existence de l'infraction – Pénalités »*, op. cit.*).
Du point de vue légistique, Monsieur MOLFESSIS explique que cette technique consiste dans « *l'invitation formelle, énoncée par la règle, à se reporter à une ou plusieurs autres dispositions. Cette acception large repose sur le fait que le terme de renvoi requiert uniquement que le texte incite* formellement *à « aller voir » ailleurs, c'est-à-dire dans un autre texte* » (N. MOLFESSIS, « Le renvoi d'un texte à un autre », *in* N. MOLFESSIS (ss. la dir.), *Les mots de la loi*, Economica, 1999, p. 55, n° 1). Il ne faudrait toutefois pas en déduire que le renvoi ne peut être qu'explicite. Le même auteur, dressant la typologie des renvois, explique qu'ils peuvent être implicites et consistent alors dans « *la seule invocation d'un concept ou d'un corps de règles qui sont traités ailleurs* » (*Ibid*., n° 4). Il précise encore que cette catégorie de renvois a « *vocation à trop embrasser, tant il est vrai que toute règle, par hypothèse, renvoie à d'autres* » (*Ibid.,* n° 4). La technique du renvoi est tantôt qualifiée d'utile car ayant pour vertu de propager la règle et de coordonner les règles entre elles (*Ibid.,* n° 6 et svt), tantôt considérée comme une manifestation de la fragilisation du principe de légalité dès lors qu'il en est usé avec excès (Sur la thématique de l'affaiblissement du principe de légalité criminelle, v. E. DREYER, *Droit pénal général*, 5ème éd., LexisNexis, 2019, n° 501 et svt.). En effet, la technique du renvoi engendre un manque de lisibilité quant aux différences de régime entre les devoirs de secrets. La confusion est patente entre le permis et l'interdit, particulièrement en ce qu'il est impossible pour les individus de comprendre l'étendue de leur devoir de silence. Enfin, concernant la multiplication des renvois à l'article 226-13 du Code pénal par des textes dont la valeur juridique diffère (législatifs ou règlementaires), la discussion porte sur l'autonomie infractionnelle des textes de désignation. Dès lors que certains d'entre eux fixent le régime du secret professionnel pour la catégorie de personne à laquelle ils se rattachent, la possibilité d'un conflit de lois entre le texte d'origine et le texte de désignation apparaît (sur l'autonomie infractionnelle de ces textes, v. M. BENEJAT, *La responsabilité pénale professionnelle*, *op. cit.*, n° 28)

[1231] A l'occasion d'un arrêt le juge répressif a rappelé la nécessité d'un texte de désignation : « *si la violation du secret professionnel est un délit général prévu et réprimé par le Code pénal, qui ne se confond pas avec la seule*

même concernant la seconde méthode, puisque de nouvelles personnes sont régulièrement soumises au secret professionnel par des textes législatifs ou règlementaires. C'est un constat unanimement souligné par la doctrine[1232] mais les raisons de cette inflation sont finalement peu étudiées[1233]. Nombre de ces textes fixent, par ailleurs, le contenu de la seconde condition préalable de l'infraction, à savoir ce que sont les informations à garder secrètes pour ces personnes, et précisent l'étendue de ce secret[1234]. Le texte d'incrimination prévoyant la profession, la mission, la fonction ou la mission temporaire comme conditions d'assujettissement, il convient d'apprécier ce que recouvrent ces termes.

b - Un critère dépassé

262. La condition d'assujettissement au secret professionnel : la profession. Selon la définition que l'on entend adopter de la « profession », le champ d'application de l'infraction peut se trouver largement étendu. La question relative à la définition de la profession est peu développée par la doctrine[1235]. Madame Bénéjat fait par exemple le choix d'une définition de la profession fondée sur huit critères doctrinaux, et définie comme « *une activité laborieuse,*

---

violation du secret médical, encore faut-il que des dispositions particulières établissent une obligation de secret sur les informations communiquées aux tiers » (Crim., 3 avr. 2002, n° 11-85571).

[1232] Ainsi Madame Rassat affirme que « *toute nouvelle parution d'une revue qui comporte une chronique sur une législation nouvelle, apporte son lot de nouvelles activités expressément astreintes au secret* » (M.- L. RASSAT, *Droit pénal spécial. Infractions du Code pénal*, 8ème éd., coll. Précis, Dalloz, 2018, n° 502). *Adde* P. CONTE, *Droit pénal spécial*, 5ème éd., LexisNexis, 2016, n° 344 *« le nombre* [de personnes tenues au secret] *n'a fait que s'accroître, par l'effet de textes divers, dont certains font expressément un renvoi à l'article 226-13* » ; M. VERON, *Droit pénal spécial*, 7ème éd., coll. Université, Sirey, n° 371 : « *La tendance contemporaine va nettement dans le sens d'une multiplication de cette référence au secret, notamment à l'occasion de la création de commissions administratives dont il est devenu impossible de prétendre établir une liste exhaustive* » () ; B. PY, « Secret professionnel : le syndrome des assignats ? », *AJ pénal*, 2004, p. 133, l'auteur constatant un « *développement apparent* » du secret professionnel.

[1233] Proposant d'en chercher les raisons à partir du fondement du secret professionnel, v. M. BENEJAT, *La responsabilité pénale professionnelle*, *op. cit.*, n° 28 et n° 225.

[1234] Par exemple, la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique soumet au secret professionnel « *les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* » (art. 6-I 2°). Le même article précise qu'ils sont assujettis au secret professionnel « *dans les conditions prévues aux articles 226-13 et 226-14 du code pénal****, pour tout ce qui concerne la divulgation de ces éléments d'identification personnelle*** *ou* ***de toute information permettant d'identifier la personne concernée****. Ce secret professionnel n'est* ***pas opposable à l'autorité judiciaire*** » (Nous soulignons).

[1235] L'on trouve par exemple sous la plume de Mesdames Lepage et Matsopoulou l'idée selon laquelle l'article 226-13 du Code pénal ne s'applique pas seulement « *aux professionnels* stricto sensu » (A. LEPAGE et H. MATSOPOULOU, *Droit pénal spécial*, coll. Thémis droit, PUF, 2015, n° 541).

habituelle, qualifiée, rémunérée, sociale, notoire et licite »[1236]. Partant, l'auteur entend démontrer que la fonction, l'état et la mission temporaire peuvent relever de l'activité professionnelle. Ainsi, la profession serait la condition unique de soumission au secret, condition sans laquelle le secret n'aurait « *de professionnel que le nom* »[1237]. De ce raisonnement, l'auteur déduit que toutes les professions – le terme de profession étant entendu largement – devraient être astreintes au secret. Elle considère d'ailleurs l'infraction punissant la violation du secret professionnel comme la « *seule infraction professionnelle d'application générale* »[1238]. Sa démonstration tend à démontrer que la rédaction de l'article 226-13 du Code pénal suggère que « *chaque professionnel* […] *est pénalement tenu de taire les informations dont il prend connaissance ès qualité* »[1239]. L'auteur précise par ailleurs que le fait que le juge pénal ne reconnaisse pas, parfois, certains professionnels comme faisant partie des professionnels soumis au secret, tient à d'autres explications[1240]. Ainsi, la confiance publique dans la profession, autre critère essentiel de soumission au secret professionnel, ne permettrait d'exclure aucune profession. Le critère s'étendrait alors à toutes les activités pouvant être assimilées à une profession dans son acception large, c'est à dire sans faire de différence entre le caractère social ou altruiste de l'activité puisque « *la discrétion est* […] *une marque de probité à laquelle toute profession est attachée* »[1241]. L'auteur en conclut que le secret est

---

[1236] M. BENEJAT, *La responsabilité pénale professionnelle*, *op. cit.*, n° 4 ; également cité par C. MANGEMATIN, *La faute de fonction en droit privé*, préf. V. MALABAT, coll. Nouvelle bibliothèque de thèses, vol. 135, Dalloz, 2014, n° 103.

[1237] M. BENEJAT, *La responsabilité pénale professionnelle*, *op. cit.*, n° 32.

[1238] *Ibid.,* n° 25.

[1239] *Ibid.,* n° 26.

[1240] Pour l'auteur, « professionnalité » et secret sont intrinsèquement liés. Pour appuyer sa démonstration, Madame Bénéjat précise qu'« *une lecture approfondie de ces arrêts révèle que l'absence de condamnation peut toujours s'expliquer autrement, soit par l'absence d'information secrète, soit par le contexte judiciaire de la révélation* » (*Ibid.*, n° 31). Elle cite, à ce titre, deux arrêts dont l'un (Crim., 4 nov. 1971) concerne le refus par la Cour de cassation de reconnaître que les éducateurs sont soumis au secret professionnel. Ce même arrêt fait l'objet d'une autre interprétation par Monsieur Couturier, lequel considère que ce n'est pas le contexte de la révélation qui a entraîné cette décision mais la marque du refus de reconnaitre le travail social comme un « *groupe constitué et autonome* » (M. COUTURIER, *Pour une analyse fonctionnelle du secret professionnel, op. cit.,* n° 476). Cette différence d'interprétation révèle une acception moins compréhensive de la notion de profession retenue par le second auteur.

[1241] *Ibid.,* n° 35. Cette formulation de l'auteur doit, à notre sens, être accueillie avec une certaine réserve. La discrétion peut en effet être attendue de tout professionnel, toutefois celle-ci ne peut se confondre avec le secret professionnel. Monsieur Py souligne d'ailleurs la différence entre ces deux notions lorsqu'il explique que la discrétion est une « *obligation qui protège l'intérêt de l'entreprise publique ou privée en interdisant des divulgations qui pourraient nuire à l'accomplissement normal ou au bon fonctionnement de l'institution. Elle s'impose à tous les salariés et/ou agents publics et recouvre une étendue très large puisque tout ce qui concerne*

inhérent à la « *professionnalité* »[1242], dès lors tous les professionnels devraient y être astreints si, précise-t-elle, « *ce n'est pas déjà le cas* »[1243]. Une telle idée n'est pas dénuée d'intérêt et a le mérite de la clarté. Toutefois, il existe une raison pour laquelle le législateur a souhaité distinguer ce qui relève de la profession, de la mission, de l'état et de la fonction. Car, si l'on peut procéder à un rapprochement de ces notions, elles recouvrent néanmoins des réalités différentes. L'on peut, sur ce point, s'appuyer partiellement sur l'étude de Madame Mangematin relative à la faute de fonction en droit privé, laquelle opère une différence entre profession, mission et fonction[1244].

263. Le sens de la distinction entre profession, mission, fonction. Tandis que Madame Bénéjat considère que la profession est une fonction en ce qu'elle « *poursuit une finalité altruiste ou sociale* »[1245], Madame Mangematin, démontrant l'autonomie de la notion de fonction par rapport à celle de profession, remarque : « *Pourtant le caractère altruiste doit être distingué d'un simple caractère social. En atteste également le fait que la considération de l'intérêt d'autrui ne joue qu'un rôle congru dans l'exercice de la profession en général, à l'exception de certaines professions en particulier* »[1246]. L'auteur note que si une fonction peut devenir une profession et qu'il existe des activités professionnelles correspondant à une fonction, profession et fonction ne peuvent se confondre en raison du caractère altruiste de la fonction qui ne se retrouve pas dans toutes les professions[1247]. Elle précise, de surcroît, que mission et fonction ne se confondent pas non plus, la différence étant d'ordre temporel. L'auteur explique encore que mission et fonction figurent souvent côte à côte dans les textes législatifs, et cite, entre autres, l'article 226-13 du Code pénal. La mission est parfois conçue, selon elle, comme une « *alternative à la notion de fonction, tantôt comme l'objet de la fonction* »[1248]. Afin d'appuyer la différence entre les deux, l'auteur poursuit : « *La première définition semble*

---

la vie interne et l'action de l'entreprise est présumé confidentiel. Dans le secteur privé, le fondement de l'obligation émane du contrat de travail et de la nécessaire confiance de l'employeur dans la discrétion de ses collaborateurs. Un manquement à la discrétion peut conduire à une rupture de la relation de travail et à un licenciement pour faute. Dans le secteur public, c'est l'article 26 de la loi n° 83-634 du 13 juillet 1983 portant statut des fonctionnaires qui impose le respect de la discrétion, dont la violation peut entraîner des sanctions disciplinaires allant jusqu'à la révocation » (B. PY, « Le secret professionnel, une obligation de se taire », *JurisAssociations* 2008, n° 386, p. 12).

[1242] M. BENEJAT utilise ce néologisme pour désigner « *l'exercice de fonctions professionnelles* ». (M. BENEJAT, *La responsabilité pénale professionnelle*, *op. cit.*, n° 4).

[1243] *Ibid.,* n° 41.

[1244] C. MANGEMATIN, *La faute de fonction en droit privé*, *op. cit.*

[1245] M. BENEJAT, *La responsabilité pénale professionnelle*, *op. cit.*, n° 132 et svt, *spéc.* n° 140.

[1246] C. MANGEMATIN, *La faute de fonction en droit privé*, *op. cit*. n° 103.

[1247] C. MANGEMATIN, *La faute de fonction en droit privé*, *op. cit*., n°103 et 104.

[1248] *Ibid.,* n° 115.

dérangeante car en tant qu'alternative à la notion de fonction, la mission apparaît incompatible avec la fonction. Le critère de cette distinction est temporel : la mission renverrait à une activité plus brève que la fonction. […] *La solution* […] *réside dans la scrutation des définitions ajuridiques des deux notions : alors que la fonction désigne le* « rôle spécifique (d'un élément, d'un organe) dans un ensemble »*, la mission renvoie à la* « charge donnée à quelqu'un d'aller accomplir quelque chose » ou au « but que l'on se donne à soi-même avec le sentiment d'un devoir ». *De ceci pourrait résulter que la fonction correspond à un rôle, un statut, une qualité, un titre dont l'effectivité suppose que soit accompli un ensemble de prestations dans l'intérêt d'autrui. La mission correspondrait à l'une de ces prestations. Dès lors, la mission pourrait tout aussi bien être évoquée en tant qu'objet de la fonction, que de manière autonome et alternative à la fonction* »[1249]. La distinction pourrait être illustrée par l'interprétation faite de l'article L. 1110-4 du Code de la santé publique[1250]. Une majorité de la doctrine considère, en effet, à cet égard, que les bénévoles intervenant dans le système de santé sont également soumis au secret[1251], ce qui aurait pour conséquence de rendre inopérante toute tentative d'unification sous la bannière de la « *profession* » et permettrait en outre d'asseoir la distinction entre mission et fonction, la première se distinguant principalement par son caractère temporel.

264. Une acception restrictive de la profession. La proposition de Madame Bénéjat nous semble donc devoir être relativisée. D'abord, il n'est pas possible d'affirmer que l'état, la mission et la fonction puissent être assimilés à la profession. Ensuite, l'activité « sociale » ne peut se confondre avec l'activité « altruiste ». Cette différence semble pouvoir expliquer que certains professionnels soient astreints au secret et d'autres non. C'est ce que l'on perçoit au travers de la définition sociologique de la profession, développée par Monsieur Dubar[1252]. Cette théorie, qui trouve un écho dans les pays de *Common Law*, fait une distinction entre les professions qui ont des activités que l'on peut qualifier de supérieures car d'intérêt public, et ce

---

[1249] *Ibid*.
[1250] CSP, art. L. 1110-4.
[1251] B. PY, « Le secret professionnel : une obligation de se taire », *op. cit.* ; Il s'agit sans doute ici d'une mission, comprise comme objet de la fonction mais renvoyant à une définition autonome. Quoiqu'il en soit, l'activité bénévole ne peut en aucun cas être considérée comme professionnelle puisque, par essence, elle n'est pas rémunérée (R. SAVATIER, « Contribution à une étude juridique de la profession », *in Etudes de droit commercial offertes à J. Hamel*, Dalloz, 1961, p. 1, spéc. p. 3).
[1252] C. DUBAR, P. TRIPIER et V. BOUSSARD, *Sociologie des professions*, 4ème éd., coll. U, Armand Colin, 2015.

qui est désigné dans les pays anglo-saxons par le terme « *occupation* ». Les critères de distinction entre les *travailleurs* et les *professionnels* sont multiples. Pour ne pas les citer tous, l'exercice libéral et intellectuel, l'autorégulation de la profession – dont la déontologie et l'existence d'un ordre professionnel sont les manifestations les plus prégnantes – et le caractère altruiste des professions[1253] sont des marqueurs de l'appartenance à une profession selon une approche sociologique. Le parallélisme entre cette définition de la profession et les professions originairement soumises au secret professionnel en droit français a pu être relevé[1254], et demeure exact pour les professions historiquement soumises au secret telles que celles du droit et de la médecine. La confiance publique et la nécessité justifient par ailleurs le secret professionnel des fonctionnaires.

265. Atténuation des particularités de la profession. Il apparaît néanmoins que la conception restrictive de la profession est de moins en moins opérante en raison de mutations sociales profondes : les professions sont fortement soumises à la logique du marché et perdent progressivement les caractéristiques qui permettaient de les distinguer d'autres activités[1255]. Aussi, de nombreux auteurs n'opèrent plus de distinction entre ce qui relève de la fonction, de la mission temporaire, de l'état ou de la profession, ni ne distinguent les professions pour s'essayer à une quelconque classification. Ils leur préfèrent le terme générique d'« *activités* »[1256] tant le champ des notions de fonction, de mission et de profession est vaste et pourrait, en définitive, trouver à s'appliquer à des situations innombrables. De plus, chacune

---

[1253] C. DUBAR, P. TRIPIER et V. BOUSSARD, *Sociologie des professions, op. cit.*, p. 9.

[1254] Tel est le cas de Monsieur Couturier, selon lequel la profession est un critère de soumission au secret professionnel. Plus encore, la soumission au secret professionnel aurait, selon lui, pour fonction de faire reconnaître l'existence d'une profession. Partant, le secret professionnel serait un déterminant de la profession (M. COUTURIER, *Approche fonctionnelle du secret professionnel*, *op. cit.*, n° 79 et 460). Cette même idée est défendue par Madame Frison-Roche lorsqu'elle affirme que « *c'est le secret qui fait le professionnel, qui crée la profession* ». (M.-A. FRISON-ROCHE (ss. la dir.), *Secrets professionnels*, coll. Essais, éd. Autrement, 1999, p. 23).

[1255] Ce constat est généralisé, ses symptômes sont constatés dans toutes les professions libérales. S'agissant par exemple des professions du droit, v. C. JAMIN, « Services juridiques : la fin des professions ? », *Pouvoirs*, 2012/1, n° 140, pp. 33-47. L'auteur explique les raisons, s'agissant des professions du droit, « *de l'abandon d'une logique professionnelle au profit d'une logique de marché* », évoquant le principe de libre concurrence au sein de l'Union européenne. L'on constate également une remise en cause de leur autorégulation : J. MORET-BAILLY, « Les rapports entre la loi et les déontologies des professions de santé après la loi du 4 mars 2002 », *RDSS* 2003, p. 581.

[1256] Monsieur Couturier utilise ce terme générique à de très nombreuses reprises (M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*). L'énumération des activités telles que mentionnées par le Code pénal n'a plus grand sens et le terme « activités » paraît pouvoir s'y substituer aisément tant la distinction entre profession, état, fonction et mission temporaire a perdu de son intérêt avec l'effacement de la place des professions dans la société.

de ces notions connaît des sens ajuridiques qui ressurgissent parfois en droit positif[1257]. L'on peut, à l'instar d'un auteur, considérer que le secret est désormais *missionnel*[1258], la mission étant sans doute le terme le plus compréhensif de la liste prévue à l'article 226-13 du Code pénal.

Dès lors que le critère de la profession n'a plus grand intérêt pour permettre d'opérer la distinction entre les situations définies à l'article 226-13 du Code pénal – d'autant que, dans le langage courant, elles peuvent recouvrir des activités diverses et possèdent tout de même des sens analogues[1259] –, il faut rechercher les autres conditions qui guident la jurisprudence et le

---

[1257] Comme le montre l'assimilation ponctuelle, par le législateur, de la mission et de la fonction, telle que le relève Madame Mangematin (C. MANGEMATIN, *La faute de fonction en droit privé*, *op. cit*., n° 115).

[1258] C. BRETON-RAHALI, *Le secret professionnel et l'action médico-sociale*, *op. cit.*, p. 45.

[1259] Il est utile de rappeler qu'est sans doute à l'œuvre ce que Christian Atias considérait comme « *l'écran complexe* » de la connaissance du droit : un phénomène de « *sédimentation* » que, ni le législateur, ni le juge, ni le chercheur ne maîtrisent et qui est à l'œuvre « *dans l'ordre sémantique selon des mouvements extrêmement variables selon les époques, les cultures, les milieux, les domaines et, aussi, selon les mots et leurs emplois.* […] *S'ils ont tous un âge et une histoire, les mots ont une force variable ; certains sont plus que d'autres chargés de significations diverses. Ils ouvrent, à la pensée, plusieurs chemins en concurrence et en ferment ou, au moins, les rendent moins disponibles, plus difficiles d'accès* » (C. ATIAS, *Questions et réponses en droit*, PUF, coll. L'interrogation philosophique, 2009, n° 267). Ainsi en est-il des termes de « profession », de « mission », « d'état » et de « fonction ». Le mot « profession », s'il est aujourd'hui majoritairement compris comme signifiant une activité ou un corps de métier, a d'abord signifié une « *déclaration publique de ses sentiments, ses idées ou sa foi* » (1155). Il n'est utilisé pour qualifier un groupe représentant une certaine force sociale qu'à partir du XVIII[e] siècle (dans ce sens, pour la première fois : N. DE CONDORCET, *Esquisse d'un tableau historique des progrès de l'esprit humain*, 1793-1794), mais il a toujours porté le sens emprunté au latin *professio* c'est-à-dire « « *déclaration publique, action de se donner comme* » d'où « *état, condition, métier* » dérivé du radical du supin *profiteri* « *déclarer ouvertement, officiellement, se donner comme* » (TLFi, *V°* « Profession »). Ainsi, la profession est à la fois un état et une action. L'« *état* » rejoint donc la profession dans ses racines les plus anciennes et c'est peut-être pourquoi il est difficile d'en proposer une seule définition qui en exclurait le second terme. Le mot « *état* » contient d'ailleurs, depuis le XIII[e] siècle la profession comme élément de définition : « 1285 « *situation sociale ou professionnelle, condition* » (*Ibid.*). Puis, au XIV[e] siècle, il désigne une « *charge, position* » (*Ibid.)*. La fonction se définit aussi, à partir de 1566 comme l'« *exercice d'une charge* » (*Ibid*.). Quant à la « mission », outre son sens religieux, le terme est d'un usage plus récent mais s'entend également d'une charge ou d'une fonction (*Ibid.)*. Cette brève plongée dans l'étymologie a pour but d'appuyer l'idée selon laquelle il est impossible de prétendre trouver une réponse dans l'une ou l'autre définition des termes utilisés par le législateur. Cela pose toutefois problème, dès lors que les termes ne renvoient pas à une situation de droit ou de fait qui serait clairement identifiable, tant elle recouvre d'hypothèses. La question de la valeur sociale juridique protégée, du fondement du secret professionnel demeure difficile à découvrir. Les tenants d'une définition sociologique de la profession admettront aisément que c'est la confiance dans la profession, voire même la profession, qui est pénalement protégée, tandis qu'admettre que le secret serait une obligation générale (qui peut être qualifiée de *fonctionnel* comme le propose Monsieur Py) invite à envisager le secret fondé sur l'intérêt de la personne concernée par les informations. Sont ainsi expliquées, en partie, les controverses opposant protection de la profession et protection de l'intimité de la vie privée de celui qui se confie. En toutes hypothèses, il faudrait encore rappeler qu'« *Aucune notion de droit, aucun principe, aucune qualification, aucune catégorie ne sont de purs instruments que le juriste sortirait d'un tiroir au moment où il en a besoin, et qu'il maitriserait. L'idée même de « concept opératoire » est un piège où la pensée se laisse prendre. Nul ne sait ce qui s'opère lorsqu'un concept juridique est mis en œuvre,*

législateur. Bien qu'elles soient difficiles à identifier[1260], la doctrine a développé certains critères qui, un temps admis de manière unanime, ont subi le même sort que la profession, une certaine relativisation : la qualité de confident nécessaire et la confiance publique. Ces deux critères ont connu des évolutions qu'il faut brièvement retracer.

2 - L'évolutions des autres critères

266. Le premier critère, la qualité de confident nécessaire. Aussitôt après l'avoir évoquée, il faut admettre que la notion de confident nécessaire[1261] comme critère d'assujetissement au secret professionnel est largement dépassée, et ce depuis la réécriture du texte d'incrimination, bien qu'elle soit encore utilisée périodiquement par les juges[1262]. C'est le terme de « dépositaire » qui figure à la lettre l'article 226-13 du Code pénal. Ce terme sied mieux à la conception de l'information à caractère secret comprise comme « *l'ensemble des informations venues à la connaissance du professionnel* »[1263]. Admettre que la personne dont l'activité est susceptible d'être soumise au secret professionnel n'est pas seulement le *confident* mais peut également être simple *dépositaire* de l'information à caractère secret implique qu'un grand nombre de personnes peut être concerné. Plus encore, le fait d'être amené à connaître des informations sur les individus dans le cadre d'une activité quelconque pourrait constituer une condition suffisante. C'est pourquoi le champ d'application de l'infraction s'est étendu à

---

parce que nul ne sait où ce concept entraîne la pensée. Sa formation n'est jamais acquise. Elle le deviendrait si le droit s'immobilisait, cessait de vivre, de se nuancer à la rencontre de difficultés toujours nouvelles » (C. ATIAS, *Questions et réponses en droit*, *op. cit.*, n° 271).

[1260] M. VERON, *Droit pénal spécial*, 17ème éd., coll. Université, Sirey, 2019, n° 372.

[1261] Ainsi, Messsieurs Floriot et Combaldieu définissaient les confidents nécessaires comme : « *ceux dont l'état ou la profession oblige les tiers à leur confier des secrets, et qui seraient dans l'impossibilité d'accomplir correctement leur tâche si, par crainte d'une indiscrétion, on devait les leur taire* » (R. FLORIOT et R. COMBALDIEU, *Le secret professionnel*, Flammarion, 1973, p. 20). Les exemples jurisprudentiels reprenant la formule sont nombreux : Par exemple, concernant le refus de soumettre au secret professionnel un directeur du personnel d'une compagnie d'assurance, considérant qu'il n'est pas un « *confident nécessaire* » : Crim., 19 nov. 1985, n° 83-92813, *Bull. crim.,* n° 364 ; *Dr. soc.* 1986, p. 419, obs. J. SAVATIER. Encore, jugeant qu'un comptable est tenu au secret professionnel : Chambéry, 22 mai 1986, *JurisData* : n°1986-600290 ; concernant un conseiller fiscal : Paris, 11 janv. 1985, *JurisData* : n° 1985-600480.

[1262] Quelques décisions prises sous l'empire de l'article 226-13 du Code pénal : CourEDH, 18 mai 2004, *Editions Plon c/ France*, n° 58148/00 ; A propos des assureurs, affirmant qu'ils ne sont pas soumis au secret puisqu'ils ne sont pas des « confidents nécessaires » : Crim., 28 sept. 1999, n° 98-86762 ; Angers, ch. corr., 2 juill. 1998, *JurisData* : n° 1998-045334 ; et à propos du directeur général d'une compagnie d'assurance particulièrement : Crim., 14 mai 1996, n° 93-80982.

[1263] V. également V. PELTIER, « Révélation d'une information à caractère secret – Conditions d'existence de l'infraction – Pénalités », *op. cit.*, n° 34. De la confidence, le secret s'entend désormais comme tout ce que le professionnel peut apprendre, constater, entendre et déduire dans l'exercice de son activité.

d'innombrables activités à raison desquelles les personnes ont à connaître des informations concernant les individus[1264]. C'est, en outre, pourquoi il n'est plus nécessaire d'opérer de distinction en fonction de la nature des activités. Moins marqué que le terme *dépositaire*[1265], il faudrait sans doute parler de *détenteur* de l'information[1266]. Tant la « *confidence* » que la « *nécessité* » de l'information ne constituent plus des critères intangibles d'assujettissement au secret professionnel. S'agissant de la « *nécessité* », elle doit en effet être nettement relativisée, suivant la profession dont elle est le corollaire[1267]. Néanmoins, l'existence d'un second critère interdit de se prononcer dans le sens d'une généralisation du secret professionnel à toutes les personnes qui seraient amenées à connaître des informations intimes sur les personnes dans le cadre de leurs activités.

267. Le second critère, la confiance publique. L'idée selon laquelle l'infraction de violation du secret professionnel sanctionnerait une « *confiance trahie* »[1268] est ancienne, et fait écho au critère du « *confident nécessaire* ». C'est sur ce diptyque que s'est construite la théorie d'un secret professionnel protégeant l'intérêt général et résumé, pour le secret professionnel médical, par la célèbre phrase de Louis Portes : « *Il n'y a pas de médecine sans confidences, de confidences sans confiance, de confiance sans secret* »[1269]. La majorité de la doctrine traite encore le secret professionnel sous l'angle de ce rapport de confiance entre un professionnel et

---

[1264] Comme le souligne un auteur : « […] *avec la multiplication à outrance des professionnels tenus au secret, on ne manque pas de s'apercevoir que ce schéma a été bouleversé. De fait, il n'est pas rare que les membres d'une commission ou les participants à une réunion soient tenus au secret sans qu'il existe au départ une quelconque confidence. À titre d'exemple, on citera les membres du directoire du fonds de réserve pour les retraites, les salariés et les préposés* (CSS, art. L. 135-13, al. 4). *Pis, il arrive que des textes disposent que les activités d'un organisme sont couvertes par le secret professionnel, sans que soient désignés ceux qu'il oblige à se taire. On se doute bien qu'il s'agit des personnes qui y ont participé, mais elles ne sont guère des dépositaires puisqu'on ne leur a rien confié.* » (V. PELTIER, « Révélation d'une information à caractère secret – Conditions d'existence de l'infraction – Pénalités », *op. cit.*, n° 28).

[1265] Qui rappelle inévitablement la notion civile propre au contrat de dépôt ainsi que la doctrine l'a autrefois relevé (E. GARCON, *Code pénal annoté*, t. 2, éd. refondue et mise à jour par M. ROUSSELET, M. PATIN et M. ANCEL, Sirey, 1956, art. 378, n° 6-7).

[1266] V. PELTIER, « Révélation d'une information à caractère secret – Conditions d'existence de l'infraction – Pénalités », *op. cit.*, n° 28.

[1267] Le confident était « nécessaire » dans la mesure où son activité l'était elle-même car elle contribuait au bon fonctionnement de la société et y occupait une place centrale. La dissipation des particularités de la profession remet également en cause leur nécessité.

[1268] P. CONTE, *Droit pénal spécial*, *op. cit.,* n° 343 ; M.- A. FRISON-ROCHE (ss. la dir.), *Secrets professionnels*, coll. Essais, éd. Autrement, 1999, p. 15.

[1269] L. PORTES, « *Du secret médical* », communication à l'Académie des Sciences Morales et Politiques, *in A la recherche d'une éthique médicale*, Masson-PUF, 1954.

un individu amené à solliciter ses conseils[1270]. Dans sa recherche visant à proposer une méthodologie pour déterminer les critères de soumission au secret professionnel, Monsieur Couturier précise que les professionnels soumis au secret font partie de « *professions nécessitant la confiance* »[1271]. Confiance qui, sans doute, peut être attendue de tous les professionnels, ce qui a amené Madame Bénéjat à estimer que le secret devrait pouvoir être exigé de la part de tous les professionnels[1272]. Mais la seule confiance dans une personne ne peut, d'une part, justifier la sanction pénale[1273], et trouve, d'autre part, une contradiction dans la jurisprudence[1274]. Enfin, la profession, nous l'avons démontré, est un critère en dérélection. Outre la confiance dans la personne, c'est donc l'importance de son activité dans la société qui explique la soumission au secret professionnel. De plus, eu égard aux évolutions qui viennent d'être exposées et à celles qui vont suivre, il faut d'ores et déjà noter que le caractère nécessaire de l'activité doit être redéfini au regard de ce pour quoi elle fait nécessité. Du confident nécessaire à la profession nécessaire ou au simple détenteur, le « maillage » de la confiance s'est en quelque sorte resserré. L'assujettissement au secret professionnel a longtemps pu se concevoir comme la confirmation qu'il existait un lien de confiance construit par ailleurs, c'est-à-dire socialement, et dont la violation méritait une sanction pénale, tandis que les

---

[1270] V. par exemple A. LEPAGE et H. MATSOPOULOU, *Droit pénal spécial*, *op. cit.*, n° 541; M.- L. RASSAT, *Droit pénal spécial*. *Infractions du Code pénal*, *op. cit.*, n° 575 ; P. CONTE, *Droit pénal spécial*, *op. cit.*, n° 343 ; E. DREYER, *Droit pénal spécial*, 3ème éd., coll. Cours magistral, Ellipses, 2016, n° 418.

[1271] M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*, n° 73 et 74.

[1272] M. BENEJAT, *La responsabilité pénale professionnelle*, préf. J.-C. SAINT-PAU, coll. Nouvelle bibliothèque de thèses, vol. 111, Dalloz, 2012. Il faut noter que l'opposition, *a priori*, entre ces deux auteurs résulte de la définition de la profession. Alors que Monsieur Couturier s'appuie sur la théorie de la sociologie des professions, laquelle différencie professions et métiers sur la base de critères liés à des considérations d'ordre sociologique (niveau d'étude, existence d'une règlementation professionnelle, confraternité…), Madame Bénéjat adopte une définition juridique de la profession, particulièrement large. Il ne s'agit pas de préférer l'une ou l'autre car elles sont tout aussi exactes, simplement aucune de ces définitions ne rend parfaitement compte des raisons pour lesquelles une personne peut être astreinte au secret professionnel.

[1273] Laquelle doit être nécessaire. Sur les travaux classiques concernant la nécessité des délits et des peines : C. BECCARIA, *Des délits et des peines,* coll. La croisée des chemins, ENS, 2009 ; H. RÉMY, *Les principes généraux du Code pénal de 1791*, Société du recueil Sirey et du Journal du Palais, 1910, disponible sur < http://gallica.bnf.fr/ark:/12148/bpt6k6574125r> (dernière consultation le 20 sept. 2019) ; J. DE SOTO, « La responsabilité pénale et la Révolution française », *in La responsabilité pénale*, Travaux du colloque de philosophie pénale (12 au 21 janvier 1959) présentés par J. LÉAUTÉ, travaux de l'Institut de Sciences Criminelles et pénitentiaires, *Annales de la faculté de droit et des sciences politiques et économiques de Strasbourg*, t. VIII, Dalloz, 1961, p. 137 ; M. ANCEL, « Les principes de la Révolution française et le droit répressif moderne », *in La République française*, 1948, p. 79.

[1274] S'agissant du président-directeur général d'une société anonyme : Crim., 5 févr. 1970, *Bull. crim*., n° 56, *D.* 1970, p. 249 ; *JCP G* 1970, II, p. 16311 ; *RSC* 1970, p. 652, obs. G. LEVASSEUR ; un administrateur provisoire d'une société : Crim., 9 oct. 1978, *Bull. crim.,* n° 263 ; *RSC* 1979 p. 560 ; un directeur de foyer d'accueil pour anciens détenus : Crim., 17 mars 1982.

évolutions décrites invitent à concevoir cet assujetissement comme *un moyen de construire la confiance*. Nous aurons l'occasion de développer ces propos lorsque nous envisagerons spécifiquement les personnes soumises au secret dans le système de santé.

268. Une évolution confirmée par l'augmentation des désignations légales et réglementaires. La qualité de confident nécessaire et la nécessité de la profession ont longtemps guidé le législateur dans la désignation des personnes soumises au secret professionnel. En effet, si les catégories classiques de professions tenues au secret professionnel demeurent, elles ne peuvent plus être regardées comme un marqueur de la finalité de l'infraction. Auparavant, les personnes soumises explicitement au secret professionnel par la loi ou le règlement pouvaient être classées dans des catégories réduites : les professions médicales, les personnes participant à l'administration de la Justice et les agents du service public[1275]. Plus tard, ces catégories furent étendues : les professions libérales et intellectuelles, les professionnels des affaires, les agents du secteur public et parapublic ont constitué des catégories plus larges[1276]. C'est à partir de ces catégories de professions, dont le secret professionnel des médecins est l'étalon originel, qu'a été conceptualisée la dualité de fondements du secret professionnel. Si ces « modèles » demeurent, ils ne sont plus significatifs tant les textes légaux et règlementaires assujettissant au secret professionnel sont nombreux et disséminés. Nous en trouverons une illustration au travers de l'étude particulière des personnes soumises au secret en raison du traitement des données à caractère personnel issues de la relation de soin.

B - Conséquences de la mutation

269. Fonctions sociales et diversité des secrets professionnels. Toutes les personnes soumises au secret par les textes *n'ont donc pas la même fonction sociale*. Ainsi en est-il, en comparaison avec les professions médicales et judiciaires, des métiers du chiffre et de la finance

---

[1275] P. GULPHE les distingue ainsi et note déjà, s'agissant de la dernière catégorie : « *L'obligation au secret professionnel constitue une clause de style dans les textes instituant un nouveau service public* » (P. GULPHE, « Le secret professionnel en droit français », *in Le secret et le droit*, Travaux de l'association Henri Capitant, t. XXV, Dalloz, 1974, pp. 110-111.

[1276] Ainsi présentées par : M. COUTURIER, *Pour une analyse fonctionnelle du secret professionnel*, *op. cit.*.

ou encore des agents de la fonction publique, dont les secrets ont une portée moindre[1277]. Si la socialisation des activités[1278] semble guider le législateur quant à l'intérêt de soumettre certaines catégories de personnes au secret, le rôle social de ces personnes au regard de leur activité a une influence évidente sur l'étendue et la portée du secret professionnel de chaque catégorie, comme le remarque Madame Frison-Roche : « *Ce qui va engendrer la multiplicité des secrets, c'est précisément la multiplicité des professions. En effet, sans pousser l'espièglerie, voire la causticité, jusqu'à inverser les causalités, on peut observer qu'il y a un secret militaire parce qu'il y a des militaires, qu'il y a un secret médical parce qu'il y a des médecins, un secret de l'instruction parce qu'il y a des magistrats. Et les offices de ces professions, les moyens et les pouvoirs qui leur sont conférés, les modes de rémunération sont si diversifiés que c'est le pluriel qui s'impose* »[1279]. Or, il paraît désormais bien possible d'inverser les causalités dans la mesure où les frontières de la profession sont progressivement atténuées. Monsieur Py, résume ce constat par une formule : « aujourd'hui, à chacun son métier, à chacun son secret ! »[1280]. Cette observation permet notamment de relativiser l'opposition entre les intérêts protégés par le secret. Le choix du législateur et du juge répressif de soumettre une personne au secret en raison de son activité dépend autant de son rôle dans la société que de la volonté de protéger l'individu qui lui communique des informations. L'un ou l'autre de ces intérêts peut toutefois être prépondérant selon l'activité et la place de l'activité visée dans la société, mais aussi selon la nature des informations que la personne doit obtenir pour remplir son office.

270. Diversité et portée des secrets professionnels. La diversité des secrets professionnels ne consiste pas uniquement dans la pluralité des activités concernées, elle se manifeste surtout quant à la portée de ces secrets. Cette diversité explique d'ailleurs que les secrets professionnels soient étudiés séparément, qu'il s'agisse de définir ce sur quoi porte le secret – la nature des informations – ou d'en déterminer la portée – l'opposabilité. Leur caractère relatif est parfois explicitement affirmé par les textes de désignation, par exemple en restreignant la possibilité

[1277] Ils doivent notamment céder devant les nécessités de fonctionnement du service (R. TUNC, « Le secret professionnel et les relations administratives », *La Revue administrative* 1948/3, p. 18).

[1278] Au sens où elles prennent place dans la société et se construisent une identité propre.

[1279] M.- A. FRISON-ROCHE (ss. la dir.), *Les secrets professionnels*, coll. Essais, Autrement, 1999, p. 21.

[1280] B. PY, « Secret professionnel : le syndrome des assignats ? », *op. cit.*

de conserver le silence lorsque leur témoignage en justice est sollicité[1281]. Le juge est également amené à opérer certaines distinctions[1282]. S'agissant de la nature du secret, c'est-à-dire ce sur quoi porte l'information qui doit être gardée secrète, il est remarquable que les secrets les plus anciens – que l'on pourrait qualifier de « véritables » – sont également ceux pour lesquels la nature du *secret-fait* connaît la plus grande amplitude. Alors qu'il est admis que le secret des médecins et des professionnels de santé couvre « *l'ensemble des informations* »[1283] venues à leur connaissance, il en est de même du secret des avocats[1284]. A l'inverse, certains textes de désignation précisent les informations couvertes par le secret professionnel ; il en est ainsi, par exemple, du secret professionnel des opérateurs techniques de l'internet[1285]. Ce phénomène a conduit à parler non pas *du* secret professionnel mais *des* secrets professionnels puisque « *les devoirs de silence de chaque profession présentent des régimes et des motivations différents* »[1286]. Toutefois, cette distinction des régimes est de plus en plus poreuse, notamment dans le système de santé.

§ 2 - La multiplication des secrets professionnels au sein du système de santé

271. La multiplication des textes de désignation et la diversité des secrets professionnels est un phénomène général mais il se constate de manière plus prégnante dans le système de santé.

[1281] Une illustration : les prestataires techniques de l'internet (L'article 6 iii-2 de la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique qui dispose que « *les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* » (art. 6 i-2 de la même loi) « *sont assujetties au secret professionnel dans les conditions prévues aux articles 226-13 et 226-14 du code pénal, pour tout ce qui concerne la divulgation de ces éléments d'identification personnelle ou de toute information permettant d'identifier la personne concernée. Ce secret professionnel n'est pas opposable à l'autorité judiciaire* »). C'est encore le cas des membres et personnels de certaines autorités administratives indépendantes, par exemple des membres et personnels de l'Autorité de régulation des jeux en ligne (Loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, art. 36).

[1282] Par exemple, s'agissant du secret professionnel des métiers de la banque dont la portée a toujours été considérée comme moindre que celle du secret professionnel des professions de santé ou des professionnels de la justice : Crim., 6 juill. 1929, *DH* 1929, p. 494 ; Crim., 30 janv. 1975, *JCP G* 1975, p. 18137, note C. GAVALDA; *RSC* 1975, p. 1011, obs. A. VITU.

[1283] CSP (Code de déontologie médicale), art. R. 4127 et art. L. 1110-4.

[1284] Ainsi, il a pu être jugé que « Sont couvertes par le secret professionnel non seulement les confidences faites par le client à son avocat, mais également toutes les informations qu'a pu recueillir ce professionnel à l'occasion de l'exercice de ses fonctions et les déductions personnelles qu'il a pu en faire », (Paris, 1er juill. 1999, *D.* 1999, IR p. 230.)

[1285] V. note n° 1248 ¤.

[1286] M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*, n° 83.

Cette généralisation a été progressive, elle est, dans un premier temps le fait de l'évolution de la pratique médicale **(A)** elle revèle ensuite d'une volonté de créer une « chaîne de secret » afin de favoriser la circulation de l'information et des données **(B)**.

A - Le canon et ses répliques

272. Du « secret médical » et du secret professionnel. Il nous faut revenir sur des propos déjà tenus à titre introductif, mais cette fois pour nous permettre de décrire le mouvement de généralisation du secret professionnel dans le système de santé. Il a été tenu pour acquis, en introduction, que toutes les personnes intervenant dans le système de santé étaient soumises au secret professionnel. Cette affirmation doit à présent être mise en relief sous le seul angle du rapport entre « secret médical » et secret professionnel.

L'histoire du « secret médical » figure en bonne place des introductions aux études relatives au secret professionnel[1287]. Il est présenté comme l'emblème, la figure archétypale servant de socle à toute recherche sur le secret professionnel. D'ailleurs, la place du médecin dans la société depuis l'Antiquité a servi de base à l'élaboration de certaines théories de la sociologie des professions[1288]. Pourtant, l'assimilation qui en a découlé, et qui s'éprouve encore aujourd'hui, engendre quelques confusions et amalgames de nature à altérer la cohérence des discours juridiques sur le secret professionnel[1289]. La distinction entre secret professionnel et

---

[1287] Par exemple : L. HELLENBRAND, *Secret et justice pénale*, th. dact. ss. la dir. de A. VITU, soutenue en 1997, Université Nancy II ; M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel, op. cit. ;* J.-P. DARTIGUELONGUE, *Le secret dans les relations juridiques*, th. Bordeaux, 1968 ; M.-A. FRISON-ROCHE (ss. la dir.), *Secrets professionnels*, *op. cit.* ; F. LOUHIBI-BENATEK, *Le secret professionnel*, th. dact. ss. la dir. de R. BERNARDINI, soutenue en 1997, Université de Nice ; A. DAMIEN, *Le secret nécessaire*, Desclée de Brouwer, 1989.

[1288] Parmi les travaux fondateurs, ceux de Talcott Parsons et notamment quant à la médecine, à propos de laquelle il consacre un chapitre de son ouvrage : T. PARSONS, *The social system*, Glencoe – Free Press, 1951.

[1289] C'est l'un des points de départ de notre étude. Rappelons que de nombreux travaux traitent du « secret médical » comme un principe ou comme le secret professionnel lui-même. V. en ce sens D. TABUTEAU, « Le secret médical et l'évolution du système de santé », *D.* 2009, p. 2629 : l'auteur évoque la « protection du secret médical », la formulation étant utilisée à de nombreuses reprises par d'autres auteurs (L. DUBOUIS, « Secret médical et liberté de la presse », *RDSS* 2004, p. 841 ; J.-D. SARCELET, « La confidentialité des informations de santé peut-elle tenir face à la protection d'autres intérêts légitimes ? – Le rôle du juge dans la confrontation des intérêts légitimes en présence », *D.* 2008, p. 1921 ; S. PORCHY-SIMON, *Jcl Resp. civ. et Assur.,* Art. 1382 à 1386, Fasc. 440-30 : « Santé – Responsabilité médicale – Responsabilité pour faute d'éthique médicale – Consentement libre et éclairé du patient – Secret médical », févr. 2011 (mise à jour août 2019)).

« secret médical » s'effectue à différents niveaux, le premier niveau permettant d'éclairer la question de l'ontologie du secret professionnel, le second étant d'ordre sémantique[1290].

273. La première confusion. Elle tient au fait que le « secret médical » renvoie à un devoir professionnel d'essence éthique consacré ensuite par des normes déontologiques[1291]. C'est que la norme – qu'elle soit éthique, morale ou déontologique – est historiquement la plus ancienne[1292], elle structure la pratique médicale depuis l'antiquité[1293]. Toutefois, il est largement admis que l'infraction n'est pas d'essence morale : en effet « *ce n'est pas le secret en lui-même qu'il faut considérer comme un impératif social, ce sont les valeurs qu'il a pour vocation de protéger*. *Le secret n'est donc pas une éthique, c'est une technique qui a pour fonction de protéger des valeurs* »[1294]. Aussi, l'utilisation du syntagme « secret médical » pour

---

[1290] P. ROUBIER le rappelait en introduction de son ouvrage *Droits subjectifs et situations juridiques* : « *Les plus grosses difficultés tiennent, à notre avis, à l'emploi d'une terminologie trop imprécise. Une science est une langue bien faite, et on doit très humblement reconnaitre que les termes dont les juristes se servent constamment manquent de netteté.* […] *le danger est trop grand, dans notre science, que les conflits d'intérêts ne deviennent insolubles si on les double de querelles de mots* » (P. ROUBIER, *Droits subjectifs et situations juridiques*, Dalloz, réédition de l'ouvrage publié aux éditions Sirey en 1963, 2005, p. II). Sur le « secret médical » en particulier, v. B. PY, « Réquisitoire contre l'expression de secret médical : plaidoyer pour l'expression de secret professionnel », *RDS*, n° 1, 2013, pp. 161-166).

[1291] Madame Thouvenin introduit d'ailleurs son ouvrage sur le secret médical par ces mots : « *Le secret médical est volontiers présenté comme une question de déontologie* […]. *En effet, étymologiquement la déontologie est la science des devoirs ; mais actuellement cette terminologie vise plus particulièrement les devoirs qu'impose à des professionnels l'exercice même de leur métier.* […] *La profession médicale a produit autour du secret un discours aussi abondant que stéréotypé, aux termes duquel le secret serait un des piliers de la médecine occidentale ayant acquis ses lettres de noblesses dès Hippocrate* ». (D. THOUVENIN, *Le secret médical et l'information du malade*, PUL, 1982, p. 9). Toutefois l'auteur emploie bien le même mot pour qualifier la norme juridique et la norme déontologique.

[1292] Notons que parler de morale, d'éthique et de déontologie ensemble ne constituent pas une assimilation rédhibitoire puisque « *la déontologie se place aux confins de la morale* » (R. VILLEY, *Histoire du secret médical*, coll. Médecine et Histoire, Seghers, 1986, p. 122). Le premier ouvrage consacré à la déontologie est, à cet égard, instructif, puisqu'il est intitulé *La déontologie ou science de la morale* (J. BENTHAM, *La déontologie ou la science de la morale*, ouvrage posthume, revu, mis en ordre et publié par J. BOWRING, Charpentier, 1934) et définit celle-ci comme la théorie des devoirs.

[1293] R. VILLEY, *Histoire du secret médical*, *op. cit.*

[1294] V. M. COUTURIER, *Pour une analyse fonctionnelle du secret professionnel*, *op. cit*., n° 332. En ce sens également, v. J. PRADEL « L'incidence du secret médical sur le cours de la justice pénale », *JCP* 1969, I, 2234 : « *le secret médical n'est pas une fin en soi. Au fond, comme tous les autres, le secret professionnel des médecins est un secret fonctionnel* » ; Dans le même sens, v. B. HOERNI, « Principes et pratiques d'un secret : le secret médical », *in* M.-A. FRISON-ROCHE (ss. la dir.), *Secrets professionnels*, *op. cit.*, 1999, p. 177 : « *Le secret médical doit ainsi être reconnu pour ce qu'il est : un moyen de respecter les patients et non une fin en soi* » ; B. BEIGNIER, *L'honneur et le droit*, préf. J. Foyer, coll. Bibliothèque de droit privé, t. 234, LGDJ, 1995, p. 124 : « *De même que la vie privée n'est pas une notion qui se suffit à elle-même, le secret professionnel n'est pas une institution qui se justifie ontologiquement*. […] *Le secret n'existe pas pour le secret. De même que la vie privée*

désigner le secret professionnel[1295] a-t-elle eu pour première conséquence de faire perdurer les interrogations sur la nature du secret professionnel dans la mesure où normes éthique, déontologique et juridique sont fréquemment confondues.

274. La seconde confusion, tient au fait que l'utilisation du vocable « secret médical » est impropre à désigner le secret professionnel dans le domaine de la santé, le problème est sémantique. Parce que la formulation laisse entendre que seuls seraient soumis au secret professionnel les professions médicales qui seraient d'ailleurs titulaires d'un « droit » sur le secret, il s'agirait « *du secret des médecins* »[1296]. Cette utilisation impropre suggère ainsi que seules sont des informations à caractère secret les informations d'ordre médical[1297]. Il en

---

n'est respectable que dans une certaine mesure ainsi le secret professionnel ne joue que pour garantir la protection d'un "intérêt légitime" ».

[1295] Cet usage indifférencié est autant le fait de la jurisprudence que de la doctrine ou du législateur. Il est d'ailleurs impossible et inutile de faire la liste des occurrences du terme « secret médical » dans la jurisprudence, une brève recherche sur la base de données de Légifrance (https://www.legifrance.gouv.fr/) est toutefois édifiante : le terme « secret médical » apparaît dans 2361 décisions (il n'est évidemment pas exclu que certaines fassent référence à la norme déontologique dès lors que le Conseil d'Etat est compétent pour contrôler les décisions prises par les Ordres professionnels. Il n'en demeure pas moins que les décisions judiciaires contenant le terme sont au nombre de 537). Par ailleurs, pour juger de manière plus prégnante de l'usage indifférencié entre secret professionnel et secret médical, l'ajout de l'article 226-13 du Code pénal comme autre terme de recherche occasionne 72 occurrences. La même recherche sur la base de données jurisprudentielle de Dalloz.fr propose un résultat de 172 occurrences. Pour ne citer que deux exemples (les premiers de la liste) : Les motifs d'une décision de Cour d'appel selon laquelle « *Le secret médical édicté par l'article 226-13 du code pénal est absolu* » (Orléans, 6 févr. 2014, n° 13/01878) ou encore un arrêt de la Cour de cassation où l'on peut lire qu' « *il ne résulte pas de l'information des charges suffisantes contre quiconque d'avoir violé le secret médical, au sens des articles 226-13 et 226-14 du code pénal* » (crim., 18 janv. 2011, n° 10-83258). En doctrine est parfois utilisée l'expression « secret médical » pour désigner le secret professionnel médical et même le secret professionnel des professionnels de santé : M. BENEJAT-GUERLIN, « Que reste-t-il de la protection pénale du secret médical ? », *AJ pénal* 2017, p. 368 ; J.-M. PANFILI, « Dossier « Hospitalisation sans consentement » - Publicité des débats et secret médical : deux principes antagonistes à concilier », *AJ famille* 2016, p. 27 ; *D. actu.*, 5 mai 2017, comm. J. SIRO, « Opposabilité du secret médical à l'expert du CHSCT ». Enfin sur le plan législatif, Monsieur Vialla a remarqué que « *La lecture du code de la santé publique, dans sa partie législative, suffit à se convaincre de la valse-hésitation terminologique du législateur. La formule « secret médical » y apparaît à 21 reprises et celle de « secret professionnel » y figure 39 fois. Ajoutons que trois articles évoquent cumulativement le « secret médical ou professionnel » et que deux articles recourent, sans davantage de précisions, au respect des secrets protégés par la loi !* » (F. VIALLA, « Perspectives pour une culture commune du secret et de l'information partagée », *JurisAssociations* 2013, n° 474, p. 30). On peut même noter que cet état de désordre ne s'est pas arrangé avec la loi du 26 janvier 2016. Ainsi pour illustration, peut-on relever le nouvel article L. 1413-12-3 du Code de la santé publique qui contient la formule suivante : « *Les conditions dans lesquelles l'Agence nationale de santé publique, ou, le cas échéant, d'autres membres du réseau national de santé publique accèdent aux informations couvertes par le secret médical, le secret professionnel ou le secret en matière commerciale et industrielle* ».

[1296] Ce que certains auteurs relèvent toutefois, lesquels considèrent que si l'infraction de violation du secret professionnel n'a pas pour finalité de sanctionner le non-respect d'une norme déontologique, cela ne signifie pas que la protection de la profession ne puisse être une fonction implicite : M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*, n° 445 et svt.

[1297] C'est le constat formulé par Monsieur Py, qui souligne d'une part « *l'extension du champ des personnes tenues au secret* » mais également la diversité des informations secrètes qui ne sont pas, loin s'en faut, des informations de nature médicale ou relatives à la santé, ce qui interdirait également de parler de *secret médical* pour viser le

découle également une autre confusion qui consiste à prendre le « secret médical » pour le secret professionnel en général[1298]. Dès lors, il convient de préférer le terme « secret professionnel médical » pour désigner le régime de ce secret particulier mais non général[1299]. Il existe, de surcroît, une diversité de secrets professionnels au sein même du *système de santé* et plus largement une multitude de professionnels amenés à connaître des informations intimes sur les individus.

275. Le secret professionnel médical, modèle du secret professionnel des professionnels de santé. La norme déontologique instaurant le devoir, pour les médecins, de garder le secret, a été par la suite répliquée dans toutes les professions qui se sont dotées d'un code de déontologie[1300]. Pour autant l'existence d'un code de déontologie ne signifie pas que le manquement au devoir déontologique soit pénalement sanctionné, le secret des psychologues et la question de de leur soumission au secret professionnel en est une illustration[1301]. Il demeure

---

secret professionnel (B. PY, « Réquisitoire contre l'expression de secret médical : plaidoyer pour l'expression de secret professionnel », *op. cit.*, pp. 162-163). Monsieur Couturier affirme, sous un angle sensiblement différent, qu'il n'existe plus de « secret médical » puisque de très nombreux professionnels sont aujourd'hui tenus au secret professionnel (M. COUTURIER « Que reste-t-il du secret médical ? », *in Mélanges en l'honneur de Gérard Mémeteau. Droit médical et éthique médicale : regards contemporains,* t. I, LEH Édition*,* 2015, pp. 351-360).

[1298] En ce sens, M. COUTURIER, *Pour une analyse fonctionnelle du secret professionnel*, *op. cit.*, n° 87 : « *D'instinct, il est ressenti par beaucoup comme le secret professionnel par excellence, à ce point que les deux notions se confondent parfois dans l'esprit de ceux qui les évoquent* ».

[1299] Proposition formulée par B. PY « Réquisitoire contre l'expression de secret médical : plaidoyer pour l'expression de secret professionnel », *op. cit.*

[1300] Monsieur Py le rappelle d'ailleurs et en dresse la liste : « *Historiquement, les professions médicales ont été les premières à imposer à leurs membres un strict respect des secrets professionnels. Cette obligation a été progressivement étendue à toutes les professions de santé en l'assortissant de sanctions disciplinaires au moyen de code de déontologie. On peut citer : les médecins (Décr. n° 95-1000 du 6 sept. 1995 portant code de déontologie médicale, art. 4, D. 1995.452, in Code de la santé publique Dalloz), les chirurgiens-dentistes (Décr. n° 94-500 du 15 juin 1994 portant code de déontologie des chirurgiens-dentistes, art. 5, D. 1994.343), les sages-femmes (Décr. n° 91-779 du 8 août 1991 portant code de déontologie des sages-femmes, art. 3, D. 1991.390), les pharmaciens (Décr. n° 95-284, 14 mars 1995 portant code de déontologie des pharmaciens, JO 16 mars)* » (B. PY, *Rép. pén.*, *V°* « Secret professionnel », févr. 2003 (mise à jour févr. 2017)). On peut ajouter à celle-ci le Code de déontologie des masseurs-kinésithérapeutes (Décret n° 2008-1135 du 3 novembre 2008 portant code de déontologie des masseurs-kinésithérapeutes) ainsi que le Code de déontologie des infirmiers (Décret n° 2016-1605 du 25 novembre 2016 portant code de déontologie des infirmiers).

[1301] Si les psychologues se sont imposés un devoir déontologique de silence, aucun texte légal ne prévoit qu'ils soient soumis au secret professionnel bien que certains auteurs l'affirment sans formuler la question (par exemple : G. CEDILLE, « Le signalement par le psychologue est-il compatible avec le respect du secret professionnel ? », *AJ pénal* 2011, p. 579). En l'absence de jurisprudence la question de savoir s'ils sont astreints au secret professionnel se pose avec acuité. Dès lors qu'ils sont agents de la fonction publique hospitalière, ils sont soumis au secret professionnel, en raison de leur statut, par l'article 26 de la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires (TA Besançon, 25 févr. 2010, n° 0900393, *AJFP* 2010, p. 203 « La violation de l'obligation de secret professionnel par un psychologue engage la responsabilité du CHU »). Il s'agit alors d'un secret dit de « système », en témoigne notamment une décision de la Cour administrative d'appel de Nancy

toutefois que c'est sur le modèle du secret professionnel des professions médicales que s'est construit le régime du secret professionnel des autres professions de santé, comme on le constate au travers d'une jurisprudence constante usant de l'expression « secret médical » pour désigner le secret des professionnels de santé en général[1302], le régime de ces secrets étant le même que celui des professions médicales. Cette unité de régime se conçoit dès lors que l'exercice de la médecine n'est plus un exercice individuel[1303]. L'affirmation d'un droit à la protection de la santé[1304] a eu pour corollaire le développement progressif d'un *droit de la santé publique*, dont les dernières évolutions se sont traduites dans l'affirmation de l'existence d'un système de santé[1305]. L'affirmation de l'existence d'un *système* explique notamment la généralisation du secret professionnel induite par la rédaction de l'article L. 1110-4 du Code de la santé publique. Dès lors que le système, selon les mots de Monsieur Truchet, désignerait « *un ensemble auquel s'appliquerait un certain nombre de règles communes, dont il fixe le champ*

---

considérant qu'une communication faite par une psychologue scolaire à une inspectrice de l'éducation nationale ne violait pas le secret professionnel : « *La communication faite à l'inspectrice en sa qualité de présidente d'une commission, elle-même tenue au secret, n'est pas considérée comme une violation du secret professionnel* » (CAA Nancy, 12 mai 1999, n° 95NC01386, *AJFP* 1999, p. 23). Par ailleurs il est possible de considérer qu'ils entrent dans la catégorie des professionnels astreints au secret lorsqu'ils interviennent dans un établissement de santé, même lorsqu'ils sont professionnels libéraux, puisque l'article L. 1110-4 du Code de la santé publique le prévoit. Ce ne serait toutefois pas le cas lorsqu'il s'agit de professionnels ayant une activité libérale. Ces derniers n'auraient qu'une obligation déontologique de secret mais qui ne peut être sanctionnée puisqu'il n'existe pas de pouvoir ordinal.

[1302] Ainsi, bien que les décisions de justice sur la question soient faibles et relèvent principalement de questions d'opposabilité du secret professionnel ou de licenciement pour violation du secret professionnel, il est constant que les juges utilisent la formulation « secret médical » pour désigner le secret des autres professionnels de santé et le considèrent également comme « absolu ». Il s'agit sans doute ici d'affirmer l'identité de régime entre le secret professionnel des médecins et celui des autres professionnels de santé. Concernant par exemple les masseurs-kinésithérapeutes : Amiens, ch. soc., 9 mars 2011, n° 10/03137 ; Orléans, ch. soc., ch. des Prud'hommes, 6 févr. 2014, n° 13/01878 ; Crim., 24 sept. 1998, n° 97-81748. Concernant encore les infirmiers : CE, 8ème et 9ème SSR, 1er juin 1994, n° 150870.

[1303] V. J.-F. MATTEI, J.-C. ETIENNE, J.-M. CHABOT, *De la médecine à la santé, pour une réforme des études médicales et la création d'universités de la santé*, Flammarion, 1997 ; M. GRASSER, C. MANAOUIL, A. VERRIER, O. JARDE, « L'équipe médicale à l'hôpital », *RGDM* 2004, n° 14, p. 13. Colloque, l'Assemblée nationale, 11 oct. 2003, *L'équipe médicale, approche pluridisciplinaire*.

[1304] « *Le préambule de la Constitution de 1946 dispose que « la Nation assure à l'individu et à la famille les conditions nécessaires à leur développement. Elle garantit à tous, notamment à l'enfant, à la mère et aux vieux travailleurs, la protection de la santé ». De même, le Conseil constitutionnel a, en plusieurs occasions, consacré la valeur constitutionnelle de ce principe. Enfin, la loi du 4 mars 2002 lui a apporté une confirmation légale*[1304]*. Bien évidemment, l'apparition du secret médical a précédé celle de l'affirmation de ce droit à la santé. Toutefois, on peut estimer que l'avènement de ce dernier n'a fait que renforcer le rôle éminent du médecin et des professions paramédicales dans l'organisation sociale, rôle qui a préexisté à l'affirmation formelle de ce droit*. » (M. COUTURIER, *Pour analyse fonctionnelle du secret professionnel*, *op. cit.*, n° 76).

[1305] Sur cet évolution v. D. TRUCHET, *Droit de la santé publique*, 9ème éd., coll. Mémentos, Dalloz, 2016, spéc. Introduction générale.

d'application »[1306], il apparaît que toutes les personnes qui interviennent dans ce *système* devraient être astreintes au secret professionnel[1307]. L'évolution de la médecine vers une pratique en équipe pluridisciplinaire explique également l'identité entre le secret professionnel médical et le secret professionnel des professionnels de santé[1308]. De plus, la santé ne résulte plus seulement des professionnels de santé, que ce soit en ville ou à l'hôpital, le nombre d'intervenants dans le « parcours de soin » – devenu « parcours de santé »[1309] – est de plus en plus important. De multiples facteurs ont resserré la chaîne de la prise en charge des personnes, celle-ci étant désormais médico-sociale. Cette évolution inviterait à ne plus envisager le secret professionnel médical au travers d'une étude particulière. Mais de considérer que la division entre le secret des médecins et celui des autres professionnels intervenant dans le champ de plus en plus large de la santé est de moins en moins opérante. Il s'agit par ailleurs de constater que cet assujetissement généralisé est guidé par une nécessité de faire circuler l'information, puis les données dans le but de faire *fonctionner le système*.

B - Le secret professionnel dans le système de santé

276. L'extension du champ d'application de l'infraction sanctionnant la révélation d'une information à caractère secret tient en premier lieu à l'évolution de ce que l'on présente comme le « système de santé » **(1)**. Nous avons, jusqu'ici, utilisé l'expression sans égard à sa signification. Ces développements seront l'occasion de constater les difficultés éprouvées par la doctrine pour en saisir les contours. Ces obstacles empêchent de conceptualiser le « système de santé » et en même temps de déterminer les personnes qui sont astreintes au secret professionnel **(2)**.

[1306] *Ibid.* p. 21.
[1307] Il reste une difficulté de taille : traçer les contours de ce système et la choses s'avère bien plus complexe qu'il n'y paraît v. *infra* n° 278 et svt.
[1308] D. HOUSSIN, « Le secret médical dans les nouvelles pratiques et les nouveaux champs de la médecine », *D.* 2009, p. 2619.
[1309] Le changement de vocable marque la volonté d'adopter une définition de la santé proche de celle de l'OMS (« *La santé est un état de complet bien-être physique, méntal et social et ne consiste pas seulement en une absence de maladie ou d'infirmité* »), ce qui fait remarquer à Monsieur Truchet que la définition à le mérite de souligner que le *droit de la santé publique* concerne donc également un volet prévention (D. TRUCHET, *Droit de la santé publique*, *op. cit.*, p. 23).

1 - Les prémisses d'un assujetissement généralisé au secret professionnel

277. Secret professionnel et travail social. L'étude des personnes soumises au secret dans le domaine de la santé ne peut plus se faire au travers des seules professions de santé, elle nécessite d'aborder le secret professionnel en matière sociale. Il ne s'agit pas, ici encore, de s'astreindre à proposer une liste des personnes soumises au secret mais de synthétiser l'essentiel des évolutions en la matière pour souligner le rapprochement entre le secteur de la santé et le secteur médico-social.

En matière de travail social, la question du secret professionnel a fait l'obet de travaux de recherche récents[1310]. L'auteur y souligne la difficulté de proposer une étude uniforme du secret professionnel des travailleurs sociaux et constate que seuls les assistants de services sociaux sont soumis au secret professionnel « par profession » tandis que de nombreux autres ne le sont qu'en raison d'une fonction ou d'une mission temporaire[1311]. Outre l'origine disparate de ces activités, il apparaît que le secret professionnel des travailleurs sociaux est un « *secret hybride* » quant à son régime : il serait à la fois un secret de système et un secret « véritable ». Ce constat tient surtout à l'opposabilité relative du secret des travailleurs sociaux, c'est-à-dire l'impossibilité, pour certains, d'invoquer la dispense de témoigner prévue à l'article 109 du Code pénal mais également d'opposer le secret à leur hiérarchie[1312]. Cette particularité est typique de la différence entre les professions libérales et les activités dont l'assujettissement au secret aurait une « *légitimité verticale* »[1313]. Ces quelques remarques relatives au secret des travailleurs sociaux doivent être appréciées à la lumière du rapprochement, voire de l'unification des secteurs sanitaire et médico-social dont le « secret partagé »[1314] est la traduction juridique.

278. Rapprochement entre le secteur sanitaire et le secteur médico-social. Le terme « rapprochement » est quelque peu restrictif, puisque l'histoire des « *droits sanitaire et*

[1310] Notamment par Madame Rahali dans sa thèse de doctorat (C. RAHALI, *Le secret professionnel et l'action médico-sociale*, th. dact. ss. la dir. de B. PY, soutenue le 20 déc. 2014, Université de Lorraine).
[1311] C. RAHALI fait d'ailleurs des propositions dans le sens d'une uniformisation (*Ibid.* n° 99 et svt).
[1312] *Ibidem.* n°81.
[1313] M. COUTURIER, *Pour analyse fonctionnelle du secret professionnel, op. cit.*, n° 101.
[1314] V. *supra* n° 236 et svt.

médico-social »[1315] s'analyse plutôt comme une succession de périodes de rapprochement et de séparation[1316]. S'il a été question des professions du social, il faut noter que les agents des caisses de sécurité sociale sont églament soumis au secret professionnel en vertu de textes renvoyant à l'article 226-13 du Code pénal ou de la jurisprudence[1317]. Il s'agirait, selon un auteur, « *d'un secret de système, car les textes instituent fréquemment des exceptions à ce devoir en instituant des obligations de communication au profit de diverses administrations* »[1318]. Aussi le secret professionnel des agents des caisses de sécurité sociale et de l'action sociale n'a-t-il pas la même portée. La sécurité sociale, en tant qu'outil de mise en œuvre de l'Etat providence, relève bien du champ sanitaire, pour cette raison, la séparation du sanitaire et du social[1319] s'est d'abord traduite par une prise en charge des soins médicaux par la sécurité sociale tandis que les soins de longs séjours – maladies chroniques, personnes âgées –, considérés comme relevant du secteur social, devaient être supportés par l'aide sociale départementale et la famille des malades. Les difficultés pour les particuliers à supporter le coût de ces hébergements a convaincu le législateur de « *sanitariser* »[1320] le secteur social. Cette volonté s'est traduite par la mise en place d'organismes d'aide au maintien à domicile, la prise en charge des personnes étant assurée sur le plan médical par des professionnels libéraux ou des salariés. Par la suite, la réunification des champs sanitaire et médico-social s'est accélérée au travers de la création des réseaux de soins dans lesquels interviennent les établissements publics et privés, les professions libérales, les services sociaux des collectivités. La logique intégrative s'est poursuivie, portée par la loi du 26 janvier 2016 relative à la modernisation de

---

[1315] D. TRUCHET, « La genèse de la construction des droits sanitaire et médico-social », *RDSS* 2014, p. 495.
[1316] *Ibid.*, v. aussi J.-M. CLEMENT, *Question de politiques hospitalières – Organisation médicale, technocratie – Droits des malades*, LEH Edition, 2015, pp. 151-161.
[1317] CSS, art., L. 161-29, s'agissant des personnels des organismes d'assurance-maladie ; CSS, art. L. 931-40 pour les membres du conseil d'administration du fonds paritaire de garantie ; S'agissant des services de prestations de vieillesse assurés par des organisations autonomes : CSS, art. L. 621-2 ; concernant les dirigeants et salariés du fonds de solidarité vieillesse : CSS, art. L. 135-13 ; CSS, art. L. 243-9 et Crim., 21 janv. 1959, *Bull. crim.,* n° 59 pour le cas particulier des praticiens conseils des organismes de sécurité sociale, tenus au secret en raison de leur profession de médecin et en vertu du Décret n° 69-505 du 24 mai 1969 fixant le statut des praticiens conseils chargés du service du contrôle médical du régime de la sécurité sociale. Enfin, s'agissant des administrateurs des caisses de sécurité sociale : Crim., 30 juin 1955, *Bull. crim.*, n° 334 ; *JCP* 1955, II, 8860 bis ; *D.* 1955, p.718 ; *Dr. soc.* 1955, p. 594 ; *Gaz. Pal.* 1955, 2, J. 137 ; Crim., 5 déc. 1957, *D.* 1958, p. 98.
[1318] M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*, n° 115.
[1319] Par la Loi n° 75-535 du 30 juin 1975 relative aux institutions sociales et médico-sociales.
[1320] C'est le terme utilisé par un auteur : C. RAHALI, *Le secret partagé dans le secteur médico-social, op. cit.*, n° 21.

notre système de santé[1321], dans laquelle le vocable « parcours de soin » a laissé place au « parcours de santé ». Depuis cette dernière loi, le discours politique a forgé une expression signifiant encore davantage cette dilution : l'on parle désormais du « *Système de santé, médico-social et social* »[1322]. Cette formulation va dans le sens d'une vision élargie de la santé mais témoigne également de la volonté de confirmer une gouvernance publique accrue indifférente au mode d'exercice des professionnels de santé.

279. Le lien avec la doctrine de la CNIL et le traitement des données issues de la relation de soin. Nos précedents développements relatifs à la doctrine de la CNIL, à propos de la détermination des personnes autorisées à accéder ou à se voir transmettre des données, trouvent ici un écho particulier. La volonté politique de rapprocher, puis d'unifier, les champs de la médecine et du social pour former un *système* s'est d'abord traduite par une mise en œuvre au niveau des acteurs. Les réseaux de soin puis de santé en sont une illustration, mais c'est avec la maîtrise médicalisée des dépenses de santé, dès 1994, que l'expression s'est propagée dans le discours politique et dans celui des commentateurs des lois et conventions qui l'instaurent[1323]. La « *coordination des différents intervenants du système de santé* »[1324] qui était l'un des principaux objectifs de la maîtrise des dépenses de santé a d'abord concerné les acteurs. Elle devait nécessairement s'accompagner d'une circulation des informations entre ces acteurs. La CNIL s'est trouvée ainsi à l'avant-poste des problèmes que pouvait poser la circulation des données[1325]. La question de la détermination des personnes soumises au secret professionnel –

[1321] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé (*JORF* n°0022, 27 janv. 2016).
[1322] L'on peut notamment lire, sur le site du ministère de la santé que ce système a pour objectif « *une prise en charge globale de la personne* » (<https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/systeme-de-sante-et-medico-social/article/systeme-de-sante-medico-social-et-social> (dernière consultation le 15 sept. 2019)).
[1323] V. notamment : A.-M. BROCAS, « La convention médicale de 1993 », *Droit social* 1994, p. 422 ; L. DUBOUIS, « La sixième convention nationale médicale : la mise en chantier de la maîtrise médicalisée des dépenses médicales », *RDSS* 1994, p. 40.
[1324] *Ibid.*
[1325] Sur le plan de l'organisation étatique, Monsieur Chevallier constate, à propos des autorités administratives, un « *processus d'intégration au milieu* » régulé (J. CHEVALLIER, « L'Etat régulateur », *RFAP* 2004/3, n° 111, pp. 481), ainsi « *chacune de ces administrations est amenée plus ou moins à intérioriser la rationnalité du secteur qu'elle est chargée d'encadrer ou de réguler* » (*Ibid.*). Cette intégration au secteur a pour conséquence, selon Madame Decoopman, de conférer au régulateur une emprise plus forte (N. DECOOPMAN, « A propos des autorités administratives indépendantes et de la déréglementation », *in* J. CLAM et G. MARTIN (ss. la dir.), *Les transformations de la régulation juridique*, coll. Droit et Société, Recherches et Travaux du RED&S à la Maison des Sciences de l'Homme, n° 5, LGDJ, 1998, p. 252) sur celui-ci. L'auteur explique que les autorités de régulation sont « *saisies en permanance* » (*Ibid.,* p. 252) tandis que la règlementation classique ne relève pas d'un contrôle mais de la sanction du non-respect d'une norme. De notre point de vue, tandis que le juge n'interviendra qu'en cas de violation du secret professionnel, ou en raison d'une atteinte au secret des informations par un tiers, la mission

et remplissant ainsi le critère de confiance de la confidentialité qui permet de les considérer comme qualifiées pour recevoir les données – s'est ainsi posée à la CNIL. En l'absence, avant 2002, d'une législation définissant clairement les personnes soumises au secret professionnel dans ce *système de santé* en construction, elle s'est appuyée sur ses propres critères pour parvenir à concilier les objectifs des politiques de santé publique, dont le traitement des données est un outil, et la confidentialité des données. Dès lors, on peut émettre l'idée selon laquelle la CNIL a été annonciatrice de l'assujettissement au secret professionnel de tous les intervenants du système de santé, voire l'un de ses instigateurs.

L'article L. 1110-4 du Code de la santé publique, issu de la loi du 4 mars 2002 relative aux droits des patients a finalement entériné la généralisation du secret professionnel. Sa portée est toutefois incertaine.

2 - Une consécration incertaine

280. La portée incertaine de l'article L. 1110-4 du Code de la santé publique. Selon la doctrine majoritaire, l'article L. 1110-4 du Code de la santé publique astreindrait au secret professionnel tous les professionnels intervenant dans le système de santé. Cet article fixerait également le régime du secret professionnel pour l'ensemble des professionnels qui y interviennent. Il semble toutefois que cette affirmation puisse être relativisée. D'une part, en raison de la portée normative de l'article au regard du droit pénal ; d'autre part, en raison de son imprécision.

---

de l'autorité de régulation « *suppose la permanence* » (*Ibid.,* p. 253). Comme le souligne encore cet auteur, le renforcemement de l'emprise des autorités de régulation consiste dans le fait qu'elles effectuent une « *boucle de contrôle* » (*Ibid.*) en ce qu'elles interviennent « *en amont et en aval, de façon préventive mais aussi coercitive* » (*Ibid.*). Le même constat est fait par le Conseil d'Etat dans son rapport relatif aux autorités administratives indépendantes, selon lequel la finalité de la régulation « *serait moins de qualifier des faits par rapport à des normes préétablies et d'aboutir au respect de celles-ci par la sanction, que de chercher par tous moyens à susciter des standards de comportement dictés par l'observation attentive de la réalité et une capacité de réaction rapide et proportionnée aux déviances constatées* […]. […] *la régulation qu'elle assure en continu l'interactivité entre le droit et le fait. Ce qui veut dire qu'il appartient à l'autorité de régulation de faire évoluer en permanence la règle qu'elle applique pour mieux suivre l'évolution de comportements sur le terrain ou l'inventivité des opérateurs, et qu'elle doit parallèlement mettre fin en permanence aux comportements déviants ou susceptibles d'affecter les équilibres du système et plus encore, si possible, les prévenir.* » (Conseil d'Etat, *Rapport Public 2001, Les autorités administratives indépendantes*, La documentation française, n° 52).

281. L'absence de renvoi vers l'article 226-13 du Code pénal. L'examen comparé des catégories de personnes soumises au secret professionnel est vain si l'on admet que l'article L. 1110-4 du Code de la santé publique a vocation à organiser le régime du secret professionnel des personnes intervenant dans le système de santé et qu'il prévoit que le régime de ce secret est identique, pour toutes ces professions, à celui du secret professionnel médical. Dans cette hypothèse, « *tous les professionnels intervenant dans le système de santé* » seraient astreints au même secret que les professions médicales. Or, il est permis de douter de cette apparente simplicité. Pour plusieurs raisons : d'abord, s'il est admis que la loi ou le règlement peut désigner les professionnels soumis au secret, encore faut-il que le renvoi à l'article 226-13 du Code pénal soit explicite ; il s'agit là d'une question de lisibilité de la loi[1326] et celle-ci se justifie d'autant plus que les confusions entre le secret professionnel et des notions sémantiquement proches sont légion. L'article L. 1110-4 du Code de la santé publique, modifié par loi du 26 janvier 2016[1327], n'a jamais opéré de renvoi à l'article 226-13 du Code pénal, même dans ses versions antérieures. Si le bon sens voudrait que l'on ignore cet « oubli » répétitif du législateur, le doute est au moins permis quant au fait de savoir si le régime du secret professionnel est identique pour tous les intervenants et, surtout, s'il est identique au régime du secret professionnel des professionnels de santé dont nous avons rappelé la filiation. Ensuite, il faut remarquer que le premier alinéa de l'article dispose du « *respect de sa vie privée et du secret des informations la concernant* », le second précisant que « *ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes* ». Cet enchaînement maladroit suggère que le secret concerne la vie privée, mais rien ne permet de confirmer qu'en cas de révélation, tous ces acteurs sont susceptibles de poursuites pénales sur le fondement de l'article 226-13 du Code pénal.

282. L'article L. 1110-4 du Code de la santé publique, un texte de désignation ? Ainsi qu'il a pu être souligné, la principale difficulté quant à la détermination des personnes tenues

---

[1326] Comme le souligne Monsieur Molfessis, selon sa qualité, le renvoi peut être « *une aide ou bien une entrave à la compréhension du texte* » (N. MOLFESSIS, « Le renvoi d'un texte à l'autre », *in* N. MOLFESSIS (ss. la dir.), *Les mots de la loi*, *op. cit.*, n° 21-22).
[1327] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé (*JORF* n°0022, 27 janv. 2016). Il a ensuite été modifié par ordonnance mais sans conséquence quant au point qui nous occupe.

au secret professionnel tient au caractère général de la formulation de l'article 226-13 du Code pénal. Tandis que l'ancien article 378 visait expressément certaines professions médicales, l'article rédigé lors de la réforme du Code pénal ne donne qu'une définition générale de cette condition. La particularité de ce texte est sa « *texture ouverte* »[1328] s'agissant de la qualité de la personne dont la révélation est sanctionnée. A ce sujet, certains auteurs affirment qu'il s'agit d'un texte de renvoi *implicite*[1329]. L'augmentation considérable du nombre de personnes soumises au secret professionnel serait alors une des conséquences de la technique de l'incrimination par renvoi[1330], ce qui a, par ailleurs, posé les difficultés que l'on connaît. Il semble désormais que l'article L. 1110-4 du Code de la santé publique ait mis fin au doute en ce qu'il astreint au secret professionnel toutes les personnes intervenant dans le système de santé. Toutefois, cette disposition n'est pas un exemple de clarté, qualité dont la matière pénale ne peut faire l'économie. L'emploi de la formule « *toute autre personne en relation, de par ses activités, avec ces établissements ou organismes* » présente un écueil majeur[1331] tenant à l'utilisation du verbe « *intervenir* » et aux frontières mouvantes du « *système de santé* ».

283. Le lien avec la doctrine de la CNIL. L'incertitude qui entoure cette formulation a, à notre sens, permis à la CNIL d'autoriser certains traitements, notamment dans le cadre des réseaux de santé, en admettant que des personnes, dont on pourrait pourtant douter qu'elles *interviennent dans le système de santé*, soient considérées comme des personnes qualifiées pour accéder ou se faire communiquer les données couvertes par le secret professionnel des professionnels de santé. La formulation particulièrement large du Code de la santé publique permet une interprétation casuistique, tant des acteurs de terrain que du régulateur, guidée par la nécessité du traitement pour la prise en charge des personnes. Cette donnée nous laisse par

---

[1328] Pour reprendre l'expression utilisée par Herbert HART à propos du droit en général : H.L.A. HART, *Le concept de droit*, 2e éd., trad. M. Van de Kerchove, PUSL, 2005, p. 143 et svt.

[1329] En ce sens : V. PELTIER, *Jcl. Pénal Code,* Art. 226-13 et 226-14, Fasc. 20 : « Révélation d'une information à caractère secret – Conditions d'existence de l'infraction – Pénalités », mai 2015 (mise à jour sept. 2016), n° 3 *;* M. BENEJAT, *La responsabilité pénale professionnelle*, *op. cit.*, n° 28.

[1330] Monsieur Conte remarque que « *la matière bénéficie d'une réputation de redoutable difficulté, qui n'est pas imméritée : la multiplication (souvent injustifiée) des professions soumises à l'obligation de se taire a introduit la nécessité de distinguer plusieurs types de secrets professionnels, plus ou moins stricts, qui interdisent de donner des solutions univoques et contraignent à des contorsions auxquelles rechigne la rigueur de raisonnement du droit pénal* » (P. CONTE, *Droit pénal spécial*, 5ème éd., LexisNexis, 2016, n° 340).

[1331] Monsieur Conte remarque, à ce sujet, que la formule *toute personne en relation, par ses activités* « *ne veut rien dire* » et adresse la même critique à la formule « *intervenant dans le système de santé* » (P. CONTE, *Droit pénal spécial*, *op. cit.*, n° 346).

ailleurs pressentir que le critère menant désormais à la soumission au secret professionnel dans le domaine de la santé tient à l'origine et à la nature des données.

284. Incertitude quant à l'unité de régime. Un arrêt de la chambre sociale de la Cour de cassation du 20 avril 2017[1332] semble confirmer une vision restrictive de la portée de l'article L. 1110-4 du Code de la santé publique. En l'espèce, le CHSCT d'un centre hospitalier a procédé à une expertise sur le fondement de l'article L. 4614-12 du Code de la santé publique. Lors de cette expertise, le directeur du centre hospitalier a refusé à l'expert l'accès aux blocs opératoires durant les périodes d'intervention ainsi qu'aux réunions quotidiennes des équipes de santé. Le directeur invoque, à l'appui de ce refus, le secret professionnel médical. La cour d'appel ayant considéré que l'expert de la CHSCT n'était pas soumis au « secret médical », l'expert et le CHSCT ont formé un pourvoi en cassation. Le pourvoi est rejeté par la Cour de cassation, qui approuve la cour d'appel d'avoir jugé que l'expert du CHSCT n'était pas soumis au « secret médical » dès lors qu'il « *n'est pas en relation avec l'établissement ni n'intervient dans le système de santé pour les besoins de la prise en charge des personnes* ». Il semble évident que l'expert du CHSCT qui révèlerait une information relative à un patient identifié et apprise lors de l'expertise pourrait être condamné sur le fondement de l'article 226-13 du Code pénal, dès lors qu'il est soumis au secret en application de l'article L. 4614-13 du Code du travail. Il peut, par contre, être déduit de la solution de cet arrêt que l'article L. 1110-4 du Code de la santé publique ne concerne que les personnes *participant à la prise en charge des personnes*. Le régime de ces secrets n'est pas identique, ce qui implique que ces catégories de personnes ne peuvent échanger des informations couvertes par leur secret respectif[1333].

La faiblesse des décisions prises sur le fondement de l'article L. 1110-4 et relatives aux personnes assujetties au secret ne permet pas de systématiser le raisonnement. Une décision plus ancienne peut toutefois appuyer notre analyse, celle-ci semblant faire une interprétation encore plus restrictive de la portée du texte. L'arrêt en question[1334] portait sur un pourvoi formé contre la décision d'une chambre d'instruction de classer sans suite une plainte pour violation du « *secret médical* » à l'encontre de deux informaticiens ayant eu accès à des dossiers patients

---

[1332] Soc., 20 avr. 2017, n° 15-27927 et n° 15-27955, publié au Bulletin ; *D.* 2017, IR, p. 920 ; *D. actu.*, 5 mai 2017, comm. J. SIRO ; *Les cahiers sociaux*, n° 297, p 302, note F. CANUT ; *LPA* 5 sept. 2017, n° 177-178, p. 16, note P. VERON.

[1333] Il s'agissait d'ailleurs de la problématique posée à la Cour. Elle y répond en distinguant les deux secrets professionnels.

[1334] Crim., 3 juin 2008, n° 08-80467.

du fait de leur mission au sein d'une association interprofessionnelle de médecine du travail (AIMT). Le troisième moyen du pourvoi arguait d'une violation de l'article 226-13 du Code pénal et de l'article L. 1110-4 du Code de la santé publique en ce qu'« *il résulte de l'article L. 1110-4 du code de la santé publique que le secret médical «s'impose à tout professionnel de santé, ainsi qu'à tous les professionnels intervenant dans le système de santé » ; qu'en vertu de ce texte, le secret médical ne se limite pas aux seuls médecins mais s'impose également non seulement à toutes les professions de santé mais encore à leur entourage professionnel ; qu'en l'espèce, Jean-Paul X... et Jacques Y..., en étant tous deux employés par une association interprofessionnelle de médecine du travail comme adjoint de direction et consultant informatique, devaient bien être considérés comme des professionnels intervenant dans le système de santé* »[1335]. L'argument ne convainc pas la Cour de cassation qui approuve l'interprétation de la chambre d'instruction selon laquelle les individus visés par la plainte « *n'étant pas médecins, il ne peut leur être reproché la violation d'un secret dont ils n'étaient pas dépositaires* »[1336]. Il n'est pourtant pas exclu qu'une violation du secret professionnel puisse être reprochée aux informaticiens, mais la précision des juges conduit à penser que le régime de ce secret n'est pas le même que celui des professionnels de santé.

285. Deux interprétations possibles en fonction des situations ? Deux interprétations peuvent se déduire de ces développements : l'article L. 1110-4 du Code de la santé publique fixe le régime du secret professionnel des professionnels qui sont en « *contact avec le patient* », ceux que l'article vise comme étant les professionnels intervenant dans le système de santé. En d'autres termes, il s'agirait des professionnels qui participent à sa prise en charge. L'on pourrait également considérer que sont soumis au secret professionnel toutes les personnes qui, par leurs activités, ont à connaître des informations relatives à la prise en charge des personnes dans le système sanitaire, médico-social et social, le régime de leur secret pouvant toutefois différer. Ces deux solutions peuvent être admises. La première pourrait être admise afin de constituer un frein à l'échange ou au partage d'informations lorsque cela a vocation, comme c'était le cas pour l'expertise du CHSCT, à faire prévaloir l'intérêt des professionnels de santé sur celui des patients. Mais la seconde interprétation permet, quant à elle, de favoriser la circulation des informations et des données lorsqu'elle s'avère nécessaire pour les besoins de la prise en charge,

---

[1335] *Ibid.*
[1336] Crim., 3 juin 2008, n° 08-80467.

ce qui explique notamment la doctrine que semble adopter la CNIL en la matière. Il nous semble toutefois qu'il faille, même dans cette dernière hypothèse considérer qu'il existe bel et bien *des* secrets professionnels au sein du *système de santé*.

286. La persistance des renvois à l'article 226-13 du Code pénal dans le Code de la santé publique. Un dernier argument confirme les doutes quant à la portée de L. 1110-4 du Code de la santé publique. Malgré l'existence d'un texte « général » dépassant la dichotomie entre le secteur public et le secteur privé et entre le secteur sanitaire et le secteur social et médico-social, de nouveaux renvois à l'article 226-13 du Code pénal au sein du Code de la santé publique apparaissent de manière régulière. Ce recours aux renvois confirme l'absence d'uniformisation du régime du secret professionnel sur le modèle du secret professionnel médical et la persistance d'une diversité de secrets professionnels.

Section 2 - Vers un critère unique ?

287. La diversité des secrets professionnels s'observe particulièrement lorsqu'il s'agit d'autoriser l'accès aux données et leur réutilisation. Ces secrets ne semblent pas répondre au même régime que celui du secret professionnel des personnes qui sont en contact avec les malades. Afin de favoriser l'utilisation des dispositifs techniques de l'information et de la communication au sein des établissements de santé et de permettre aux traitements des données de remplir les finalités qui leur sont assignées, le législateur a assujetti au secret professionnel de nombreux acteurs techniques (**paragraphe 1**). La loi informatique et liberté contient également un texte de désignation visant les personnes réutilisant les données issues de la prise en charge des personnes dans le système de santé **(paragraphe 2)**. L'on remarque, en dernier lieu, que certains instruments de la CNIL comportent des renvois à l'article 226-13 du Code pénal ce qui interroge les sources du secret professionnel **(paragraphe 3)**. De cet ensemble nous pensons pouvoir dégager un critère qui n'est pas de ceux traditionnellement admis par la doctrine.

§ 1 - L'assujettissement au secret professionnel des acteurs techniques

288. Le traitement des données issues de la prise en charge des personnes dans le système de santé, médico-social et social implique que de nouveaux intervenants puissent être amenés à accéder à ces données tandis qu'elles sont originellement confiées à ces personnes – en tant

qu'elles prennent directement part à la prise en charge –, voire produites par eux[1337]. S'assurer de l'efficacité de l'outil n'est possible que par le recours à des professionnels spécialisés, les professionnels participant à la prise en charge médicale et médico-sociale de la personne ne sont pas en mesure de gérer eux-mêmes les logiciels et les systèmes d'informations informatisés, c'est-à-dire d'en assurer le fonctionnement et la sécurité bien qu'ils puissent être responsables des traitements. Ainsi, certains professionnels qui n'interviennent pas dans la prise en charge du patient mais permettent le traitement des données ont été soumis au secret professionnel par des textes spécifiques. Ces textes, procédant par renvoi à l'article 226-13 du Code pénal, méritent une analyse détaillée. Nous en distinguerons deux catégories : les acteurs de l'information médicale, de l'informatique et des *data* **(A)** et les acteurs du stockage des données **(B)**. Cet examen est guidé par une interrogation centrale : quel est le critère qui justifie leur assujettissement au secret professionnel ?

A - Les acteurs de l'information médicale et de l'informatique

289. La place des acteurs techniques dans le traitement des données à caractère personnel dans le domaine de la santé. L'informatisation des cabinets médicaux privés s'est développée à partir de la mise en œuvre, au niveau national, de la télétransmission des feuilles de soin et l'emploi des cartes SESAM-VITALE et Professionnel de santé (CPS)[1338]. En milieu hospitalier comme en établissement privé, l'implantation et l'utilisation massive des dispositifs techniques de l'information et de la communication a consisté dans la mise en place d'un

---

[1337] Selon un auteur : « *En tant que décodeur de la maladie, le médecin est à l'origine de l'information. Aussi, aux confidences faites par le patient au médecin comme à tout professionnel, s'ajoutent toutes les informations produites par le médecin sur le malade. Et c'est cette aptitude du médecin à créer des informations qui a fait la spécificité du secret médical, car elle lui en assure la maîtrise puisqu'il en est à l'origine* » (D. THOUVENIN, « Secret médical et loi du 4 mars 2002 : Quels changements ? », *LAENNEC* 2007/1 n° 55, p. 23 ; L'idée a été largement développée par le même auteur dans sa thèse de doctorat (D. THOUVENIN, *Le secret médical et l'information du malade*, PUL, 1982). L'information produite n'est plus seulement liée à la maladie, nous l'avons souligné : ce sont des données à caractère personnel, en général sensibles, qui sont produites par un ensemble d'acteurs dans le système de santé.

[1338] Pour un historique de la mise en œuvre de ces outils v. A. LOTH, « Systèmes d'information et cartes de santé », *Dr. Soc.*, 1996, p. 829 ; M. HARICHAUX, « La télétransmission des feuilles de soins », *RDSS*, 1998, p. 496 ; P. PEDROT, « Carte d'assurance maladie. Carte électronique individuelle interrégime », *RDSS* 1998, p. 911.

programme de médicalisation des systèmes d'informations (PMSI)[1339] ayant pour finalité l'analyse et l'évaluation des soins[1340]. Les politiques de santé se sont saisies des outils informatiques pour mettre en œuvre efficacement leurs politiques. La CNIL a très tôt souligné le problème posé par les acteurs techniques. Ils devaient avoir accès aux données – nécessité – mais n'étaient pas soumis au secret professionnel – confiance –, ils ne pouvaient donc pas, en principe, être considérés comme des personnes autorisées à traiter les données au sens de la loi informatique et libertés. Si elle a, à plusieurs reprises, souligné ce problème, nous avons pu remarquer que la CNIL s'était employée à inciter les acteurs à user de la voie contractuelle pour garantir le silence de ces acteurs du traitement des données. Le législateur va progressivement prendre acte de ce problème et astreindre au secret professionnnel tous les acteurs techniques intervenant dans le traitement des données issues de la prise en charge des personnes dans le *système de santé*.

290. Assujettissement au secret professionnel des acteurs de l'analyse de l'activité médicale. Dès 1985, la CNIL a souligné l'importance de mettre en place des dispositifs spécifiques permettant de garantir le « *secret médical* »[1341] dans le cadre de l'analyse de l'activité médicale. Les personnes intervenant dans le traitement des données issues de la relation de soin à des fins d'analyse de l'activité médicale ont été soumises au secret professionnel par décret en 1994[1342]. Des départements d'information médicale (DIM) sont créés au sein des établissements publics et privés. Le responsable des départements d'information médicale dans chaque établissement est un médecin[1343], soumis au secret par sa profession, il est assisté dans sa tâche par d'autres personnes. Ces dernières ne sont ni médecins, ni professionnels de santé mais techniciens de l'information médicale, statisticiens, analystes de données, informaticiens. C'est d'abord l'article R. 710-5-5 du Code de la santé publique,

---

[1339] C'est à l'occasion de la mise en œuvre du programme de médicalisation des systèmes d'information que le premier grand chantier d'informatisation des établissements de santé voit le jour, il participe également de la maîtrise médicalisée des dépenses de santé.
[1340] P. LAFARGE, « Secret professionnel, confidentialité et nouvelles technologies d'informations », *Gaz. Pal.* 1998, pp. 481-489.
[1341] C'est le terme utilisé par la CNIL dan la délibération n° 85-39 du 10 septembre 1985 portant avis sur le projet d'arrêté du Ministère des Affaires Sociales et de la Solidarité Nationale relatif à l'informatisation dans les établissements hospitaliers des résumés de sortie standardisés (RSS) élaborés dans le cadre du projet de médicalisation du système d'information.
[1342] Décret n° 94-666 du 27 juillet 1994 relatif aux systèmes d'informations médicales et à l'analyse de l'activité des établissements de santé publics et privés et modifiant le code de la santé publique (deuxième partie : Décrets en Conseil d'Etat).
[1343] CSP, art. L. 6113-7.

devenu l'article R. 6113-5 du même code, qui désigne ces personnes et prévoit leur assujettissement au secret professionnel en faisant expressement référence à l'article 226-13 du Code pénal.

Ce texte a connu une évolution importante, modifié par un décret du 26 décembre 2018[1344]. La CNIL est encore à l'origine de cette modification. Il faut noter, au préalable, que l'analyse de l'activité médicale est la source de financement principale des établissements, c'est en fonction de cette analyse que les soins des établissements sont financés par la sécurité sociale. Le travail de codage des actes s'est perfectionné pour satisfaire à une logique de rentabilité croissante. Les établissements se sont trouvés contraints, pour optimiser le codage des actes, de faire intervenir des prestataires extérieurs[1345]. Cette pratique a été portée à la connaissance du public par un médecin chargé de l'information médicale au sein d'un établissement public[1346]. A la suite de ces révélations, la CNIL s'est saisie du dossier et a prononcé une mise en demeure de l'établissement en question[1347]. A cette occasion, la Commission a constaté que si les prestataires extérieurs sont tenus à la discrétion par une clause de confidentialité, ils ne sont pas astreints au secret professionnel, à l'inverse des personnes intervenant sous la direction du médecin comme le prévoit l'article R. 6113-5 dans son ancienne rédaction[1348]. Le décret du 26 décembre 2018 est finalement intervenu pour remédier à cette situation à l'occasion de l'entrée en vigueur du RGPD. Outre les dispositions spécifiquement attachées à la mise en œuvre du RGPD[1349], l'article soumet au secret professionnel les personnes intervenant dans l'établissement support des groupements hospitaliers de territoires chargées de l'évaluation de l'activité médicale des autres établissements parties[1350], les

---

[1344] Décret n° 2018-1254 du 26 décembre 2018 relatif aux départements d'information médicale.

[1345] V. par exemple : IGAS, *L'évolution du volume d'activité des établissements de santé : description, déterminants et prévision*, sept. 2013, spéc. pp. 82-83.

[1346] J.-J. TANQUEREL, *Le sermet d'hypocrite. Secret médical, le grand nauvrage*, coll. Essais-Documents, Max Milo, 2014.

[1347] Décision n° 2013-037, 25 sept. 2013.

[1348]« *En effet, ces pratiques conduisent à permettre un accès à des données couvertes par le secret médical par des tiers non autorisés, ce qui constitue un manquement à l'obligation de confidentialité des données* » (*Ibid.*).

[1349] Concernant l'étendue de l'information données aux personnes soignées (CSP, art. R. 6113-7), la traçabilité des accès et opérations effectuées sur les données (CSP, art. R. 6113-9-2).

[1350] Les Groupements hospitaliers de territoires sont des modes de coopération entre les établissements publics de santé à l'échelle d'un territoire. Chaque établissement est partie à une convention instituant le GHT autour d'un projet de santé commun. Dans cette hypothèse, un seul établissement peut être désigné pour être le support de l'analyse de l'activité médicale de tous les établissements parties à la convention. Sur les conventions de GHT :

intervenants sur le matériel et les logiciels utilisés pour le traitement, les commissaires aux comptes qui ont accès, pour consultation uniquement et sans possibilité de création ou de modification aux traitement de données ainsi que les prestataires extérieurs qui inteviennent sous la responsabilité des médecins du département d'information médicale. Ainsi, toutes les personnes qui auraient accès à ces données, même de manière incidente et ponctuelle, sont soumises au secret professionnel. Plutôt que d'interdire l'accès aux données, il a été préféré de soumettre au secret professionnel les personnes en raison de la nécessité d'accéder aux données issues de la relation de soin alors même qu'*ils ne participent pas à la prise en charge*. Ils ne sont *ni des confidents, ni des dépositaires, pas plus que des détenteurs*. La nécessité ne tient pas, quant à elle, au rôle social de ces acteurs mais *aux finalités du traitement*. Aussi, c'est la source des données, le fait qu'elle soient couvertes par le secret professionnel qui justifie leur assujettissement au secret professionnel.

291. Le cas du délégué à la protection des données. Il convient, en outre, de constater que les délégués à la protection des données, dont la désignation est rendue obligatoire pour certains traitements de données depuis l'entrée en vigueur du RGPD[1351], tiennent une place essentielle dans le traitement des données de santé, donc également dans le cadre du traitement des données issues de la prise en charge des patients par une personne intervenant dans le système de santé[1352]. Toutefois, le RGPD précise simplement que « *le délégué à la protection des données est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres* »[1353]. Or, aucun texte ne prévoit expressement que les délégués à la protection, dans le domaine de la santé, sont soumis au secret professionnel. Une telle solution pourrait néanmoins se déduire de l'article L. 1110-4 du Code de la santé publique selon l'interprétation qui en est admise. Dans l'hypothèse d'un traitement de données consistant en une réutilisation des données issues des soins, il serait également envisageable de le déduire de l'article 68 du RGPD prévoyant que les personnes appelées à mettre en oeuver ce type de traitement, ainsi que

---

J. HARDY « Les catégories juridiques à l'épreuve de la réforme administrative », *AJDA* 2017, p. 919 ; C. BERGOIGNAN-ESPER, « L'hôpital public au sein du plan « Ma santé 2022 » », *RDSS* 2019, p. 15. A propos de l'établissement-support : F. VARNIER, M. TREPEAU, « La coopération hospitalière au service de la modernisation de notre système de santé », *RDSS* 2016, p. 620.

[1351] Section 4 du RGPD.

[1352] Leur désignation est obligatoire dans presque toutes les situations en ce qui concerne le traitement des données issues de la relation de soin (exception faite, en général, des traitements mis en œuvre par des professionnels de santé en exercice individuel).

[1353] RPGD, art. 38.

celles qui ont accès aux données sur lesquelles il porte, sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du Code pénal.

B - Le stockage des données

292. Le recours à des tiers pour le stockage sécurisé des données. Le traitement des données issues de la prise en charge des personnes dans le système de santé a eu pour conséquence notable de déposséder, en partie, le professionnel de santé des informations qu'il produit sur le patient. Lorsque les supports de l'information faisaient l'objet d'un stockage physique, le médecin et les professionnels de santé en étaient les seuls détenteurs. De même, en milieu hospitalier, le stockage et l'archivage étaient mis en œuvre au sein des établissements par le personnel de l'hôpital. Sans marquer la fin du stockage physique et des supports papier[1354], le traitement informatique des données issues de la relation de soin se caractérise par un besoin croissant d'espace numérique de stockage mais la sensibilité des données impose une sécurité accrue, les structures participant au parcours de santé des personnes – publiques ou privées – traitant des données couvertes par le secret professionnel externalisent ce service.

Par la loi du 4 mars 2002, le législateur a donc instauré des règles spécifiques concernant le stockage et la conservation des données issues de la prise en charge des personnes dans le système de santé. L'hébergement des données de santé, lorsqu'il n'est pas effectué par l'établissement ou le professionnel, peut être externalisé. En toutes hypothèses, les prestataires de service d'hébergement ou l'établissement qui hébergent des données de santé à caractère personnel devront obtenir un certificat de conformité délivré par l'organisme de certification qualifié[1355]. Les hébergeurs de données de santé sont soumis au secret professionnel en vertu de l'article L. 1111-8, V, al. 2 du Code de la santé publique qui précise : « *Les hébergeurs de données de santé à caractère personnel et les personnes placées sous leur autorité qui ont accès*

[1354] L'article L. 1111-8 du Code de la santé publique prévoit les conditions d'hébergement pour les données de santé à caractère personnel mais également pour les informations représentées sur support papier. Toutefois, le régime de l'hébergement de ces dernières requiert un agrément du ministère de la Culture (cela est également valable pour les données dans le cadre de l'archivage électronique) : Loi n° 2008-696 du 15 juillet 2008 relative aux archives et Décret n° 2009-1124 du 17 septembre 2009 modifiant le décret n° 79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques.

[1355] Ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel.

aux données déposées sont astreintes au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pénal ». Il convient de remarquer que, malgré la formule employée pour le qualifier, le recours à un hébergeur de santé n'est obligatoire que pour les traitements de données de santé à caractère personnel « *recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social* »[1356]. Les données de santé qui seraient traitées par des acteurs n'ayant aucun lien avec ces activités – lorsque le consentement de la personne est obligatoire – ne requièrent donc pas ce type d'hébergement. Cela tend à confirmer que le *critère qui justifie leur soumission au secret tient dans la source originelle dont elles émanent*[1357].

293. La portée incertaine du secret des hébergeurs de données de santé. La rédaction du texte laisse des zones d'ombre quant au régime de ce secret. S'il semble commode d'affirmer que le secret professionnel des hébergeurs de données de santé découle de leur qualité « *d'intervenants dans le système de santé* »[1358], l'existence d'un texte spécifique semble contrevenir à une telle interprétation. Ce qu'appuie, en outre, l'absence de renvoi à l'article 226-14 prévoyant les faits justificatifs spéciaux inscrits à l'article 226-14 du Code pénal. Il apparaît, en outre, que l'hébergeur ne saurait bénéficier de l'autorisation de la loi de partager ou d'échanger des données au même titre que les professionnels inscrits à l'article L. 1110-4 du Code de la santé publique. L'article L. 1111-8, V du même code précise que « *L'accès aux données ayant fait l'objet d'un hébergement s'effectue selon les modalités fixées dans le contrat dans le respect des* articles *L. 1110-4 et L. 1111-7* ». Les modalités d'accès prévues

---

[1356] CSP, art. L. 1111-8.

[1357] *Contra*, considérant que c'est la nature des données qui le justifie, v. I. VACARI, « L'hébergement des données de santé : entre contrat et statut », *RDSS*, 2002, p. 695 « […] *la nature des données qu'ils hébergent fait entrer les hébergeurs dans le cercle des professionnels intervenant dans le système de santé. Aussi le législateur leur a-t-il étendu les institutions les plus caractéristiques du statut des professions de santé : l'agrément, le contrôle ou le secret* ».

[1358] En dehors de Madame Vacari, d'autres auteurs affirment que les hébergeurs de données sont des professionnels intervenant dans le système de santé au même titre que les professionnels de santé et qu'en conséquence ils sont également soumis au « *secret médical* », soit à un secret professionnel répondant au même régime que le secret des professionnels de santé (J.-F. FORGERON et V. SEGUINOT, « Le dossier médical personnel : L'activité des hébergeurs de données de santé », *Gaz. Pal.*, 26 janv. 2006, n° 26, p. 10).

correspondent à celui du « secret partagé » et au droit d'accès reconnu aux personnes concernées et aux tiers en cas de décès[1359].

294. L'hébergeur de données de santé, détenteur des données ? Le terme de « *coffre-fort numérique* »[1360] parfois utilisé pour qualifier les prestations proposées par les hébergeurs de données illustre les particularités de ce type de contrat que la doctrine a pu qualifier de contrat de dépôt[1361]. Les services d'hébergement de données ont connu des évolutions techniques importantes depuis l'apparition du « *cloud computing* »[1362]. Certains ont pu le qualifier de

---

[1359] « *En cas de décès du malade, l'accès des ayants droit, du concubin ou du partenaire lié par un pacte civil de solidarité à son dossier médical s'effectue dans les conditions prévues au dernier alinéa du V de l'article L. 1110-4* » (CSP, art. 1111-7 *in fine*).

[1360] La CNIL a adopté une recommandation concernant les prestations de services dites de « coffre-fort numérique », relative à l'hébergement des données personnelles. Elle rappelle que, s'agissant du stockage de données de santé à caractère personnel, ce type de service est encadré par le Code de la santé publique.

[1361] G. PIGNARRE, « Le contrat de dépôt éclairé par le prisme de l'opération de qualification », *AJ contrat* 2016, p. 508 ; A. GENDREAU, « La dématérialisation du dépôt : l'exemple du contrat de cloud computing », *AJ contrat* 2016, p. 519 ; P.-Y. GAUTIER, « Du contrat de dépôt dématérialisé : l'exemple du cloud computing », *in* B. TEYSSIE (ss. la dir.), *La communication numérique, un droit, des droits*, éd. Panthéon-Assas, 2012, p. 157 et svt. : « *La tradition classique ne pouvait imaginer ce que les progrès de la technique pourraient faire comme prodiges, en dématérialisant le monde réel : « l'immatériel n'en reste pas moins réel », aux sens de la physique et du droit. C'est très métaphysique. De sorte qu'il n'existe pas d'obstacle déterminant à faire entrer le « cloud computing » dans ce vieux contrat, ce qui lui donnera un « coup de jeune »* » (également cité par G. PIGNARRE, « Le contrat de dépôt éclairé par le prisme de l'opération de qualification », *op. cit.*). Toutefois, certains auteurs refusent de considérer que le contrat d'hébergement ou celui de *cloud computing* puisse être qualifié de contrat de dépôt, lequel exige le dépôt et la garde d'une chose corporelle. En ce sens, v. G. BRUNAUX, « Cloud computing, protection des données : et si la solution résidait dans le droit des contrats spéciaux ? », *D.* 2013. p. 1158.

[1362] Il s'agit d'un hébergement amélioré dans la mesure où il permet, à la différence des techniques d'hébergement précédentes, lesquelles consistent dans la « location » d'un espace de stockage limité sur des serveurs que l'on peut situer physiquement, d'un service de stockage d'une capacité illimitée. L'image du « nuage » vient du fait que, dans ce genre d'infrastructure, les applications et leurs données sont contenues dans des ordinateurs distants (Communication de la Commission européenne, *Exploiter le potentiel de l'informatique en nuage en Europe*, 2012). La locution connaît plusieurs définitions : « *Mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire. L'informatique en nuage est une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients* » (Commission Générale de Terminologie et de Néologie - JO du 6 juin 2010 - texte n° 42 - Vocabulaire de l'informatique et de l'internet - NOR : CTNX1012892X) ; « *Modèle qui permet d'accéder par le réseau à une masse évolutive et élastique de ressources physiques ou virtuelles et qui implique un service à la demande et une administration à la demande. Précision : Quelques exemples de ressources incluent les serveurs, les OS, les réseaux, les logiciels, les applications et les équipements de stockage* » (Norme ISO/IEC 17788 : 2014) ; « *L'expression "Cloud computing", ou "informatique dans les nuages", recouvre une variété de services fondés sur un aménagement du mode de fonctionnement des systèmes informatiques et de communication, qui se caractérise par le stockage à distance de données dans le but d'en permettre la consultation et/ou la reproduction sur une pluralité d'appareils, connectés à internet, au profit des utilisateurs de cette technologie.* » (CSPLA, Rapport « Informatique dans les nuages », 23 oct. 2012) ; « *Le Cloud computing est un modèle permettant l'accès sur demande, permanent, commode à un lieu de partage en temps réel des ressources informatiques (p. ex., réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement configurées et libérées avec une interaction et un effort minimal de la part du fournisseur du service* » (The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology - NIST

contrat de dépôt dématérialisé[1363] puisque se retrouvent les obligations à la charge du dépositaire : la garde de la chose, l'obligation de non-utilisation et la restitution de la chose[1364].

Que le contrat d'hébergement puisse ou non être qualifié de contrat de dépôt, il demeure que le rôle de l'hébergeur de données de santé à caractère personnel ainsi que de l'hébergeur en général est « purement technique ».

295. Remarque générale sur le secret professionnel des acteurs techniques. Le secret professionnel des prestataires techniques nous semble être une forme de secret « dégradé ». Le mouvement amorcé par le législateur contemporain, consistant à étendre toujours davantage le champ d'application du secret professionnel, se confirme de manière plus nette les concernant. Outre que le critère de désignation tient désormais clairement dans la nécessité de leur permettre l'accès à des données couvertes par le secret, un changement essentiel doit être relevé : tandis que l'infraction punissant la violation du secret professionnel sanctionnait la « confiance trahie », cette technique juridique de protection de l'information sert désormais davantage à inspirer la confiance. En d'autres termes, l'infraction, qui sanctionnait la rupture d'un lien de confiance forgé par une rencontre entre deux individus, a désormais *aussi* pour but d'inspirer la confiance dans ces acteurs. Plus encore que la confiance des individus envers ces prestataires inconnus d'eux, c'est la construction d'une confiance des professionnels de santé envers ces nouveaux acteurs qui semble également justifier leur soumission au secret professionnel. Quant à la nécessité de leur activité dans la société – nécessité qui était à l'origine l'apanage de certaines professions seulement –, elle interroge également. De manière plus générale, il est aujourd'hui acté que le droit est un vecteur de confiance dans les dispositifs techniques[1365]. Ainsi Madame Rochfeld, à propos de la loi pour la confiance dans l'économie numérique,

---

- US Department of Commerce - Sept. 2011). Ces définitions sont également citées par C. ZORN, « Contrats de Cloud computing et données personnelles : éléments de rénovation des techniques contractuelles », *Dalloz IP/IT*, 2016, p. 453. Le *cloud computing* a amené les auteurs à pointer les insuffisances de la législation relative à la protection des données avant l'entrée en vigueur du RGPD en raison, notamment, du caractère territorial des règles tandis que l'informatique en nuage est, par nature, « *ubiquitaire* » (C. ZOLINSKY et A. BENSAMOUN, « Cloud computing et big data. Quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux* 2015/1 n° 189, pp. 103-121). Le champ d'application de la législation depuis l'entrée en vigueur du RGPD a été élargi en conséquence (RGPD, art. 3).

[1363] A. GENDREAU, « La dématérialisation du dépôt : l'exemple du contrat de cloud computing », *op. cit*.

[1364] P.-Y. GAUTIER, « Le dépôt : exercice de qualification », *RDC* 2014, p. 149.

[1365] G. HAAS, A. DUBARRY, M. D'AUVERGNE, R. RUIMY, « Enjeux et réalités juridiques des Objets Connectés », *Dalloz IP/IT* 2016, p. 394.

remarque qu'elle « *entend promouvoir l'usage des nouvelles technologies, par la confiance que ces dernières seraient à même d'inspirer chez leurs utilisateurs* »[1366]. Notons d'ailleurs, que l'article 6 de la loi prévoit que les hébergeurs de données personnelles recueillies sur internet sont soumis au secret professionnel, alors que leur activité est économique plutôt que sociale. Se pose, dès lors, la question de savoir si la société peut perdurer sans l'internet et, *a fortiori*, sans les technologies de l'information et de la communication. L'interrogation dépasse, certes, le cadre de notre étude, mais laisse entrevoir toute la complexité des transformations induites par la société de l'information et de la communication.

§ 2 - L'assujettissement au secret professionnel des personnes réutilisant les données

296. Deux catégories de personnes ont été soumises au secret professionnel pour leur permettre de réutiliser des données issues de la relation de soin, à des fins d'élaboration de statistiques **(A)** et à des fins de recherche dans le domaine de la santé **(B)**.

A - La réutilisation des données pour l'élaboration des statistiques

297. Le secret professionnel en matière de statistiques. Dès 1986, les agents de l'Institut national de la statistique et des études économiques (INSEE) ont été soumis au secret professionnel[1367], mesure conçue comme une garantie permettant à ces agents d'accéder aux données personnelles. Les travaux préparatoires de la loi de 1986 sont, à cet égard, éclairants : « *Les auteurs du projet de loi ont ainsi entendu permettre à l'INSEE et aux services statistiques ministériels de partager le secret professionnel auquel sont tenues les administrations dépositaires d'informations relatives aux personnes physiques ou aux personnes morales : cette obligation au secret n'étant que le corollaire de la faculté d'obtenir des administrations toute information dès lors que la finalité exclusive du transfert est l'élaboration de statistiques* »[1368]. Dès 1994, une exception est posée au secret professionnel des professionnels de santé, de sorte que les agents de l'INSEE puissent accéder également aux données recueillies par ces derniers. La soumission au secret professionnel est une condition de partage et d'accès aux données

---

[1366] J. ROCHFELD, « La loi n° 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique », *RTD civ*. 2004, p. 574.
[1367] Loi n° 86-1305 du 23 décembre 1986 portant modification de la loi 51711 du 07-06-1951 sur l'obligation, la coordination et le secret en matière de statistiques (*JORF*, 26 déc. 1986, p. 15596).
[1368] J. THYRAUD, Rapport n° 530 fait au nom de la commission des lois, 29 oct. 1986.

produites par les professionnels de santé exerçant dans les établissements publics. En somme, il ne s'agit plus seulement de soumettre au secret professionnel les personnes dont l'intervention est nécessaire pour permettre la mise en œuvre du traitement des données dans le respect de la loi, comme c'est le cas de ceux que nous avons désignés comme des acteurs techniques, mais d'astreindre au secret professionnel les personnes dont les pouvoirs publics souhaitent qu'elles puissent accéder aux données. L'extension du champ d'application du secret professionnel est, en somme, la première étape d'un processus visant à permettre la réutilisation des données et partant leur circulation. La seconde étape consistant systématiquement en l'érection d'un nouveau fait justificatif, que nous aurons l'occasion d'évoquer ultérieurement, d'autant que la question se prolonge au travers de l'*open data en santé*[1369]. Le processus est davantage perceptible s'agissant de la recherche dans le domaine de la santé.

B - La réutilisation des données pour la recherche dans le domaine de la santé

298. La soumission au secret professionnel et la réutilisation des données issues de la relation de soin. La question des conditions de réutilisation des traitements de données issues de la relation de soin à d'autres fins que la prise en charge des personnes a été posées à la CNIL dès 1980. Tandis qu'elle rendait un avis défavorable pour la mise en œuvre du fichier GAMIN[1370] en raison de l'inadéquation des données traitées par rapport aux finalités déclarées[1371], elle reconnaissait néanmoins « *l'intérêt que présente l'établissement de statistiques anonymes* […] *pour la recherche médicale et spécialement l'étiologie des handicaps* »[1372] et formulait à cet effet un avis favorable à l'utilisation du fichier dans son application *statistique et anonyme*. La réutilisation des données issues de la relation de soin à des fins de recherche épidémiologique s'est posée de façon bien plus évidente, dans la même décennie, à propos des traitements ayant vocation à constituer des « *registres du cancer* »[1373]. Réutiliser les données nécessite qu'elles soient transmises par leur détenteur premier. Dans le

[1369] V. *infra* n° 382.
[1370] CNIL, Délibération n° 81-74 du 16 juin 1981 portant décision et avis relatifs à un traitement d'informations nominatives concernant le traitement automatisé des certificats de santé dans les services de la protection maternelle et infantile.
[1371] Considérant notamment que la subjectivité des informations recueillies présente un risque pour les libertés des personnes (CNIL, *Rapport d'activité 1980-1981*, p. 28 et svt).
[1372] *Ibid.,* p. 30.
[1373] V. *supra* n°234.

cas des données de santé, il s'agit du responsable de traitement, qu'il s'agisse d'un professionnel de santé ou d'un établissement de santé. A l'époque de la mise en œuvre des registres du cancer, la CNIL avait habillement souligné l'illégalité de ces transmissions[1374]. L'intervention tardive du législateur s'est faite à un double niveau. Il a astreint au secret professionnel toutes les personnes accédant et traitant des données issues de la relation de soin à des fins de recherche. De surcroît, il a créé un fait justificatif au secret professionnel dans le but d'autoriser les professionnels de santé à communiquer les données aux chercheurs. L'extension du champ d'application de l'infration s'accompagne donc d'un affaiblissement de la force du secret. L'évolution des dispositions créées par le législateur en 1994 doit être mise en exergue.

299. Un texte de désignation particulièrement compréhensif. Les modifications apportées à la loi informatique et libertés par une loi dédiée aux traitements des données pour des finalités de recherche dans le domaine de la santé[1375] a surtout été commentée en raison de l'aménagement du secret professionnel qu'elle érige[1376]. Il n'est, par contre, jamais porté attention à l'assujetissement au secret professionnel qui en découle. Il faut, pour prendre la mesure de son intérêt, revenir aux travaux préparatoires de la loi. L'intérêt collectif de l'utilisation des données issues de la relation de soin pour la recherche dans le domaine de la santé avait convaincu le législateur qui avait pris acte, sous l'influence évidente de la CNIL, de la nécessité de poser une nouvelle exception au secret professionnel. Ainsi, dans un rapport au sénat, Monsieur Türk, alors membre de la Commission des lois du Sénat, a exposé les raisons pour lesquelles un « aménagement » du secret professionnel était nécessaire afin de permettre la transmission des données – qualifiées de nominatives à cette époque – à des fins de recherches médicales. Ce rapport éclaire, par ailleurs, les raisons pour lesquelles l'ancien article 40-3 de la loi informatique et libertés – actuel article 68 – soumettait au secret professionnel les personnes accédant aux données : « *Pour les besoins de la recherche, il aménage le secret*

[1374] V. *supra* n° 224.
[1375] Loi n° 94-548 du 1 juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[1376] I. DE LAMBERTERIE et H.-J. LUCAS, *Informatique, libertés et recherche médicale*, coll. CNRS droit, CNRS, 2002.

professionnel afin de permettre la transmission des données de santé tout en garantissant très strictement leur confidentialité par l'extension du secret à toute la chaîne de ceux qui les manipulent »[1377]. L'extension du champ d'application du secret professionnel à toutes les personnes qui manipulent les données appelle quelques remarques. D'abord, les personnes concernées ne sont pas clairement désignées, rendant la loi peu lisible[1378] ; surtout, parce que cette formule ne désigne en réalité personne, elle permet de désigner *tout le monde*.

300. Un seul critère, l'accès aux données ? Il suffit de constater l'extension du champ d'application de ce qu'était, auparavant, le chapitre V de la loi informatique et libertés pour se convaincre de ce que le critère légitimant l'assujettissement au secret professionnel tient uniquement à la source des données auxquelles il est donné accès. Ce chapitre de la LIL était en effet exclusivement consacré au traitement des données issues de la prise en charge dans le domaine de la santé. Les chapitres V *bis* et V *ter* prévoyaient des conditions de traitement de données de santé à caractère personnel différenciés. S'agissant, pour le premier, d'un chapitre portant sur les traitements automatisés de données « nominatives » ayant pour finalité la recherche dans le domaine de la santé, il prévoyait, en son article 40-3, l'exception au secret professionnel afin de permettre la transmission de données nominatives détenus par des professionnels de santé à des organismes de recherche[1379] ainsi que la soumission au secret

---

[1377] A. TURK, Rapport n° 209, sur le projet de loi relatif au traitement de données nominatives ayant pour fin la recherche en vue de la protection ou l'amélioration de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Le constat de cette extension du champ d'application de l'infraction est également soulevé par un auteur : « *Elle* [la vie privée] *doit être protégée contre les indiscrétions, les divulgations. Le respect de la vie privée passe par la confidentialité. Cette confidentialité est principalement et traditionnellement assurée par l'incrimination de violation du secret professionnel. Mais cette seule incrimination ne saurait suffire, car ne protégeant pas des indiscrétions commises par ceux qui ne sont pas astreints au secret professionnel. Deux solutions s'offrent alors au législateur : soit augmenter le nombre des personnes soumises au secret, soit créer des incriminations spécifiques. En matière de santé, ces deux voies ont été suivies. L'astreinte au secret professionnel a été étendue à toute personne appelée à mettre en oeuvre le traitement de données nominatives (ou ayant accès à ces données) ayant pour fin la recherche dans le domaine de la santé, d'une part* (l'auteur fait référence à l'article 40-3 de la LIL). *D'autre part, en matière de suivi thérapeutique, est incriminée toute atteinte ou tentative d'atteinte à la confidentialité du dossier médical ; et les lois dites bioéthiques ont toutes, avec leurs sanctions spécifiques, incriminé la divulgation d'informations*. » (G. GIUDICELLI-DELAGE, « Droit à la protection de la santé et droit pénal en France », *RSC* 1996, p. 13).

[1378] Cette manière de procéder est symptomatique du droit pénal technique qui privilégie « *l'efficacité de la norme pénale à sa qualité* » (P. MISTRETTA, « La médecine énergétique traditionnelle chinoise et les piqûres du droit pénal médical », *RSC* 2015 p. 413).

[1379] L'article 40-3 de la loi informatique et libertés dispose : « *les personnes appelées à mettre en œuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte, sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du Code pénal* ». Messieurs Frayssinet et Pedrot soulignent que cette disposition permet d'assurer « *la confidentialité tout au long de la chaîne de traitement* » et remarquent encore que, sur ce point, la loi n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi du 6 janvier 1978 relative à l'informatique,

professionnel des chercheurs. Le chapitre V *ter* énonçait, quant à lui, les conditions de traitement automatisé des données personnelles de santé à des fins d'évaluation ou d'analyse des activités de soins et de prévention. Il s'agissait des données issues des systèmes d'informations[1380]. Concernant ces catégories de données, l'article 40-12 disposait qu'elles ne pouvaient « *être communiquées à des fins statistiques d'évaluation ou d'analyse des pratiques et des activités de soins et de prévention que sous la forme de statistiques agrégées ou de données par patient constituées de telle sorte que les personnes concernées ne puissent être identifiées* ». La loi du 26 janvier 2016 relative à la modernisation du système de santé est ensuite intervenue pour rassembler ces deux chapitres au sein d'un unique chapitre IX inséré dans la LIL, relatif aux traitements de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé. L'article 55 de ce chapitre reprenait en substance l'ancien article 40-3 mais acquérait une portée générale, s'appliquant à tous les traitements et non plus seulement à ceux concernant la recherche. Depuis la loi du 24 juillet 2019[1381], une dernière modification a encore étendu son champ d'application puisque la section III qui en dispose désormais vise les « *Traitements de données à caractère personnel dans le domaine de la santé* » et concerne des traitements qui doivent seulement être mis en œuvre *en considération d'une finalité d'intérêt public*[1382]. Ce qui était autrefois décrit comme un décloisonnement entre le soin et le recherche, apparaît sous cet angle comme la marque d'une instrumentalisation du secret professionnel. Présenté comme une institution, celui-ci est réduit à une technique de préservation de l'information dénuée de fondement éthique, un outil pour construire la confiance.

D'autres textes ont, par la suite, astreint au secret professionnel des personnes non désignées, en raison de l'autorisation qui leur a été faite d'accéder aux données issues de la relation de soin. Ainsi, l'article L. 1461-1 du Code de la santé publique, qui fixe les modalités

---

aux fichiers et aux libertés « *a le mérite d'attirer l'attention sur les solidarités fonctionnelles et pénales qui existent entre tous les participants, à des titres divers, à la protection du secret* » (J. FRAYSSINET et P. PEDROT, « La loi du 1er juillet 1994 relative au traitement des données nominatives ayant pour fin la recherche dans le domaine de la santé », *JCP G* 1994, doctr. 3810).

[1380] CSP, ancien art. 710-6.

[1381] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (*JORF* n° 0172, 26 juill. 2019).

[1382] LIL, art. 66.

de mise à disposition des données de santé[1383], encadre également la mise à disposition des données du système national des données de santé et des traitements utilisant des données à caractère personnel issues de ce système. Le IV, 2° de cet article dispose : « *Les personnes responsables de ces traitements, ainsi que celles les mettant en œuvre ou autorisées à accéder aux données à caractère personnel qui en sont issues, sont soumises au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pén*al ». Ainsi présentée, la soumission au secret professionnel semble trouver sa seule justification dans la source des données auxquelles il est donné accès. La formulation suggère en effet que toute autorisation d'accès entraîne soumission au secret professionnel.

301. Remarque sur la portée de ces secrets professionnels. Les exemples qui viennent d'être exposés ont comme spécificité de ne pas faire référence dans le texte de désignation – si tant est que l'on puisse encore les qualifier comme tels – à l'article 226-14 du Code pénal. Il en résulte que les personnes astreintes au secret professionnel en vertu de ces textes ne peuvent se prévaloir des faits justificatifs spéciaux. L'option de conscience[1384], qui fait la particularité du secret professionnel des professions libérales, ne leur est pas offerte. Si certains ont pu saluer l'établissement, par ce texte, d'« *une solidarité dans le respect du secret professionnel* »[1385] ou d'un « *secret professionnel élargi* »[1386], cette particularité en fait néanmoins des secrets professionnels de second rang.

§ 3 - Une diversification des sources du secret professionnel

302. Recherche translationnelle et médecine personnalisée, effacement des frontières et soumission généralisée au secret professionnel ? Il est un dernier élément qu'il nous faut mentionner. Les évolutions conjointes de la science médicale et de l'informatique ont engendré une imbrication croissante des disciplines et ont contribué à brouiller les frontières entre la

---

[1383] L'ouverture des données de santé désignée sous le terme « *open data* » concerne les données publiques, c'est-à-dire les données anonymisées. Sur *l'open data*, v. L. CLUZEL-METAYER, « Les limites de l'open data », *AJDA*, 2016, p. 102. Sur l'*open data*, v. *infra,* n° ¤.

[1384] V. *infra,* n°351.

[1385] J. FRAYSSINET, « Données nominatives et recherche biomédicale », *Médecine et Droit*, sept.-oct. 1995, n° 8, p. 111.

[1386] C. MARLIAC-NEGRIER, *La protection des données nominatives informatiques en matière de recherche médicale*, préf. M. GENIOT, PUAM, 2001, p. 535 ; A. COULIBALY, *La protection des données à caractère personnel dans le domaine de la recherche scientifique*, th. dact., ss. la dir. d'E. VERGES et I. DE LAMBERTERIE, soutenue le 25 nov. 2011, Université de Grenoble, p. 671.

recherche et le soin[1387]. Il est désormais question de « recherches translationnelles » et de « médecine personnalisée ». La recherche translationnelle « *est une activité aux interfaces entre recherche fondamentale et clinique, fluidifiant et accélérant les échanges bidirectionnels entre la recherche à visée cognitive et la recherche orientée vers les patients, ou la recherche à visée cognitive et la santé des populations* »[1388]. La médecine personnalisée est, quant à elle, une application de cette recherche, elle exige « *une connaissance plus fine de l'individu au niveau de sa génétique et de son environnement. La personne est davantage appréhendée par son identité biologique et physique unique* »[1389]. L'effacement progressif des frontières entre le soin et la recherche passe par le prisme du traitement des données[1390] et implique non seulement une multiplication des acteurs mais également une diversité de leurs profils au fil des progrès techniques. La massification des données – les *Big Data* – a par exemple engendré l'émergence de nouveaux acteurs essentiels pour le développement de l'intelligence artificielle : les *data analyst* ou *data scientist*[1391]. L'ubiquité des données engendré par les *Big Data* est aussi un facteur de la multiplication des acteurs appelés à les traiter. S'il est tentant d'affirmer qu'ils sont tous soumis au secret professionnel dès lors qu'ils ont accès à des données à caractère

---

[1387] B. BEVIERE-BOYER, « Médecine personnalisée : de la délimitation entre le soin et la recherche », *in* C. HERVE et M. STANTON-JEAN (ss. la dir.), *Les nouveaux paradigmes de la médecine personnalisée ou médecine de précision*, coll. Thèmes & Commentaires, Dalloz, 2014, p. 129.

[1388] D. THOUVENIN, « La recherche translationnelle. Présentation de la Journée d'étude « Les frontières entre recherche et soin : Diagnostic et pronostics juridiques » », *in* M. BERNELIN et E. SUPIOT (ss. la dir.), *Les frontières entre recherche et soin : Diagnostics et pronostics juridiques*, Cahiers Droit, Sciences & Technologies, PUAM, 2015, pp. 25-38, spéc. n° 12.

[1389] B. BEVIERE-BOYER, « Médecine personnalisée : de la délimitation entre le soin et la recherche », *op. cit.*, spéc. p. 130.

[1390] « *Les progrès dans le domaine de la génétique, de la génomique, des biotechnologies, de la bio-informatique, de l'imagerie, de l'utilisation des données personnelles (Big Data), de la thérapie génique, de la pharmaco-génomique* » (*Ibid.*) sont au centre de la médecine personnalisée. « *Le caractère translationnel de la recherche correspond à une organisation marquée par un impératif de rapidité, qui nécessite le regroupement, au sein d'un même pôle, de scientifiques travaillant en recherche fondamentale, d'experts techniques divers (informatique, imagerie, ingénierie) et de médecins, investigateurs et/ou cliniciens. Se profile ainsi un véritable continuum de la recherche, c'est-à-dire un processus fluide et ininterrompu allant du laboratoire au lit du patient et vice et versa* » (Il s'agit de la présentation de l'appel à communication de la journée d'étude du réseau *Droit, Sciences & Technologies* ayant donné lieu à la publication précitée).

[1391] « *Ce terme désigne les experts de la gestion et de l'analyse des données massives. Ils conçoivent les modèles et algorithmes pour collecter, traiter et restituer les données. Il faut y ajouter les curateurs chargés de nettoyer les données* » (CCNE, Avis n° 130, *Données massives et santé : une nouvelle approche des enjeux éthiques*, 29 mai 2019, p. 18). Le Cour de cassation et le Conseil d'Etat ont d'ailleurs fait appel à deux *data scientist* pour mener à bien un projet visant, pour la première, à trouver « *les divergences jurisprudentielles* » au sein de la masse de ses décisions et pour la seconde à identifier « *des séries de contentieux faisant appel à une solution commune* » (G. THIERRY, « La Cour de cassation et le Conseil d'État s'emparent de l'intelligence artificielle », *Dalloz act.* 23 juill. 2019).

personnel issues de la relation de soin, le doute semble néanmoins permis. Ce doute est renforcé par l'analyse des méthodologies de référence de la CNIL.

303. Des textes de désignation au sein des méthodologies de référence ? Il a été observé que la CNIL, par le biais de certains de ses instruments, opérait des renvois aux articles 226-13 et 226-14 du Code pénal. En vue de faire disparaître progressivement les formalités préalables pour le traitement des données à caractère personnel dans le domaine de la santé et visant notamment la réutilisation des données issues de la prise en charge des personnes dans le système de santé, la loi du 26 janvier 2016 a apporté d'autres modifications à la loi informatique et libertés en prévoyant la possibilité pour la CNIL de prendre des méthodologies de référence[1392]. Ces méthodologies sont des outils de droit souple et ne sont donc pas contraignants. Elles servent simplement de références, comme leur nom l'indique, pour les responsables de traitement désireux de mettre en œuvre des traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé sans effectuer de formalités préalables. Un traitement qui ne serait pas conforme à ces méthodologies devrait donc obtenir une autorisation de la Commission. Les méthodologies MR-001[1393], 003[1394] et 004[1395] opèrent toutes un renvoi aux articles 226-13 et 226-14 du Code pénal en précisant que toutes les personnes listées dans la méthodologie de référénce sont soumises au secret professionnel. Si la valeur des instruments doit interdire de déduire que ces personnes[1396]) sont effectivement soumises au secret

[1392] « *Pour les catégories les plus usuelles de traitements automatisés de données de santé à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, la Commission nationale de l'informatique et des libertés peut homologuer et publier des méthodologies de référence destinées à simplifier la procédure d'examen. Celles-ci sont établies en concertation avec le comité d'expertise et des organismes publics et privés représentatifs des acteurs concernés* » (Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, art. 193).

[1393] Délibération n° 2018-153 du 3 mai 2018 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé avec recueil du consentement de la personne concernée (MR-001) et abrogeant la délibération n° 2016-262 du 21 juillet 2016 (*JORF* n° 0160, 13 juill. 2018).

[1394] Délibération n° 2018-154 du 3 mai 2018 portant homologation de la méthodologie de référence relative au traitement des données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé ne nécessitant pas le recueil du consentement de la personne concernée (MR-003) et abrogeant la délibération n° 2016-263 du 21 juillet 2016 (*JORF* n° 0160, 13 juill. 2018).

[1395] Délibération n° 2018-155 du 3 mai 2018 portant homologation de la méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches n'impliquant pas la personne humaine, des études et évaluations dans le domaine de la santé (MR-004) (*JORF* n° 0160, 13 juill. 2018).

[1396] Comme, par exemple, le personnel habilité agissant sous la responsabilité de l'organisme d'assurance garantissant la responsabilité civile du promoteur, cité dans les trois méthodologies de référence.

professionnel cela ne signifie pas que ces désignations sont dénuées de toute force normative[1397] dès lors qu'elles ont un veritable effet sur les pratiques et que l'ensemble des acteurs y adhèrent. Il n'est pas impossible d'ailleurs de rapprocher ce mode désignation des propositions « palliatives » de la CNIL consistant à proposer aux responsables de traitement de soumettre certains intervenant au secret professionnel par l'entremise d'un contrat[1398]. Ce qui confirme encore la vision utilitariste que la Commission a du secret professionnel et, sans doute, du droit.

304. Conclusion de chapitre. L'institution du secret professionnel a pour fonction première de réserver l'information. Le secret est par ailleurs la première protection de l'information et des savoirs puisqu'elle implique une absence de communication. L'on pourrait alors considérer que l'astreinte généralisée au secret professionnel est une démonstration de l'importance attachée à la protection des individus et à travers eux, de la société toute entière. Il se pourrait toutefois que cette généralisation doive s'analyser comme une façon d'assurer la circulation des données. Dès lors que la confidentialité a pour fonction d'*organiser* la réservation des données tout au long de leur cycle de vie, c'est-à-dire de prendre en compte leur ubiquité, le secret professionnel n'est plus qu'un instrument ordinaire, qu'un « secret » moyen parmi d'autres. L'influence de la CNIL dans le processus de généralisation du secret professionnel témoigne de la vision utilitariste qui le caractérise.

305. A l'occasion des septièmes entretiens du Conseil d'Etat en droit social sur le thème « *Santé et protection des données* »[1399], Monsieur Sauvé soulignait que « *La protection des données de santé est également assurée par l'obligation de secret pesant sur les professionnels*

[1397] Nous évoquerons à nouveau le concept de force normative. Il convient de retenir, pour le moment, qu'il s'agit d'un concept forgé par Madame Thibierge (C. THIBIERGE *et alii*, *La force normative. Naissance d'un concept*, LGDJ-Bruylant, 2009) lequel permet de penser les normes non plus seulement au regard des critères traditionnels de la juridicité mais par le jeu des relations entre trois pôles formés par la « valeur normative », la « garantie normative » et la « portée normative ». Ainsi, une norme peut émaner d'une autorité dont la légitimité est discutable (valeur normative faible), engendrer une réaction potientielle faible et effective nulle du système juridique pour en assurer le respect (garantie normative faible) mais produire des effets régulateurs sur les acteurs qui l'acceptent et la respectent (portée normative forte) (C. THIBIERGE, « Conclusion », *in* C. THIBIERGE *et alii*, *La force normative. Naissance d'un concept*, *op. cit.*, p. 821 et svt.).

[1398] V. *supra,* n°226.

[1399] *Les Entretiens du Conseil d'État en droit social : Santé et protection des données*, Colloque organisé par la section sociale et la section du rapport et des études du Conseil d'Etat, 1er décembre 2017.

de santé »[1400]. La soumission généralisée au secret professionnel comme conséquence du traitement des données issues d'information secrète dans le domaine de la santé paraît, à l'évidence, aller dans le sens d'une protection accrue des individus. Il nous semble toutefois que l'on peut également y voir un argument en faveur du traitement des données issues de la relation de soin. La confiance sécrétée par le secret professionnel doit en effet progressivement être accordée – par l'individu dont les données sont traitées et par les professionnels historiquement soumis au secret – à l'ensemble des personnes intervenant dans le traitement. En somme, le secret professionnel contribue autant à la protection de l'individu qu'à l'acceptation sociale du traitement généralisé des données issues de la relation de soin. La technique juridique du secret professionnel est *utilisée* comme moyen de changement social[1401] et l'une de ses fonctions se trouve au service du progrès apporté par le traitement des données. Si la fonction de protection de la vie privée demeure, il s'agit par ailleurs de créer la confiance, non plus dans des professions mais dans l'espace que constitue *l'écosystème des données*[1402] car « *il importe de susciter la confiance* »[1403] dans l'économie numérique. Deux remarques doivent enfin être formulées. La première est d'ordre terminologique : la diversité des secrets

---

[1400] *Ibid.* Introduction au colloque de J.- M. SAUVE disponible sur <http://www.conseil-etat.fr/Actualites/Discours-Interventions/Sante-et-protection-des-donnees#_ftnref6> (dernière consultation le 8 janv. 2019).

[1401] Le terme est employé en référence à l'*utilitarisme* : « *la conception instrumentale du droit* […] *est sous-jacente à une démarche où le droit est conçu comme moyen de changement social. Selon cette conception, le droit ne résume pas à un ensemble de règles qui a vocation à être appliqué par les juges pour résoudre des litiges. Il est surtout un instrument d'action, voire de lutte, qui permet d'encadrer les dynamiques sociales et économiques et de créer les conditions du progrès*. […] *La conception instrumentale mobilise l'idée capitale du droit comme outil inachevé, constructible et programmable pour résoudre des questions et défis concerts, par opposition à un système clos de règles générales instituées* ». Sur la notion d'utilitarisme v. R. VON JHERING, *La lutte pour le droit*, présentation d'O. Jouanjan, Dalloz bibliothèque, Dalloz, réedition 2006.

[1402] Le vocable « écosystème » est emprunté à la biologie, il est de plus en plus utilisé dans le discours politique et notamment sur les technologies (l'on dénombre cinquante-neuf occurrence du mot dans le rapport de la mission parlementaire dirigé par C. VILIANI intitulé *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne de la donnée*, La document Française, Mars 2018. Ce rapport préconise de « *renforcer l'écosystème européen de la donnée* » *ibid.* p. 26 et svt.). L'écosystème est défini comme un « *Ensemble formé par une communauté d'êtres vivants, animaux et végétaux, et par le milieu dans lequel ils vivent. Les composants d'un écosystème sont en interaction constante* ». L'écosystème est dans celui des données qui « *un complexe dynamique, agissant en interaction, doté d'unité fonctionnelle*. *La personne concernée est au centre de la régulation des données* » (B. FAUVARQUE-COSSON et W. MAXWELL, Protection des données personnelles, *op. cit.*). S'agissant d'un *milieu* dont les *composantes* sont en interaction constante, le terme est marqué par le dynamisme, le mouvement, les échanges de flux. Pour qu'un écosystème survive il ne faut pas contraindre sa nature dynamique, transposé aux données il s'agirait de l'alimenter et de favoriser la circulation des flux de données ce qui ne serait possible qu'avec la confiance de l'individu qui est au centre.

[1403] RGPD, consid. 7. Ce que remarquait d'ailleurs E. BROSSET lorsqu'elle constate l'influence conjointe du Conseil de l'Europe et de l'Union européenne dans l'élaboration des règles relatives à la protection des données et évoque le « […] *rôle complémentaire de l'exigence de respect des droits fondamentaux et de l'objectif du marché intérieur dans la construction de principes européens dans le domaine médical* » (E. BROSSET, « Brèves observations sur un secret de Polichinelle: l'influence du droit européen sur le droit médical à travers l'exemple du secret médical », *in* E. LECA (ss. la dir.), *Le secret médical*, LEH, 2012, Pp. 51-66).

professionnels, l'effacement des critères d'assujettissement permet de moins en moins d'user d'expressions trop précises comme celle de « secret médical » pour qualifier le secret professionnel dans le domaine de la santé. La seconde, concerne les différences de régime entre ces secrets, il nous semble qu'ils n'ont pas tous la portée. Certains sont de premier rang, ceux des professions historiquement soumises au secret professionnel tandis que le secret professionnel des acteurs techniques et des personnes réutilisant les données peut être qualifié de secret de « second rang ».

Chapitre 2 - La dilution du secret professionnel

306. L'extension du champ d'application de l'infraction sanctionnant la violation du secret professionnel ne semble pas être un gage d'affermissement de sa portée. En effet, toutes les fois qu'un nouveau texte de désignation apparaît, il est accompagné d'un aménagement au secret des professions qui sont en contact avec les patients, soit aux secrets que nous avons désignés comme des secrets professionnels de « premier rang ».

Cette extension semble donc s'accompagner d'une dilution du secret professionnel[1404]. Nous nous proposons de décrire le mouvement que nous désignons, au regard des finalités assignées aux traitement des données issues de la relation de soin. S'agissant majoritairement de traitements publics, notre étude consistera à mettre en lumière la façon par laquelle est opérée la balance entre les intérêts protégés par le secret professionnel et ceux au service desquels sont mis les traitements et les outils dont ils permettent l'efficacité. Notre démarche implique de mener notre étude tant sous l'angle du droit public que du droit privé **(Section 1)**.

La multiplication des permissions et des obligations de révéler ayant pour objet de permettre le traitement des données pour des finalités d'intérêt public fait apparaître un autre mouvement. Il est affirmé, de part et autre dans le discours politique, mais également dans celui des juristes et des économistes, que ces données sont des *communs* **(Section 2)**.

Section 1 - La multiplication des permissions et des obligations de révéler

307. Dans le cadre de ce développement il s'agira d'étudier d'une part les faits justificatifs érigés pour permettre certaines opérations de traitement **(paragraphe 1)** et de réserver un développement relatif à la place du consentement des personnes dans le processus d'affaiblissement du secret professionnel **(paragraphe 2)**. Ce dernier développement, à part des faits justificatifs, tient à ce que nous ne pensons pas que le consentement puisse revêtir la qualification de fait justificatif dans le contexte du traitement des données.

[1404] B. PY, « Le secret professionnel : le syndrôme des assignats ? », *AJ pénal* 2004, p. 133.

§ 1 - Une condition d'efficacité du traitement des données

308. L'angle sous lequel nous abordons ce développement ne peut se départir d'une réflexion sur l'aspect politique et économique de la loi informatique et libertés et notamment sur la logique de compromis qui la sous-tend **(A)**. Tandis que le secret professionnel est également soumis à une logique de compromis **(B)**.

A - Les enjeux des traitements de données Etatiques

309. La logique de compromis qui est à l'œuvre est inscrite dans les gènes de la loi informatique et libertés. Créée comme un rempart contre la surveillance des populations elle avait vocation à réguler les tendances de l'Etat et des personnes publiques à faire primer l'intérêt public sur les droits fondamentaux des personnes. Les traitements de données à caractère personnel sont en effet apparus comme des instruments essentiels de l'Etat **(1)** dès lors qu'ils sont mis au service de l'intérêt général **(2)**.

1 - Le traitement des données à caractère personnel instrument de l'Etat

310. La recherche d'équilibre qui est au centre de la loi informatique et libertés et de la régulation du traitement des données à caractère personnel peut s'expliquer au regard des enjeux de pouvoir décrit par certains auteurs **(a)**. Bien que le point de vue de certains de ces auteurs soit parfois clairement engagé, leurs propos doivent faire l'objet d'une brève synthèse en ce qu'ils éclairent l'équilibre qui a présidé à l'élaboration de la loi informatique et libertés **(b)**.

a - Les informations, l'informatique et le pouvoir

311. Le traitement des informations relatives aux personnes : fichage et surveillance des populations. Le fichage des individus n'est pas né avec l'informatique[1405], les techniques dites *d'identification* sont anciennes et remontent, pour certaines, au Moyen-âge[1406]. Les registres

---

[1405] V. GAUTRON, « Usages et mésusages des fichiers de police : la sécurité contre la sûreté », *AJ pénal*, 2010, p. 266.

[1406] On peut par exemple mentionner le « billet de santé », créé à l'occasion des épisodes de pestes que l'Europe connut entre le XVI^e^ et le XVII^e^ siècle. Il s'agissait d'un document dont la présentation était exigée des étrangers qui voulaient entrer dans le Royaume de France et permettait de garantir l'innocuité de la personne qui en était porteuse (Pour une étude historique sur l'identification des individus en France v. V. DENIS, *Une histoire de*

permettent par la suite à l'Eglise comme à l'Etat d'organiser « *la conservation structurée d'informations* »[1407] relatives aux personnes. Le savoir de l'Etat s'est en effet construit sur la connaissance des individus[1408] : « *L'identification est aussi un processus de connaissance construit par et pour l'Etat : sa maîtrise, qui permet de mobiliser et localiser les hommes dont il souhaite contrôler les mouvements sur son territoire, mais aussi de classer les populations et plus généralement d'agir, représente un enjeu considérable pour l'édification de l'Etat moderne* »[1409]. Le fichage des individus s'est ensuite généralisé, le domaine sécuritaire était[1410], et est toujours[1411], le terrain privilégié de l'usage des fichiers[1412]. Que le fichage serve à « surveiller et punir »[1413] ou à connaître pour décider ou gérer[1414], il s'agit toujours d'affirmer un pouvoir. L'on renverra sur ces points à l'éclairante étude d'ensemble relative aux fonctions

---

l'identité. France 1715-1815, coll. Epoques, Champ Vallon, 2008 ; I. ABOUT, V. DENIS, *Histoire de l'identification des personnes,* coll. Repères-Histoire, La Découverte, 2010).

[1407] C'est ainsi que l'on peut définir le fichier au sens commun : F. EDDAZI, « Prolégomènes », *in Le fichier*, Actes du colloque organisé les 26 et 27 novembre 2015 par le Centre de recherche juridique Pothier de l'Université d'Orléans, F. EDDAZI et S. MAUCLAIR (ss. la dir.), coll. Grands Colloques, LGDJ, 2017, p. 3.

[1408] « […] *un même fichier peut tout à la fois être un moyen de connaissance de la réalité sociale, servir au contrôle ou à la surveillance d'une frange de la population et être utilisé pour la fourniture de prestations* […] » (J. CHEVALLIER, « Les fichiers administratifs, instrument de l'action publique », *in Le fichier*, *op. cit.*, p. 125 et svt).

[1409] *Ibid.* p. 446.

[1410] Le fichier central de la police des étrangers créé en 1935 comptera 7 000 000 de fiches en 1939 (I. ABOUT, « Identifier les étrangers dans la France de l'entre-deux-guerres », *in* G. NOIRIEL, *L'identification, Genèse d'un travail d'Etat*, Belin, 2007, p. 152 ; Les écrits d'E. LOCARD, père de la police scientifique, sur la mise en fiche des individus invite aussi à envisager l'interconnexion des fichiers dans un but prédictif et cela dès le début du XXe siècle. L'efficacité de l'outil technique que sont les fichiers papiers sert déjà l'idée de performance et de sécurité (E. LOCARD, *La police ce qu'elle est, ce qu'elle devrait être*, Payot, 1919, spéc. p. 161 et svt).

[1411] On peut citer les fichiers les plus connus que sont le FAED (fichier automatisé des empreintes digitales), le FNAEG (le fichier national automatisé des empreintes génétiques), le FPR (fichier des personnes recherchées) ou encore le fichier des personnes radicalisées ; au niveau international les fichiers d'Interpol que sont l'ICIS (Interpol criminal information system), l'AFIS (base de données des empreintes digitales), DNA (base des profils génétiques), le SLTD (fichier des documents de voyage volés ou perdus), le SMV (fichier des véhicules volés). Les fichiers relatifs à la sécurité concernent aussi les détenus, puisqu'il existe un système automatisé de gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS).

[1412] Le terme de fichiers est issu de la loi informatique et libertés mais les dénominations sont variées, comme le souligne un auteur « *Elles ne peuvent permettre d'en repérer les objectifs, ni les activités qui y sont rattachées : catalogue, fichier, livre, liste, registre, répertoire, traitement de données ou encore recueil, index, voire référentiels ou barèmes, etc.* » on peut d'ailleurs y ajouter le terme de *dossier*s (G. KOUBI, « Fichier « et » service public » *in Le fichier*, *op. cit*, p. 151).

[1413] En référence à l'ouvrage de Michel Foucault (M. FOUCAULT, *Surveiller et punir*, coll. Tel, Gallimard, 1993).

[1414] V. *supra* n°158.

d'identification et de localisation des personnes physiques de la biométrie, réalisée par Monsieur Sztulman[1415].

312. Aspect historique du fichage et de la surveillance de l'état de santé des individus. Le domaine de la santé n'échappe pas à la pratique du fichage, mais elle nécessite des médecins la révélation d'informations que la déontologie – avant que la violation du secret professionnel ne soit pénalement sanctionnée – leur prescrit de garder secret. Parmi les premières informations qui font l'objet d'une conservation et d'un traitement relativement centralisé figurent celles concernant les maladies contagieuses. Dès le Moyen-âge, et suivant les épisodes épidémiques, il est demandé aux médecins de signaler certaines maladies[1416]. La déclaration obligatoire des malades contagieux (plus que de la maladie elle-même) sera parfois accompagnée de sanction à l'égard des médecins qui ne s'y soumettent pas[1417]. La surveillance sanitaire des populations n'est pas linéaire et la déclaration obligatoire des maladies sera finalement entérinée par une loi du 15 février 1902 relative à la santé publique[1418]. Outre la déclaration des maladies, d'autres informations recueillies par les professionnels de santé font l'objet de déclarations obligatoires et sont conservées au sein de registres : les décès sont des éléments de l'état civil mais constituent également des données essentielles pour les études démographiques et épidémiologiques dès lors que les causes de ceux-ci sont également conservées[1419]. On peut également citer, à la frontière entre le domaine sécuritaire et la santé,

---

[1415] M. SZTULMAN, *La biométrie saisie par le droit public*. *Etude sur l'identification et la localisation des personnes physiques*, coll. Bibliothèque de droit public, Préf. de X. BIOY, LGDJ, 2019.
[1416] R. VILLEY, *Histoire du secret médical*, coll. Médecine et Histoire, Seghers, 1986, p. 79.
[1417] R. VILLEY retrace quelques épisodes comme l'ordonnance du 6 septembre 1721 qui punissait *à peine de vie* les médecins, chirurgiens, apothicaires et autres personnes servant les malades qui omettraient de ne pas déclarer la découverte d'un malade contagieux aux maires, consuls et officiers municipaux. Il cite encore la déclaration obligatoire, accompagnée de peine sévère, de la variole, de la peste, du choléra, de la fièvre jaune et du typhus (*Ibid.*, p. 83).
[1418] *Ibid.* p. 85.
[1419] La déclaration des décès avant de devenir un outil de l'état civil des personnes était une façon pour les autorités publiques de dénombrer les morts durant les grandes épidémies de peste, ces recensements sont les premiers pas du contrôle de la santé des populations et de son outil de prédilection, la statistique qui va faire naître l'épidémiologie et la démographie : « *La peste a aussi indirectement contribué à la naissance de la statistique sanitaire. Non seulement elle a parfois motivé la tenue de recensements en prévision ou à la suite d'une épidémie, mais elle a surtout été l'occasion de renforcer l'intérêt pour un enregistrement systématique continu des décès par les services administratifs. Au départ, certes, cet enregistrement qui avait pour but de dénombrer les victimes de la peste se limitait à ces dernières et n'avait lieu qu'épisodiquement. Mais dès le XVIe siècle, à Londres, il a pris un tour systématique et permanent sous la forme des fameux* bills of mortality *à partir desquels John Graunt (1662) a pu établir ses célèbres observations, à l'origine de la naissance de la démographie et de l'épidémiologie* » (G. CASELLI, J. VALLIN et G. WUNCH, *Démographie : Histoire des idées et politiques de population*, t. VII, INED, 2006, p. 312).

les registres des certificats d'internement pour les psychopathes dangereux[1420]. Le contrôle de l'état de santé des individus va évoluer avec l'affermissement du rôle de l'Etat et la naissance de la santé publique[1421]. A partir des années 1970, l'Etat va s'engager dans un grand projet d'informatisation de l'administration et procéder à l'automatisation des systèmes et traitements d'informations malgré les réticences du parlement. Ce dernier avait en effet rejeté, en 1970, une proposition de loi relative à la création d'un fichier national de santé[1422]. Aussi, certains fichiers

---

[1420] Loi nº 7443 sur les aliénés du 30 juin 1838. La tentative de trouver dans les connaissances médicales des appuis pour prédire la dangerosité des individus est aussi constante que la question de la dangerosité et les rapports entre droit pénal, criminologie et politique criminelle en sont imprégnés : v. J. PRADEL, *Histoire des doctrines pénales*, coll. Que sais-je ?, PUF, 1991, p. 72 ; E. TILLET, « Histoire des doctrines pénales », *Rep. pén. Dalloz,* juin 2002 (act. oct. 2010) ; J. DANET, « La dangerosité, une notion criminologique, séculaire et mutante », Champ pénal, Vol. V, 2008, *varia*. La psychiatrie tient une place particulière dans la prédiction de la dangerosité et plus encore dans son approche la plus inquiétante pour la société, la récidive. Aussi, la tentation de ficher les malades mentaux est une constante dans l'histoire et Michel FOUCAULT l'avait, le premier, mis en exergue (M. FOUCAULT, *Surveiller et punir*, coll. Tel, Gallimard, 1993).

[1421] La santé publique recouvre trois dimensions, synthétisées par A. MORELLO et D. TABUTEAU en ces termes : « *la santé publique est d'abord un objectif politique : préserver et améliorer l'état de santé d'une population donnée vivant sur un territoire donné. Elle représente même une visée ultime pour l'État, ce que la Rome antique avait proclamé d'un lapidaire :* salus populi suprema lex*. La santé publique est une fin ;*
– la santé publique est aussi une politique publique, c'est-à-dire l'application d'un ensemble cohérent et articulé de mesures, d'une législation et d'une réglementation, politique mise en œuvre par un dispositif institutionnel, administratif pour l'essentiel, mais aussi associatif ou libéral. La santé publique est un moyen ;
– la santé publique est enfin une démarche intellectuelle, marquée par la multidisciplinarité, mais où l'épidémiologie tient une place fondatrice et centrale. La santé publique est un mode de raisonnement ». (A. MORELLO et D. TABUTEAU, *La santé* publique, coll. Que sais-je ?, PUF, 2017, p. 6). Au travers de ces différentes dimensions de la santé publique, l'on perçoit l'importance, pour les pouvoirs publics, de disposer d'informations fiables, stabilisées et précises sur les individus. Le « biopouvoir » théorisé par Michel FOUCAULT (*Ibid.*) ne peut se maintenir que si le pouvoir central détient les informations nécessaires à la réalisation de ses objectifs politiques par la mise en œuvre de politiques publiques dont la légitimité trouve appui dans une démarche intellectuelle. Par ailleurs, l'information source de pouvoir est aussi un mode de légitimation de l'action publique. M. RONAI développe ainsi ce lien « *L'information a, de tout temps, été une affaire d'Etat, mais elle relevait classiquement de l'intendance. La construction de l'Etat moderne (Etat de justice, Etat de finance, Etat de police) s'est traduite par le lancement et l'entretien de « grands travaux informationnels », visant à améliorer la connaissance du pays, et non plus seulement à dénombrer les hommes et les ressources pour gérer les populations, lever l'impôt ou assurer les recrutements de l'armée. Depuis le XVIII^e^ siècle, la connaissance et la surveillance de la production de richesses et des populations (statistiques), du territoire (cartographie), des comportements des personnes, citoyens et étrangers (police), de l'état de santé des populations (médecine d'Etat, santé publique, épidémiologie), de l'environnement et des menaces internationales (diplomatie et services de renseignement) ont mobilisé des moyens de croissants. L'émergence de l'Etat-providence, puis son expansion vers la régulation de l'économie (l'Etat keynésien) se sont traduites par une extension de la sphère informationnelle publique et une augmentation des* « impôts informationnels *» tant auprès des personnes qu'auprès des entreprises (enquêtes et questionnaires obligatoires, procédures de* « publicité légale » » (M. RONAI, « L'Etat comme machine informationnelle », *in Les données publiques, RFDP*, oct.-déc. 1994, n° 72, p. 571). Sur l'information comme mode de légitimation l'action publique v. V. LASSERRE, *Le nouvel ordre juridique. Le droit de la gouvernance*, LexisNexis, 2015, n° 76 et svt).

[1422] La CNIL, dans son rapport d'activité de l'année 1992, explique notamment que si la création d'un fichier national de santé est rejetée par le parlement : « *Trop souvent, lors de la conception des systèmes, les arguments de gestion et de lutte contre la fraude qui penchent en général, en faveur de la centralisation, ne sont pas*

seront créés sans consultation du parlement. La prise de conscience de l'importance d'une législation sur l'informatique et les libertés interviendra à l'occasion de la création de deux fichiers, les informations relatives à la santé des personnes devant être mises au service d'un contrôle de l'Etat dans les deux cas. D'abord, le fichier GAMIN (Gestion automatisée de médecine infantile), auquel se sont fermement opposés les professionnels de santé et les travailleurs sociaux. Ce fichier devait créer des profils de normalité ou d'anormalité pour les nouveau-nés à partir du croisement d'informations sanitaires et sociales et sur la base de probabilités statistiques[1423]. La contestation s'est étendue à l'ensemble de la société civile lorsqu'a été révélé dans la presse[1424] le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus). Il s'agissait de faire du numéro de sécurité social[1425], qui permettait d'identifier l'ensemble des citoyens français, un identifiant unique. Cette identification unique des individus par les différentes administrations et les entreprises devait ensuite permettre l'interconnexion des fichiers notamment médicaux, sociaux, professionnels, bancaires, etc. Le secret entourant ce fichier met en lumière la façon dont les enjeux politiques de l'informatique ont été passés sous silence.

313. De la société disciplinaire à la société de contrôle. L'évolution vers un Etat de plus en plus sécuritaire sur fond de « *crise démocratique* » durant la décennie 1970[1426] va inciter les Etats à utiliser les technologies de l'information et de la communication, non seulement pour surveiller – bien qu'elles puissent aussi servir à surveiller en lieu clos – mais aussi pour contrôler les individus. L'informatique est alors un outil de la société de contrôle décrite par Gilles Deleuze, société dans laquelle le contrôle est assuré par la mesure de toute chose[1427].

---

suffisamment contrebalancés par la prise en compte d'autres considérations, notamment les droits de la personne et le respect de son intimité » (CNIL, 13e rapport d'activité, 1992, La documentation française, p. 92, disponible en ligne <https://www.cnil.fr/sites/default/files/atoms/files/20171116_rapport_annuel_cnil_-_rapport_dactivite_1992_vd.pdf> dernière consultation le 17/09/2018).

[1423] « *C'est à partir d'une loi de juillet 1970 qui rendait obligatoire la collecte d'informations sur les nouveau-nés, afin de dépister les handicaps, qu'a été construit progressivement dans le plus grand secret, sur la base de simples circulaires, un énorme système de tri, totalement ignoré des familles. Les capacités de la machine étaient utilisées pour cibler et discriminer une population devant faire l'objet d'un traitement et d'une surveillance particulière* » (A. MATTELART et A. VITALIS, *Le profilage des populations. Du livret ouvrier au cybercontrôle,* La Découverte, Paris, 2014, p. 118).

[1424] P. BOUCHER, « Safari ou la chasse aux français », *Le Monde*, 21 mars 1974, p. 9.

[1425] Il s'agit de sa dénomination commune, ce numéro est en fait le *numéro d'inscription au répertoire* (NIR) attribué par l'INSEE aux individus dès leur naissance.

[1426] Pour une synthèse de l'évolution du fichage des populations dans la seconde moitié du XXe siècle et de son emballement à partir des années 1970, v. A. MATTELARD et A. VITALIS, *Le profilage des populations. Du livret ouvrier au cybercontrôle*, *op. cit,* p. 101 à 111.

[1427] G. DELEUZE, « Post-scriptum sur les sociétés de contrôle » *in* G. DELEUZE, *Pourparlers 1972-1990*, Éditions de Minuit, 1990, p. 244.

L'utilisation de l'informatique dans le traitement des informations sur les personnes est ainsi résumée par deux auteurs, dont il nous semble utile de reproduire la synthèse *in extenso* : « *Au début des années 1970, les capacités de stockage et de traitement de l'ordinateur vont apporter une puissance inconnue jusqu'alors. Dix ans plus tôt était apparue aux Etats-Unis la notion de système d'information qui marque l'importance réformatrice attribuée à une modification en profondeur du recueil et du traitement des données. L'implantation de ces systèmes dans les administrations doit permettre de gouverner plus rationnellement. Il s'agit de maîtriser l'abondance d'informations, de rassembler ce qui est épars, d'en assurer un traitement systématique, de perméabiliser les frontières, de créer des banques de données. Toutes ces applications aboutiront, en ce qui concerne l'information sur les personnes, à une véritable révolution du contrôle. L'ordinateur apporte des capacités de stockage presque illimitées, confirmées ultérieurement par la baisse vertigineuse des coûts et la miniaturisation des composants. L'informatisation des fichiers se traduit dans la plupart des cas par la collecte d'un supplément d'informations. La centralisation de ces informations dans de vastes fichiers est effectuée avec la plus grande facilité.* […] *Ce sont les capacités de traitement de la machine qui constituent cependant l'innovation la plus décisive. L'interconnexion entre les fichiers jusqu'alors séparés aboutit à une transparence totale de l'individu, qui devra vivre dorénavant avec un double informatique à partir duquel de nombreuses décisions seront prises sur lui. L'établissement de profils montre que l'on peut fabriquer des informations nouvelles à partir des informations rassemblées. Les profils et les segmentations comportementales réalisés seront de précieux outils pour prévenir et gérer les risques sociaux en attribuant aux individus des identités préfabriquées au moyen de calculs statistiques »*[1428]. L'informatique par les transformations du temps et de l'espace qu'elle induit est un outil essentiel de la société de

[1428] A. MATTELARD et A. VITALIS, *Le profilage des populations. Du livret ouvrier au cybercontrôle*, *op. cit.*, p. 112-113.

contrôle[1429], et l'on conçoit que sa maîtrise constitue un enjeu de pouvoir, en ce que son usage permet notamment de gouverner par les données[1430].

314. L'évolution de la loi informatique et liberté : convergence et démocratisation des techniques informatiques, liberté de circulation des flux de données. La loi informatique et liberté a évolué à la suite d'une modification d'ampleur : la loi du 6 août 2004[1431], marquée par l'empreinte de l'Union européenne puisqu'il s'agissait, entre autres, de transposer une directive européenne du 24 octobre 1995[1432]. Les transformations qui en résultent s'expliquent par trois facteurs sociaux et techniques qui modifient les équilibres précédemment évoqués. La première de ces causes consiste dans la démocratisation de l'informatique. Alors que la première mouture de la loi informatique et liberté arbitrait entre les velléités liberticides de l'Etat qui userait sans frein des dispositifs techniques, et la nécessité de saisir les opportunités de l'informatique, c'est en raison du passage « *à la micro-informatique privée et démocratisée* »[1433] que le champ

---

[1429] Dans une perspective de comparaison entre le système de surveillance théorisé par Michel Foucault et la société de contrôle décrite par Gilles Deleuze, des auteurs proposent une analyse comparative des caractéristiques du système disciplinaire et de la société de contrôle. Ils notent que la théorie foucaldienne s'appuie sur une analyse de l'espace caractérisée par l'enfermement, l'immobilité, la fixité de l'espace, l'espace limité et le confinement physique tandis que la théorie deleuzienne envisage l'espace en termes de désenfermement, de mouvement, de liberté et surtout de contrôle continu à travers une communication instantanée. S'agissant du temps, le premier auteur évoque un temps court, tandis que le second caractérise la société de contrôle dans un temps continu, réel et intrusif. Comme l'observe ces auteurs : « *L'approche deleuzienne offre une relecture des systèmes de contrôle, intégrant davantage les usages des technologies modernes et les nouveaux espaces-temps dans lesquels elles opèrent. Cette perspective semble à même d'appréhender les nouveaux dispositifs de contrôle basés sur l'utilisation de TIC ubiquitaires, qui se sont généralisées dans les organisations et la société au cours des deux dernières décennies. Cette perspective permet en effet une prise en considération de l'évolution des temporalités et des espaces d'exercice du contrôle, du rôle de la subjectivité individuelle et des nouvelles modalités du contrôle* » (A. LECLERCQ-VANDELANOITTE et H. ISSAC, « Technologies de l'information, contrôle et panoptique : Pour une approche deleuzienne », *Système d'information et management* 2013/2, vol. 18, n° 18).

[1430] Sur ce point v. nos développements relatif à la concurrence des normes *infra* n° Titre II Partie II. Pour une étude sectorielle, sur le méga-fichier Cassiopée v. B. FERY, *Gouverner par les données ? : Pour une analyse des processus de traduction dans l'usage des systèmes d'information : Déploiement et utilisations de Cassiopée dans l'Institution pénale*, thèse de doctorat en sciences politiques, ss. la dir. de J. DE MAILLARD, soutenue le 28 sept. 2015,Université de Versailles-Saint-Quentin-en-Yvelines.

[1431] LOI n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* n°182 du 7 août 2004, p. 14063.

[1432] La directive 95/46 CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[1433] A. TURK, *Rapport fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'assemblée nationale, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,* p. 21.

d'application de la loi a été élargi. Par ailleurs, la « *convergence technologique* »[1434] a imposé le changement de vocable de « *l'information nominative* » vers « *les données à caractère personnel* »[1435]. Enfin, il s'agissait d'assurer que les législations internes des Etats européens ayant mis en place un dispositif protecteur des individus ne constituent pas un frein exagéré à la libre circulation des flux de données. En somme, tandis que les législations de nombreux pays occidentaux entendent trouver un compromis entre les droits et libertés des personnes et les opportunités de l'informatique[1436], « *les droits international et européen font de cette protection la contrepartie du principe de libre circulation de l'information* »[1437].

b - Entre progrès technique et protection des droits et libertés

315. Les enjeux du traitement des données personnelles. Si la représentation de l'information sur un support numérique nécessite d'interroger le statut de l'information en droit privé au travers de la dualité matériel/immatériel[1438] et mérite un exercice d'articulation entre les normes juridiques, l'on comprend, au travers des évolutions qui viennent d'être retracées, que le traitement de l'information entretient des liens étroits avec les notions de pouvoir, de liberté, de contrôle[1439]. Les enjeux sont éminemment politiques, mais également économiques. Au travers de ses recherches en sciences politiques, Monsieur Vitalis a proposé une analyse de ces rapports. Ses ouvrages abordent les enjeux socio-politiques et économiques du traitement

---

[1434] *Ibid.* p. 21-22. La convergence technologique est un terme employé pour la première fois dans un rapport de la National Science Fondation (National Science Fondation, *Converging Technologies for Improving Human Performance nanotechnology, biotechnology, information technology and cognitive science*, Springer, 2003), il décrit les rapprochements entre plusieurs disciplines scientifiques et notamment les nanotechnologies, la biotechnologie, l'informatique et les sciences cognitives mais également entre la physique et les théories de l'informatique permettant d'opérer « *des calculs au niveau atomique, et créer des espaces de mémoire à cette échelle* » (T. BERTHIER, « Convergence technologique : l'homme, la machine et la société », *The Conversation*, 28 mai 2017).

[1435] V. *supra* n° 141-142.

[1436] C'est du moins le discours dominant sur cette question ; v. *contra* Monsieur Ochoa, qui estime que la loi informatique et libertés est en réalité la première qui reconnaît une liberté de traiter les données à caractère personnel (N. OCHOA, *Le droit des donnees personnelles, une police administrative speciale*, Th. dact., ss. la dir. de C. TEITGEN-COLLY, soutenue le 8 déc. 2014, Université Paris I-Panthéon-Sorbonne).

[1437] A. TURK, rapport préc., p. 23.

[1438] V. *supra* n° 63.

[1439] A. MATTELART et A. VITALIS, *Le profilage des populations. Du livret ouvrier au cybercontrôle*, La Découverte, 2014 ; Sur le fichage manuel v. M. FOUCAULT, *Surveiller et punir*, Gallimard, 1975, p. 287.

automatisé de l'information[1440] puis des données[1441] et précisent ainsi les l'évolution des équilibres. De cette étude, notamment inspirée des travaux de Jaques Ellul[1442] et de Lewis Mumford[1443] sur la technique, il nous semble utile de retenir un élément essentiel pour la suite de nos développements. L'axiome[1444] sur lequel ces réflexions sur la technique sont menées et qu'il importe de garder à l'esprit lorsqu'on évoque les rapports entre technologies numériques, pouvoirs et libertés[1445] est le suivant : la technique n'est pas dénuée de valeur, elle est toujours pensée en termes d'efficacité[1446]. L'auteur affirme ainsi que « *Dans des sociétés techniciennes où ce qui importe avant tout est le choix des moyens les plus efficaces, la technique n'est plus dépendante des choix politiques et du libre arbitre de l'utilisateur* »[1447]. La technique acquiert une forme d'autonomie et si la finalité assignée, par l'homme, aux dispositifs techniques de l'information et de la communication consiste dans la libération de la société[1448], elle n'est

---

[1440] A. VITALIS, *Informatique, Pouvoir et Libertés*, 2e éd., coll. Politiques comparée, Economica, 1988 ; A. MATTELART et A. VITALIS, *Le profilage des populations. Du livret ouvrier au cybercontrôle*, *op. cit.*

[1441] A. VITALIS, *L'incertaine révolution numérique*, coll. Systèmes d'information, web et société, Série informatique et société connectées, vol. 1, ISTE éditions, 2016.

[1442] J. ELLUL, *La technique ou l'enjeu du siècle,* coll. classiques de sciences sociales, Economica, 2004 ; *Le système technicien*, Le cherche midi, 2012 ; *Le bluff technologique*, Pluriel, 1988.

[1443] L. MUMFORD, *Technique et civilisation*, coll. eupalinos, Parenthèses, 2016 ; « Technique autoritaire et technique démocratique », *in Technology and Culture*, John Hopkins University Press, 1963.

[1444] « *Énoncé admis comme base ou principe d'une construction scientifique* » v° « Axiome », TLFi, *op. cit.*

[1445] A. VITALIS, *L'incertaine révolution numérique*, *op. cit.*

[1446] L'efficacité est la qualité de ce qui est efficace, c'est-à-dire ce qui produit l'effet attendu. Pris en ce sens la technique répond à un but qui lui est extérieur.

[1447] *Ibid.*, p. 104 ; en ce sens mais du point de vue d'un linguiste révélant cette fois les enjeux culturels mais parvenant au même constat : « *En adoptant la perspective mcluhanienne du déterminisme technologique, les stratégies et les discours* […] *tendent donc à éviter toute réflexion sur le culturel, la médiation et le symbolique au profit de la seule efficacité technique* » (I. BABOU, « Des discours d'accompagnement aux langages : les nouveaux médias », *Études de linguistique appliquée*, 114, 1998, pp. 407-420). Sur les discours d'accompagnement v. *introduction*¤.

[1448] Alain Supiot exprime cette idée au travers de l'exemple de la déshumanisation du travail mais celle-ci a une portée générale s'agissant de l'efficacité, de l'esprit de *performance* dont sont imprégnées les techniques de l'information et de la communication : « [...] *les nouvelles technologies de l'information peuvent être un formidable instrument de libération de l'Homme lorsqu'elles lui permettent de concentrer les forces de son esprit sur la part la plus créative de son travail, c'est-à-dire la plus poétique au sens premier du terme. Nos nouveaux outils informatiques pourraient donc être une chance d'arracher le travail à l'abrutissement où l'avait plongé le taylorisme. Mais ces possibilités sont ignorées dès lors qu'on pense le travailleur sur le modèle de l'ordinateur au lieu de penser l'ordinateur comme un moyen d'humaniser le travail. Astreint à une réactivité en « temps réel », absorbé dans une représentation virtuelle du monde et évalué à l'aune d'indicateurs de performance sans rapport avec les conditions de son exécution, le travail n'est plus ce monde essentiel d'inscription de l'être humain dans la réalité du monde, qui permet d'avoir et garder raison. Il l'enferme au contraire dans un système de signifiants sans signifiés qui exige de lui une augmentation indéfinie de ses* « performances » […] » (A. SUPIOT, *La gouvernance par les nombres*, *Cours au collège de France (2012-2014)*, coll. poids et mesures du monde, Fayard, p. 257). Cette libération est aussi celle qui traverse l'idée (voire l'utopie) du *village global* qu'est internet (M. McLUHAN, *Pour comprendre les médias*, coll. points, Seuil, 1968) et de la société de la connaissance qui se révèle plutôt être société de l'information (signifiant sans signifiés). Elle trouve également un écho dans le rapport de S. NORA et A. MINC sur l'informatisation de la société, lesquels voient dans l'informatique un moyen

jamais acquise et l'utilisation des dispositifs crée des problèmes appelant une intervention des pouvoirs publics[1449]. C'est du moins la pensée dominante, critiquée par Monsieur Ochoa dans sa thèse de doctorat. L'auteur explique que l'opposition entre danger du traitement des données personnelles et protection des personnes a donné lieu à une vision mythologique de la loi informatique et liberté. L'auteur affirme : « *Une telle conception encourt légitimement le qualificatif de mythologique en ce qu'elle s'apparente plus au sens sociologique du terme à un récit sacré de l'origine du monde qu'à une description de la réalité historique factuelle.* [...] *cette mythologie conduit à une survalorisation du rôle de l'Etat en tant que défenseur des droits de l'Homme et des libertés qui tend à occulter l'intégralité des enjeux en présence* »[1450]. Au sujet de ces enjeux l'auteur critique la « *cécité partielle* » qui a saisi les commentateurs de la loi informatique et libertés. Il vise notamment la maladresse de l'article premier de la loi disposant que l'informatique doit être mise au service des citoyens, qui, selon lui, a pour conséquence de « *mettre l'accent sur la fonction de protection des droits et libertés de la personne fichée et, ce faisant, de méconnaître l'objectif premier de cette loi : le développement de l'informatique* »[1451]. Selon cet auteur, la vision d'un Etat protecteur des individus face aux potentialités du traitement des données à caractère personnel relève de l'angélisme[1452], les enjeux de pouvoir tant sur le plan interne qu'international amènent à relativiser les discours et analyses consistant à *ranger* la loi informatique et libertés parmis les textes protégeant la personnalité[1453].

316. L'informatique maîtrisée, le creuset du déterminisme. Les choix politiques vont s'orienter vers une *maîtrise de la maîtrise*[1454]. Le projet de loi rapporté par Jean Foyer présentait

---

« *d'accroître l'adaptabilité, la liberté, la communication, de telle sorte que chaque citoyen, chaque groupe se prennent en charge de façon plus responsable* » (S. NORA et A. MINC, *Rapport au président de la République – L'informatisation de la société*, La documentation française, 1978 – *Adde* A. MATTELARD et A. VITALIS, *Le profilage des population, du livret ouvrier au cybercontrôle*, La Découverte, 2014, p. 105).

[1449] A. VITALIS, *L'incertaine révolution numérique*, *op. cit.*, p. 135.

[1450] N. OCHOA, *Le droit des données personnelles, une police administrative spéciale*, Thèse de droit public, ss. la dir. de C. TEITGEN-COLLY, soutenue le 8 décembre 2014, Universite Paris I - Pantheon-Sorbonne, p. 32.

[1451] *Ibid*., p. 33.

[1452] *Ibid.*

[1453] Comme c'est notamment le cas dans J.-C. SAINT-PAU, *Traité de droit de la personnalité*, coll. Traités, LexisNexis, 2013.

[1454] La formule exacte : « *La question maintenant est de maîtriser la maîtrise et non plus la nature* » (M. SERRES, *Hermès III, la traduction*, Ed. de Minuit, 1974, p. 93). La pensée de Michel Serres fait écho, selon nous, à la position du législateur. Le traitement mathématique des données et l'internet qui constituent le noyau technique

la conciliation entre progrès technique et protection des personnes[1455]. A sa suite, le rapport élaboré par Alain Minc et Simon Nora au sujet de l'informatisation de la société[1456] est un point de départ important pour comprendre la façon dont sera assurée cette *maîtrise*. Les auteurs, comparant l'électricité à la télématique[1457] comme moyens de communication, expliquent que « *la télématique, à la différence de l'électricité ne véhiculera pas un courant inerte, mais de l'information, c'est-à-dire du pouvoir* »[1458]. L'idée qui veut que, par la loi informatique et libertés la société serait en mesure de maîtriser la technique, consiste à nier le déterminisme technique. Cette orientation politique permet d'intégrer le traitement des données à l'intérêt général. Puisque la technique est maîtrisée, elle pourrait donc être mise au service de cet intérêt, dans le respect des droits et libertés des personnes. De plus, la valeur efficacité, inhérente à la technique, fait de cette dernière un outil privilégié de l'administration et de l'action publique.

317. Les dispositifs de l'information et de la communication, des outils de l'action publique. Comme l'explique Monsieur Chevallier, les fichiers sont des instruments de l'action publique, des « *dispositifs techniques embarqués dans les politiques publiques* »[1459]. Selon certains auteurs « *les nouvelles technologies constituent un puissant outil bureaucratique et technocratique devenu essentiel pour la rationalisation de la gestion publique, l'action de la*

---

des dispositifs de l'information et de la communication sont ce que l'auteur nomme des « objets-monde » : « *Appelons objets-monde,* […]*, la bombe atomique, les résidus nucléaires ou la Toile elle-même, parce que l'une de leurs dimensions physiques, énergie, temps ou espace, accède à l'échelle de l'une des dimensions du monde* […]*. Lorsque ces objets-monde quittent le statut strict d'outils ou de machines propres au travail sur les choses, pour devenir des quasi-objets, comme les médias en général, ils se transforment en machines à société* » (M. SERRES, *Retour au contrat naturel*, coll. Conférences et Etudes, BNF, 2000, p. 12) « *des outils dont l'une des dimensions est commensurable à l'une des dimensions du monde. Un satellite, pour la vitesse, une bombe atomique, pour l'énergie, l'Internet, pour l'espace, les résidus nucléaires pour le temps... voilà quatre exemples d'objets-monde* » (*Ibid.*). Seule la volonté des Hommes peut alors nous permettre de prendre nos responsabilités face aux objets que nous créons et qui transforme l'echelle de la réalité : « *nous dépendons nous-mêmes désormais de choses qui dépendent des actes que nous entreprenons. Notre survie dépend du monde que nous créons au moyen de techniques dont les éléments dépendent de nos décisions* » (*Ibid.* p. 14).

[1455] A propos du projet de loi sur l'informatique et les libertés : « *La considération fondamentale qui l'inspire est uq'on ne peut interdire purement et simplement l'usages procédés informatiques.* […] *Mais cette technique ne doit pas progresser plus vite que son contrôle et il convient, avant tout, d'éviter qu'il ne soit fait un usage abusif et préjudiciable aux droit inviduels* » (J. FOYER, *Informatique et libertés*, Rapport n° 3125 de l'Assemblée nationale, session ordinaire de 1977-1978, Tome 1, p. 13).

[1456] S. NORA et A. MINC, *Rapport au Président de la République – L'informatisation de la société*, La documentation française, 1978.

[1457] Ce que nous nommons aujourd'hui technologies de l'information et de la communication en ce qu'il s'agit de l'usage combiné de l'informatique et des télécommunications v. *supra* n° 8.

[1458] S. NORA et A. MINC, *Rapport au Président de la République – L'informatisation de la société*, *op. cit.*, p. 60.

[1459] J. CHEVALLIER, « Les fichiers administratifs instruments de l'action publique », *in* F. EDDAZI et S. MAUCLAIR (dir.), *Le fichier*, Actes du colloque organisé les 26 et 27 novembre 2015 par le Centre de recherche juridique Pothier de l'Université d'Orléans, coll. Grands Colloques, LGDJ, p. 125, spéc. p. 126.

police et de la justice, la conduite des politiques publiques (santé, emploi, aides publiques...), la lutte contre les fraudes, la prévision. Pratiquement toutes les relations administration-administré passent par un fichage »[1460]. Pour d'autres encore, les fichiers, et plus largement le traitement de l'information, seraient consubstantiels à l'Etat moderne[1461]. Les travaux de Monsieur Chevallier en science administrative nous éclairent, non seulement sur l'intérêt pour l'administration de traiter l'information[1462], mais aussi sur celui que présentent les dispositifs de l'information et de la communication pour la mise en œuvre des politiques par l'administration. Celle-ci « *est chargée d'appliquer les politiques en mobilisant les moyens, juridiques, matériels et humains dont elle dispose* »[1463]. Cette mise en œuvre doit répondre à une contrainte d'*efficacité*[1464] et d'*efficience*[1465]. Au regard de cette seconde contrainte,

---

[1460] A. LUCAS, J. DEVEZE, J. FRAYSSINET, *Droit de l'informatique et de l'Internet*, PUF, 2001, p. 8.

[1461] « *Pour l'accomplissement de ses missions, de tout temps, l'administration a collecté, produit et utilisé de l'information ; l'information est consubstantielle au rôle que la collectivité publique a à jouer ; ce phénomène n'a cessé de s'accroître à tel point qu'on a pu qualifier l'État de « machine informationnelle* » (H. MAISL, *Le droit des données publiques*, LGDJ, 1996, p. 1) ; Dans le même sens, v. notamment N. OCHOA, *Le droit des données personnelles. Une police administrative spéciale*, *op. cit.*, p. 91 et s. : « […] *la pertinence du traitement de cette information conditionnant l'équilibre interne de l'institution, la rationalisation de cette fonction apparaît comme une condition de la survie même de toute institution. L'histoire des fichiers établis par la puissance publique en France en atteste : ces derniers n'apparaissent de manière systématique qu'au moment où l'État développe un savoir sur ses moyens dans le but d'accroître sa puissance sur ses rivaux. L'existence de tout phénomène institutionnel implique donc, d'un point de vue théorique et historique, l'existence d'un traitement rationnel de l'information personnelle* » (*Ibid.* spéc. p. 97)

[1462] « *l'administration se trouve, dans le schéma d'ouverture, reliée à l'environnement par un flux continu et circulaire d'informations et d'échanges : elle importe de l'environnement l'énergie et l'information nécessaires (input) qu'elle transforme (throughput) en décisions et en actions (output)* » (J. CHEVALLIER et D. LOCHAK, *Science administrative*, t. II, *L'administration comme organisation et système d'action*, LGDJ, 1978, p. 180).

[1463] J. CHEVALLIER, *Science administrative*, coll. Thémis Droit, 6e éd. mise à jour, PUF, 2019, p. 517.

[1464] Jacques Chevallier explique le problème que soulève l'efficacité pour l'application des politiques par l'administration : « *il s'agit que les objectifs fixés soient atteints ce qui suppose à la fois que les fonctionnaires, responsables de l'exécution, s'y conforment et qu'ils veillent à ce que les administrés, destinataires et cibles des politiques, adoptent le comportement voulu* » (J. CHEVALLIER, *Science administrative*, *op. cit.* p. 517). Reprenant notamment les travaux de Jacques Chevallier et Danièle Lochak, Nicolas Ochoa résume ainsi, plus largement, le rapport entre efficacité et adminstration : « *Cette recherche d'efficacité de l'action publique explique le délaissement d'une optique uniquement juridique pour y intégrer ou lui substituer des considérations relatives à la gestion et à la théorie des organisations. L'institution administrative est alors considérée comme une organisation au sens large, indépendamment de sa fonction de service de l'intérêt général. Or, dans la théorie des organisations, la question de l'efficacité d'une institution dépend de son adaptation à ses fins et à son environnement. Cette capacité d'adaptation est indissociablement liée à sa faculté d'acquérir et d'employer rationnellement l'information sur son environnement extérieur. L'enseignement qui en est tiré en science administrative est qu'une des causes de l'inefficacité supposée de l'administration publique à une certaine époque réside dans un processus congestionné d'acquisition et de circulation de l'information* » (N. OCHOA, *Le droit des données personnelles. Une police administrative spéciale*, *op. cit.*, p. 85-86).

[1465] L'efficience consistant, dans ce cadre précis, en ce « *que les objectifs soient atteints au moindre coût, avec une économie de moyens* » (J. CHEVALLIER, *Scence administrative*, *op. cit.*, p. 517).

Monsieur Chevallier explique que *« la recherche d'une plus grande efficience dans l'utilisation des ressources est le prolongement direct de la diffusion dans l'administration publique du mode de raisonnement managerial* »[1466] et d'ajouter ce qui a amené à une utilisation massive des dispositifs de l'information et de la communication. Résumant le mouvement du « tout numérique » vers « l'Etat-plateforme », il explique : « *La gestion administrative a connu une première transformation à partir des années 1960 avec l'introduction de l'informatique, qui eu toute une série d'applications :* […] *en matière de documentation et de statistiques, l'ordinateur à été utilisé pour l'enregistrement et le traitement de données qui sont la base ou le résultat du travail administratif (fichiers, informatique juridique…)* ; *enfin, l'informatique a apporté une aide pour l'accomplissement des tâches administratives, par la mobilisation rapide de l'information concernant les usagers (conducteurs, casier judiciaire, Sécurité sociale, etc.)* […] »[1467].

318. Le traitement des données, l'information sur les personnes mobilisée à tous les niveaux. En somme, nous pouvons affirmer que l'utilisation des dispositifs de l'information et de la communication est nécessaire tant au niveau de la définition des choix politiques internes et internationaux, car créant et véhiculant du pouvoir, qu'au niveau de la mise en œuvre de ces politiques au niveau interne puisqu'elle favorise, voire conditionne, l'efficience de l'action publique. Or, en France, l'Etat a « *la mission de poursuivre des fins qui s'imposent à l'ensemble des individus, par-delà leurs intérêts individuels* »[1468], ce qui correspond à la conception nationale de l'intérêt général[1469]. Il est nécessaire de développer davantage le rapport entre le traitement informatique des données à caractère personnel et l'intérêt général.

[1466] J. CHEVALLIER, *Science administrative*, *op. cit.*, p. 524. Nous avons évoqué le *New public management* lorsque nous avons défini les opérations de traitement, ce développement vient donc compléter nos propos précédents : v. *supra* n° 158.

[1467] *Ibid.*

[1468] D. BOURCIER, « Le bien commun, ou le nouvel intérêt général » *in Mélanges en l'honneur du professeur Jacque Chevallier – Penser la science administrative dans la post-modernité*, LGDJ, 2013, p. 92, spéc. p. 94.

[1469] L'intérêt général revêt, selon Monsieur Chevallier, deux sens. La première définition est fonctionnelle, la seconde conceptuelle. Dans la première acception, l'intérêt général est la « *finalité de l'institution et de l'action de l'Etat* », dans la seconde acception, il s'agit du « *principe de légitimation de l'Etat* » (J. CHEVALLIER, *in Dictionnaire critique et interdisciplinaire de la participation*, *V°* « intérêt général », disponible sur <http://www.participation-et-democratie.fr/es/print/1334>, dernière consultation le 12 avr. 2019). La conception française de l'intérêt général a longtemps été strictement volontariste, alors conçu « *comme un intérêt public, résultant du dépassement des intérêts particuliers tels qu'ils s'expriment sur le marché : expression de la volonté générale des citoyens, animés par le souci du bien public, il serait d'essence différente et l'État en serait le traducteur et le garant »* (J. CHEVALLIER, *« Réflexions sur l'idéologie de l'intérêt général* », *in Variations autour de l'idéologie de l'intérêt général*, PUF, coll. CURAP, 1978, vol. 1, p. 11). Dans un second sens, « *La*

2 - Le traitement des données à caractère personnel et l'intérêt général

319. Mutation de l'intérêt général. Comme l'explique Madame Bourcier, l'évaluation de l'intérêt général par le juge, et particulièrement le Conseil d'Etat, a eu pour conséquence de rendre la notion incertaine[1470]. L'auteur souligne que le changement consiste dans le fait que le juge « *passe du contrôle de l'application du concept législatif universaliste d'intérêt général à une analyse casuisitique fondée sur le modèle du bilan* « *coûts-avantages* » »[1471]. A cela s'ajoute encore la confrontation de cette conception à la conception utilitariste de l'intérêt général, qui prévaut dans l'Union européenne. A propos de celle-ci, l'auteur affirme : « *L'Etat-Janus n'arrive plus à définir l'intérêt général sans référence à des intérêts stratégiques liées aux grandes entreprises particulièrement en matière d'energie de télécommunications ou de banques* »[1472]. Au regard du bilan coût-avantage, le traitement informatique des informations constitue un outil essentiel car il se présente toujours comme le plus efficient, il est un outil d'optimisation et de rationalisation essentiel pour parvenir aux objectifs d'intérêt général[1473].

320. Le traitement informatique des données *dans* l'intérêt général. Depuis les premiers travaux parlementaires relatifs à l'informatisation et au traitement des données, il est affirmé que les craintes liberticides des individus à propos du fichage informatisé et de l'interconnexion sont largement fantasmées[1474]. En témoigne le rapport sur l'informatisation de la société, dans lequel les auteurs expliquent les bases du projet de la société de l'informatique au sein d'un

---

notion d'intérêt général se présente comme un principe fondamental de légitimation du pouvoir dans les sociétés modernes : tout pouvoir quel qu'il soit est en effet tenu d'apparaître comme porteur d'un intérêt qui dépasse et transcende les intérêts particuliers des membres ; cette représentation permet d'ancrer la croyance dans son bien-fondé et de créer le consensus indispensable à son exercice. Tout se passe comme si le pouvoir, dans les sociétés modernes, ne pouvait être pensé que recouvert du sceau de l'intérêt général : celui-ci constitue, non seulement l'un des attributs du pouvoir étatique, mais encore une référence nécessaire pour toutes les institutions qui quadrillent l'espace social ; l'intérêt général apparaît ainsi comme la matrice de tous les discours de légitimation des formes sociales instituées » (J. CHEVALLIER, *in Dictionnaire critique et interdisciplinaire de la participation*, *V°* « intérêt général », *op. cit.*).

[1470] D. BOURCIER, « Le bien commun, ou le nouvel intérêt général », art. préc., p. 95.

[1471] *Ibid*. p. 95, note n°6.

[1472] *Ibid.* p. 96.

[1473] J. CHEVALLIER, *Science administrative*, *op. cit.*, p. 524-525.

[1474] V. Mettant en balance les intérêts de l'interconnexion et le renforcement de la protection des données à caractère personnel : B. PLESSIX, « L'interconnexion des fichiers entre administrations », *in* N. DEFFAINS et B. PLESSIX (ss. la dir.), *Fichiers informatiques et sécurité publique*, coll. « droit, politique, société », PUF-EUL, 2013, pp. 109-124.

développement intitulé « *Liberté, efficacité* »[1475] : « *Le meilleur avenir est celui où la société accepte les avantages de l'informatique, son efficacité et ses simplifications, en opposant à ses éventuelles indiscrétions un climat imperturbablement démocratique* »[1476]. En réponse aux craintes nées du scandale des fichiers GAMIN et SAFARI, les pouvoirs publics proposent donc non pas une protection des individus mais une conciliation entre les intérêts. Cette conciliation fait écho aux théories développées en socio-politique et en philosophie des techniques précédemment évoquées : l'efficacité est la valeur de la technique. Le traitement informatique de l'information va en effet être mis au service de **l'intérêt général** tout en garantissant aux individus une protection de leurs libertés et des droits permettant leur exercice, objectifs affichés de la loi informatique et libertés[1477]. Or, l'intérêt général doit en principe émaner d'un choix de société[1478]. Le traitement des données, comme nous l'avons vu, a été, en quelque sorte, postulé par le législateur[1479]. Plus encore, les travaux préparatoires de la loi nous apprennent notamment que les dimensions internationale et économique ne sont pas ignorées du législateur, elles sont même extrêmement prégnantes[1480]. Un auteur explique d'ailleurs qu'en raison du poids économique des grandes entreprises informatiques, « *toute action d'intérêt général est l'action de l'Etat et des groupes industriels dominants* »[1481]. Il souligne encore que « *L'industrie*

[1475] S. NORA et A. MINC, *Rapport au Président de la République – L'informatisation de la société*, *op. cit.*, p. 60.
[1476] *Ibid.*
[1477] Sur ce compromis voir encore S. LACOUR, « Chapitre 3- Nouvelles technologies et patrimonialisation des données personnelles : un changement de paradigme », *in* F. VIOLET (dir.), *Personne et patrimoine en droit – Recherche sur les marqueurs d'une connexion*, Bruylant, 2015, p. 369 et svt.
[1478] « *Chaque grand choix technologique contient aussi un choix de société. Il devrait donc s'opérer au travers d'un choix démocratique et pas seulement être la simple acceptation du fait accompli scientifique ou technique* » (H. OBERDORFF, « Quelle intervention du droit ? » *in* CERCRID, *Le droit au contact de l'innovation technologique*, Université Jean Monnet-Saint Étienne, 1989, p. 13).
[1479]« *L'objet de ce texte était et demeure aujourd'hui celui de veiller à ce que l'informatique ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. A aucun moment au cours du processus législatif n'a été posée la question de l'opportunité de l'informatique* » (J. EYNARD, *Les données personnelles. Quelles définitions pour un régime de protection efficace ?*, Michalon, 2013, p. 10) ; v. également N. OCHOA, *Le droit des données personnelles, une police administrative spéciale*, *op. cit.*, spéc. pp. 79-82.
[1480] « *Afin d'éviter que le texte ne tourne à un procès de l'informatique et ne risque d'en freiner le développement, votre commission s'est, en particuler, attachée à la dimension internationale que l'utilisation de l'informatique introduit dans le traitement de l'information. Sur ce point elle a estimé que la loi ne devait pas être restrictive. Un excès de protection pourrait être en effet de nature à pénaliser notre pays tant au niveau de la fabrication que de l'utilisation des ordinateurs* » (J. THYRAUD, *Rapport au Sénat fait au nom de la commission des lois, sur le projet de loi relatif à l'informatique et aux libertés*, Première Session ordinaire 1977-1978, Annexe au procès verbal de la séance du 10 novembre 1977, n° 72, p. 18).
[1481] « *La domination que fait peser International Business Machines (I.B.M.) sur le marché informatique et sur les entreprises françaises, plus particulièrement (Compagnie des Machines Bull, Compagnie internationale pour l'informatique C.LI. puis C.I.I.-Honeywell-Bull) est écrasante. L'impériale I.B.M. impose sa loi, à savoir ses tarifs, ses innovations et ses matériels aux autres constructeurs comme aux utilisateurs* » (J.-L. LAVILLE, « Politique

française de l'informatique n'est pas un ensemble autonome fonctionnant dans le seul périmètre national, mais s'insère profondément dans les structures économiques et commerciales internationales »[1482]. L'idée selon laquelle l'informatique – et plus spécifiquement le traitement informatique de l'information et désormais des données en masse – porte l'intérêt général est diffusée dans la doctrine et le discours politique[1483].

321. Rationalisation et intérêt général dans le domaine de la santé. Il faut rappeler que l'informatique est définie comme la « *Science du traitement rationnel, notamment par machines automatiques, de l'information considérée comme le support des connaissances humaines et des communications dans les domaines technique, économique et social* »[1484]. La rationalité du traitement explique qu'il s'agisse d'un outil indispensable de l'action publique. Dans le domaine de la santé le traitement informatique des données a caractère personnel va servir la santé publique dans laquelle s'incarne l'intérêt général. Dans le rapport relatif à l'informatisation de la société et au traitement des données à caractère personnel, rédigé par Guy Braibant, il est fait mention de ce que le traitement des données à caractère personnel doit notamment permettre d'atteindre certains objectifs d'intérêt général[1485] tels que la protection de

---

de l'informatique et intérêt général », *in Variations autour de l'idéologie de l'intérêt général,* CURAPP, Volume 1, 1978, p. 209).

[1482] *Ibid.*

[1483] On peut encore citer Guy Braibant : « *le développement des fichiers informatiques permet, à maints égards, de renforcer l'efficacité de l'action publique au bénéfice direct des administrés* », de même qu'un développement est consacré au traitement des données personnelles dans l'intérêt général (G. BRAIBANT*, Données personnelles et société de l'information – Rapport au Premier ministre*, La Documentation française, Collection des rapports officiels, 1998, p. 4 et p. 15). Dans la doctrine, pour ne citer qu'un exemple, on peut par exemple lire que « *l'intérêt général de l'amélioration de la santé publique est porté par l'utilisation accrue des techniques dites du Big data* » (F. EON, « L'accélération du numérique en santé : enjeux et conditions de son succès », *RDSS* 2019, p. 55).

[1484] TLFi, *V°* « Informatique ».

[1485] Dans une analyse jurisprudentielle récente un auteur définit l'intérêt général comme « fonction-objet » d'une part et comme une « fonction-fin » d'autre part. (V. COQ, *Nouvelles recherches sur les fonctions de l'intérêt général dans la jurisprudence administrative*, préf. B. PLESSIX, coll. Logiques juridiques, L'Harmattan, 2015). Comme « fonction-objet », il peut être qualifié de standard, mais l'intérêt général n'est pas seulement un standard en ce qu'il a une essence ontologique et répond à des finalités politiques (« fonction-fins »), la notion est donc également idéologique. Ainsi, dans la jurisprudence administrative, l'intérêt général peut renvoyer à la « *protection de la santé publique* », il s'agit alors de l'une de ses « déterminations matérielles » (*Ibid.*, n° 2). Mais dans la mesure où l'intérêt général n'est pas un contenu mais désigne une catégorie, il reviendra au juge administratif de démontrer qu'un fait peut être considéré comme d'intérêt général (le qualifiant à cet égard de « *concept qualificateur* » *Ibid.*, n° 195 et svt). Cette qualification variera au regard des finalités de l'intérêt général, lesquelles sont conditionnées par la nature politique de l'intérêt général (*Ibid.*, Partie II, p. 293 à 567). Le Conseil constitutionnel a par ailleurs eu l'occasion de reconnaître une valeur constitutionnelle à ces composantes de l'intérêt général (G. MERLAND, « L'intérêt général, instrument efficace de protection des droits fondamentaux ? », *Cahiers du Conseil constitutionnel*, juin 2004, n° 16).

la santé publique[1486], et la maîtrise des dépenses de santé qui correspond à un autre objectif d'intérêt général : la garantie de l'équilibre financier de la sécurité sociale[1487]. Le rapport précise ainsi que « *les progrès des technologies de l'information permettent de franchir de véritables sauts qualitatifs, aussi bien dans la garantie des droits individuels à la santé que dans une démarche globale de santé publique* »[1488]. Sont successivement évoqués : la *« simplification de l'accès aux soins* », en facilitant « *l'échange de données sur un patient entre son médecin généraliste et les spécialistes ou l'hôpital* »[1489] ; « *la recherche scientifique* »[1490] ; les « *progrès considérables en matière épidémiologique, grâce à la mise en place de réseaux d'alerte et au suivi en temps réel de la prévalence des pathologies* »[1491] ; enfin « *Dans un contexte de contrainte financière, les dispositifs automatisés – comme ceux qui permettent d'asseoir la tarification hospitalière sur l'établissement de profils de patients (Programme Médicalisé des Systèmes d'Information) – garantissent une approche médicalisée de la maîtrise des dépenses de santé* »[1492]. Chacune de ces préoccupations participant soit à l'objectif de protection de la santé publique soit à la maitrise des dépenses de santé doit être précisée au regard des outils mis en œuvre pour les atteindre et au regard des données concernées.

322. Santé publique et traitement informatique des données couvertes par le secret. Le traitement des informations couvertes par le secret professionnel pour réduire les risques sanitaires n'est pas une préoccupation neuve[1493] mais ce traitement s'est accru avec les progrès de l'informatique et ses utilités se sont développées en raison de l'exigence croissante de performance du système de santé. **D'abord**, leur traitement participe à l'efficacité et à l'efficience du système de santé[1494] et l'on constate que du point de vue de l'économie et de la

---

[1486] G. BRAIBANT, *Données personnelles et société de l'information – Rapport au Premier ministre*, *op. cit.*, p. 4-5. S'agissant de la reconnaissance de la protection de la santé publique comme objectif d'intérêt général v. Cons. const., 8 janv. 1991, n° 90-283 DC, Rec. p. 11.
[1487] G. BRAIBANT, *Données personnelles et société de l'information*, *op. cit.*, p.4 ; Reconnu comme un objectif d'intérêt général par Cons. const., 18 déc. 1997, n° 97-393 DC, Rec. p. 320.
[1488] *Ibid.*
[1489] *Ibid.*
[1490] *Ibid.*
[1491] *Ibid.*
[1492] *Ibid.*
[1493] L'obligation de déclarer certaines maladies : Loi sur l'exercice de la médecine (*JORF* 1er déc. 1892) et Loi relative à la protection de la santé publique (*JORF* 19 févr. 1902).
[1494] En ce sens, Etude annuelle du Conseil d'Etat, *Numérique et droits fondamentaux*, Annexe 3, La doctumenation française, 2014, p. 367 ; mais surtout, bien que l'ouvrage n'ait pas été réedité et mis à jour : P.- L. BRAS, G. DE POURVILLE et D. TABUTEAU (ss. la dir.), *Traité d'économie et de gestion de la santé*, Ed. Presses de Sciences Po – Editions de santé, 2009. L'approche économique de cet ouvrage met notamment en exergue l'importance des

gestion, la performance du système de santé est évaluée au regard de critères qui rejoignent les droits reconnus aux malades : l'accès au soin et la qualité des soins[1495]. L'évaluation des politiques de santé vise directement à la performance du système de santé et se nourrit, entre autres informations[1496], de celles issues du parcours de santé des personnes. Monsieur Sauvé, lors de l'introduction des septièmes entretiens du Conseil d'Etat a rappelé ces objectifs d'intérêt général et a présenté ceux auxquels concourt également le traitement de ces données et qui répondent tous à l'objectif d'efficacité et d'efficience[1497]. **Ensuite,** ce traitement automatisé des données est devenu l'outil de prédilection pour mettre en œuvre les vigilances, et particulièrement la vigilance pharmaco-epidémiologique[1498], dans un objectif de qualité et de gestion des risques[1499]. **Enfin,** le traitement des données de santé favorise la recherche et la veille sanitaire[1500]. La Cour des comptes avait d'ailleurs souligné l'intérêt de développer

---

informations pour évaluer la performance du système de santé (O. ZYENEP, « Pourquoi et comment évaluer la performance des systèmes de santé ? » *in Traité d'économie et de gestion de la santé*, *op. cit.*, p. 75) et, conditionnant cette performance, l'apport des systèmes d'information informatisés et du traitement des données de santé dans la recherche d'efficience (G. DE POURVILLE, « L'économie de la santé : périmètre et questions de recherche », *Ibid.*, p. 15, spéc. p. 22 ; M. GAGNEUX, « Systèmes d'information et efficience du système de santé », *Ibid.*, p. 477). A ces objectifs s'ajoute la contrainte de maîtrise des dépenses de santé, ce qui implique une recherche d'efficience dans un contexte de gestion globale des ressources : « L' « efficience » […] *renvoie au concept de rendement : l'utilisation optimale des ressources disponibles pour obtenir des résultats maximums. Elle correspond à la capacité d'un système à fonctionner de façon moins coûteuse sans diminuer les résultats possibles et souhaitables.* […]. *L'OCDE considère que « l'efficience » est également un objectif fondamental des systèmes de santé* » (O. ZEYNEP, « Pourquoi et comment évaluer la performance des systèmes de santé ? », *Ibid.*, p. 76-77).

[1495] *Ibid.* p. 79.

[1496] Madame Lasserre explique que l'information est un mode de sociologisation du droit lequel se traduit notamment par des « *ajustement successifs entre le droit et la société* ». Ces ajustements sont une réponse à une crainte d'ineffectivité de la loi et plus le domaine d'intervention de la loi est technique plus les pouvoirs publics « se rapprochent du terrain ». Le système de santé n'échappe pas à ce phénomène dont l'information est l'outil principal (V. LASSERRE, *Le nouvel ordre juridique*, LexisNexis, 2015, n° 90 et svt). Plus largement, ce phénomène marque le « *basculement de la rationalité juridique traditionnelle vers une rationalité technico-économique* » (J. CHEVALLIER, *L'Etat post-moderne*, LGDJ, 3e éd. 2008, p. 137).

[1497] J.-M. SAUVÉ, « Introduction », *in Santé et protection des données, Septièmes entretiens du Conseil d'Etat en droit social*, 1er décembre 2017.

[1498] *Ibid.*

[1499] Le décret n° 2016-1606 du 25 novembre 2016 (*JORF* 27 nov. 2016, texte n° 276) fixe les modalités de déclaration à l'agence régionale de santé des effets indésirables liés aux soins, le décret n° 2017-885 du 9 mai 2017 (*JORF* 10 mai 2017, texte n° 109) prévoit les mesures réglementaires relatives aux vigilances sanitaires (nutrivigilance, toxicovigilance, addictovigilance et pharmacovigilance) ; A.- C., MAILLOLS-PERROY, « Les vigilances », *RDS*, n° 3, 2005, p. 81. Sur l'exigence de qualité et les établissements de santé v. L. CLUZEL-METAYER, *Le service public et l'exigence de qualité*, préf. J. CHEVALLIER, Nouvelle bibliothèque de thèses, Dalloz, 2006, *spéc.* n° 87 et svt.

[1500] J.-M. SAUVÉ, « Introduction » *in Santé et protection des données, Septièmes entretiens du Conseil d'Etat en droit social, op. cit.*

l'utilisation des données contenues dans le SNIIRAM à ces fins[1501] ainsi que celui de rassembler ces données avec des *données médicales*[1502] contenues dans d'autres grandes bases. Ce à quoi le législateur s'est employé en créant le système national des données de santé (SNDS) qui tend à devenir la *Plateforme nationale des données de santé*[1503].

323. Maîtrise des dépenses de santé et équilibre financier de la sécurité sociale. Surtout, la maîtrise des dépenses de santé est l'argument fort du traitement automatisé des données à caractère personnelles issues de la prise en charge des personnes par le système de santé, *« dans une logique économique prévenant la surconsommation inefficace de médicament et la multiplication tout aussi vaine de traitement* »[1504]. Comme nous l'avons mentionné, la performance du système de santé ne peut uniquement s'envisager en termes d'efficacité et chaque politique de santé visant l'amélioration de la prise en charge, la qualité et la sécurité des soins, chacun de ces objectifs porté par la recherche, doit également se faire au regard de l'impératif de maîtrise des dépenses de santé. Cela conditionne l'intégralité du maintien du système de santé français et du choix de société qu'il reflète, celui de la solidarité[1505].

324. Politique sécuritaire, l'intérêt général au-delà du système de santé. Dans une optique éloignée des considérations relevant de la performance du système de santé, le traitement des données à caractère personnel issues de la prise en charge sanitaire est également sollicité pour répondre à une demande croissante de sécurité[1506] des personnes et des biens,

---

[1501] C'est le terme utilisé par le Cour des comptes : Cour des comptes, *Les données personnelles de santé gérées par l'assurance maladie – Une utilisation à développer, une sécurité à renforcer,* Communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale, Mars 2016.

[1502] *Ibid.* p. 27 et svt.

[1503] V. *infra* n° 387.

[1504] J.-M. SAUVÉ, « Introduction », *in Santé et protection des données, Septièmes entretiens du Conseil d'Etat en droit social, op. cit.*

[1505] Sur la complémentarité des objectifs d'intérêt général, v. D. CRISTOL, « Le droit à la protection de la santé face aux exigences de maîtrise des dépenses de santé », *in Mélanges en l'honneur de Jean-Henri Soutoul*, LEH, 2000, p. 103.

[1506] « *La sécurité est l'objet même de l'engagement en société* » (M. GAUCHET, *La démocratie contre elle-même*, Gallimard, coll. Tel, 2002, p. 215). Elle peut se définir, au prisme du pouvoir, comme outil de normalisation des populations ainsi que l'explique un auteur (O. THOLOZAN, « Sécurité et droit : la nécessité au feu de l'imprévisibilité », *in* U. NGAMPIO-OBELE-BELE (ss. la dir.), *La sécurité en droit public*, coll. Colloques & Essais, Institut Universitaire Varenne, 2018, p. 16) reprenant les propos de Michel FOUCAULT au Collège de France (M. FOUCAULT, *Il faut défendre la société. Cours au collège de France (1975-1976)*, Seuil-Gallimard, 1997), lequel avait souligné le passage d'une vision de la souveraineté consistant à « *faire mourir et laisser vivre* » à un pouvoir displinaire notamment fondé sur la sécurité et visant à « *faire vivre et laisser mourir* ». En droit pénal et particulièrement en matière de politique pénale, la sécurité a supplanté la surêté face à des phénomènes d'insécurité ou de danger tant extérieurs qu'intérieurs, si bien que l'approche foucaldienne est également pertinente

cette exigence ayant pour « *support principal l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public* »[1507]. Le traitement de ces données peut constituer alors un outil de surveillance et de contrôle, ce qui rejoint les propos antérieurement développés[1508].

Les objectifs d'intérêt général que les politiques ont fait dépendre, en partie, du traitement automatisé des données à caractère personnel et de santé révèlent les éléments en balance dans la conciliation qui constitue la matrice de la loi informatique et libertés et plus largement des dispositions relatives à la protection des données. Les secrets professionnels, et particulièrement les secrets des professionnels du domaine de la santé, sont également l'objet de conciliations.

B - Le secret professionnel objet de conciliation

325. C'est au regard des enjeux en présence **(1),** que s'apprécient les aménagements concédés aux secrets professionnels de premier rang dans le domaine de la santé **(2)**, mais également hors de celui-ci **(3)**.

1 - Les enjeux de la conciliation

326. Secret relatif, relativisation constante. Le mouvement de relativisation du secret professionnel n'est pas récent et a longtemps occupé la doctrine. Emile Garçon évoquait déjà la nécessité de relativiser l'interdiction faite aux professionnels de révéler les secrets dont ils prennent connaissance dans l'exercice de leur activité. En conclusion du développement consacré au secret professionnel médical dans son Code pénal annoté, les continuateurs de l'œuvre d'Emile Garçon citent les propos d'André Lemaire : « *Le secret professionnel est un principe d'intérêt public affirmé à une époque où l'intérêt public se confondait avec l'intérêt individuel des malades. Aujourd'hui l'intérêt public paraît s'aligner sur le collectif et*

(M. DELMAS-MARTY, *Libertés et sûreté dans un monde dangereux*, coll. La couleur des idées, Le seuil, 2010 ; v. également les travaux de C. LAZERGES et par exemple « Le déclin du droit pénal : l'émergence d'une politique criminelle de l'ennemi », *RSC* 2016, p. 649).

[1507] X. DUPRES DE BOULOIS, « Existe-t-il un droit fondamental à la sécurité ? », *RDLF* 2018, chron. n° 13 ; M. NICOD (ss. la dir.), *Qu'en est-il de la sécurité des personnes et des biens*, Actes du colloque des 19 et 20 oct. 2006, coll. Travaux de l'IRF, n° 7, Presses de l'Université Toulouse 1 Capitole, LGDJ - Lextenso Editions, 2008.

[1508] V. *supra* n° 311.

surclasser l'individuel »[1509]. La controverse entre les défenseurs du secret et ses détracteurs, n'a pas cessé depuis lors et la liste des faits justificatifs est allée en s'allongeant[1510]. Si le secret professionnel médical n'est pas le seul en cause, il est à la fois celui dont le caractère absolu est le plus revendiqué, par les médecins eux-mêmes, et le plus décrié. Dans un ouvrage maintes fois cité dans les études relatives au secret professionnel, André Damien constatait, en 1989 une *fonte* du secret professionnel : « […] *sur le plan médical dans la mesure où le principe du secret étant posé, l'obligation est faite aux médecins de dénoncer des maladies de plus en plus nombreuses ; les cours-circuits administratifs concernant la communication des ordonnances à des services de sécurité sociale, les problèmes concernant l'exercice de la médecin du travail, rendent souvent le secret médical illusoire* […]. *Ainsi, non seulement le législateur sape le secret professionnel par des coupes importantes et répétées, mais les citoyens et l'opinion publique ne tolèrent plus le maintien d'un secret qui leur paraît contraire aux intérêts du bien commun*. »[1511]. La « logique » du compromis entre des intérêts *a priori* opposés et hierarchisés est l'instrument principal de l'affaiblissement du secret professionnel. Les questions de l'équilibre entre le secret professionnel et d'autres objectifs d'intérêt général ou des intérêts individuels ont principalement concerné le secret professionnel et le droit à la preuve[1512], le

---

[1509] A. LEMAIRE, « Le secret professionnel, une conception périmée », *Le Monde*, 31 juillet 1953 – *Adde* E. GARCON, *Code pénal annoté*, t. 2, éd. refondue et mise à jour par M. ROUSSELET, M. PATIN et M. ANCEL, Sirey, Paris, 1956, art. 378, p. 549.

[1510] Le mouvement de relativisation s'est illustré par un nombre croissant d'obligations et de permissions de révéler.

[1511] A. DAMIEN, *Le secret nécessaire*, coll. Micromégas, Desclée de Brouwer, 1989, p. 20-21.

[1512] S'agissant principalement de contentieux dans lesquels l'opposabilité du secret professionnel était en cause quelques décisions ont affirmé la primauté des secrets professionnels sur le droit à la preuve en matière civile : Civ. 1re, 14 janv. 2010, n° 08-21.854, *D.* 2010, p. 1125, obs. V. AVENA-ROBARDET ; *ibid.*, p. 2671, obs. P. DELEBECQUE, J.-D. BRETZNER et I. GELBARD-LE DAUPHIN ; *D*. 2011, p. 552, obs. B. BLANCHARD ; Com. 3 mai 2012, n° 11-14.008, *D*. 2012, p. 1343 ; *Rev. sociétés* 2012, p. 721, note E. STERU et E. DEZEUZE ; s'agissant du secret professionnel médical : Civ. 1re, 11 juin 2009, n° 08-12.742, *D.* 2009, p. 1760 ; *ibid.*, p. 2714, obs. P. DELEBECQUE, J.-D. BRETZNER et T. VASSEUR ; *RTD civ.* 2009, p. 695, obs. J. HAUSER ; Com. 10 fév. 2015, n° 13-14.779, *D.* 2015, p. 428 ; *D.* 2015, p. 959, obs. J. LASSERRE-CAPDEVILLE ; *RDT* 2015, p. 191, obs. P. ADAM ; *Dalloz act.*, 24 févr. 2015, obs. V. AVENA-ROBARDET ; *JCP G* 2015, 226, obs. C. BARRIERE ; *LEDB* mars 2015, obs. R. ROUTIER. L'importance des contributions dans les mélanges témoigne de la constance de l'intérêt que l'ensemble de la doctrine a porté à la conciliation entre ces intérêts : H. LECLERC, « La justice et le secret », *in Mélanges en l'honneur de Robert Badinter*, *L'exigence de justice*, Dalloz, 2016, p. 545 ; G. CLÉMENT, « Le secret de la preuve pénale », *in Mélanges dédiés à Bernard Bouloc*, *Les droits et le droit*, Dalloz, 2007, p. 183 ; B. BOULOC, « Le secret professionnel de l'avocat », *in Mélanges offerts à Raymond Gassin*, PUAM, 2007 p. 121 ; P. LAMBERT, « Le respect du secret professionnel de l'avocat, composante du droit à un procès équitable », *in Mélanges en l'honneur de Serge Guinchard*, *Justice et droit du procès: Du légalisme procédural à l'humanisme processuel*, Dalloz, 2006 p. 291 ; J. PENNEAU, *Le secret médical et la preuve (ou l'introuvable solution)*, *in Mélanges dédiés à Dominique Holleaux*, Litec, 1990 p. 345 ; J. PENNEAU, « De quelques incidences du secret médical sur l'expertise judiciaire », *AJ Pénal* 2009, p.169.

secret professionnel et le droit à l'information[1513], le secret professionnel et la recherche des infractions pénales[1514], le secret professionnel et la protection des personnes concernées par les informations couvertes par le secret[1515] ou plus spécifiquement la santé des tiers[1516]. L'intervention du législateur afin de prévoir des permissions ou obligations[1517] de révéler pour la défense d'intérêts considérés comme supérieurs est régulièrement sollicitée au gré des faits divers[1518]. L'informatique étant un outil, il peut servir chacun des objectifs d'intérêt général. S'il est en quelque sorte transparent dans la recherche d'équilibre, son efficacité va tendre à convaincre qu'il s'impose en ce qu'il constitue le meilleur moyen de préserver l'intérêt hierarchiquement supérieur.

[1513] Dont l'exemple le plus illustre est celui de l'affaire du *Grand secret* : CEDH 18 mai 2004, n° 58148/00, Plon c/ France, *D.* 2004, p. 1838, note A. GUEDJ et p. 2539, obs. N. FRICERO ; *RDSS* 2004, p. 841, note L. DUBOUIS ; *RTD civ.* 2004. 483, obs. J. HAUSER. Pour une synthèse sur cette question v. A. GUEDJ, « Liberté et responsabilité en droit européen et international », *in* B. BEIGNIER, B. DE LAMY, E. DREYER (ss. la dir.), *Traité de droit de la presse et des médias*, coll. Traités, LexisNexis, 2009, n° 218.

[1514] Notamment en matière financière : C. GHICA-LEMARCHAND, « Une certaine idée du secret bancaire », *in Mélanges offerts à André Decocq, Une certaine idée du droit*, Litec, 2004, p. 279 ; Y. REPIQUET, « Le secret professionnel de l'avocat et la lutte contre le blanchiment d'argent », p. 433 ; B. BOULOC, « Les limites du secret bancaire », *in Mélanges AEDBF*, Revue Banque Edition, 1997, p. 71.

[1515] Par exemple : C. JONAS, « Protéger ou trahir ? Réflexion d'un praticien sur les contradictions entre assistance à autrui et secret professionnel », *in Mélanges en l'honneur de Jean-Henri Soutoul*, LEH, 2000, p. 133 ; B. PY, « Le secret professionnel : une obligation de parler », *JA* 2008, n°386, p.15.

[1516] *Ibid.*

[1517] Sur le fondement de l'ordre ou l'autorisation de la loi et est prévue par l'article 122-4 du code pénal.

[1518] L'émotion est maîtresse en la matière et la presse se fait l'écho de la suspicion de la société civile envers le secret professionnel. Pour ne citer que deux exemples relativement récents : L'affaire du vol GWI18G Barcelone-Düsseldorf de la Germanwings en 2015 à l'occasion duquel le pilote, souffrant de dépression, avait volontairement écrasé l'avion dans les Alpes françaises, avait été l'occasion de remettre en cause le secret professionnel des médecins. Le Bureau d'Enquêtes et d'Analyses avait demandé que soit prévu un fait justificatif obligeant les médecins a révéler certaines informations sur l'état de santé des pilotes. Les titres de la presse européenne témoignent de la cristallisation des débats à propos du secret professionnel médical (P. BIENVAULT, « Faut-il lever le secret médical face à un pilote de ligne dépressif ? », *La croix*, 14 mars 2016 ; S. FAURE, « Les médecins doivent-ils renoncer au secret professionnel pour sauver des vies ? », *Libération*, 4 avril 2015 ; F. MODOUX, « Pilote inapte, le secret médical en procès », *Tribune de Genève*, 29 mars 2015). La crainte du terrorisme entretient le climat de défiance envers le secret professionnel ce que met notamment en exergue Caroline Kleiner à propos du secret professionnel bancaire : C. KLEINER « Les droits de l'homme et le secret bancaire : opposition ou subsomption ? », *Journal du droit international (Clunet)* n° 4, Oct. 2014, doctr. 15. S'agissant du phénomène de *radicalisation* (C. GUIBET-LAFAYE et A.-J. RAPIN, « La « radicalisation », Individualisation et dépolitisation d'une notion », *Politiques de communication* 2017/1, p. 127 s.) la tentation est grande d'ériger une obligation de révéler dans le but de prévoir une supposée *dangerosité* des individus dont les médecins pourraient penser qu'ils sont en cours de *radicalisation* (D. VIRIOT-BARRIAL, « Secret médical et terrorisme », *RDSS* 2019, p. 236 ; également CNOM, *Risque terroriste et secret professionnel du médecin*, Rapport adopté lors de la session Conseil national de l'Ordre des médecins de janvier 2017).

327. De la conciliation au compromis : l'affaiblissement des secrets professionnels. A l'occasion d'une intervention dans un colloque consacré au secret professionnel, Madame Frison-Roche analysait la *logique* qui provoque le déclin des secrets professionnels[1519]. L'auteur critique le manque d'intelligibilité de ce qu'elle nomme la « *méthode du troc* »[1520] au regard de laquelle chaque nouvelle exception au secret professionnel est discutée et de constater qu'« *en ce qui concerne les secrets professionnels, quels qu'ils soient, la puissance est du côté de la transparence, fer de lance d'une administration désormais internationale et soudée* »[1521]. Elle souligne que, derrière le discours visant à chercher un *équilibre*, au sens de conciliation, chaque exception concédée est le résultat « *d'un rapport de force, c'est à dire un compromis dans l'attente de la prochaine avancée de la levée des secrets professionnels* »[1522]. Bruno Py pose un constat identique lorsqu'il affirme : « *Le secret, devenu suspect, s'effacerait devant l'ordre public* »[1523]. L'idée est par ailleurs largement répandue dans la doctrine[1524].

328. Logique du compromis, hiérarchisation et opposition des intérêts. Arguant de la nécessité d'une méthode fondée sur le seul intérêt de la personne au bénéfice de laquelle le secret est institué[1525], Marie-Anne Frison-Roche considère encore que la hiérarchisation et l'opposition entre intérêt général et intérêts particuliers est pernicieuse[1526]. L'auteur le résume ainsi : « *Dans un modèle libéral, il est d'intérêt général de défendre les intérêts particuliers.* […]. *La distribution entre intérêt général et intérêt particulier est rapidement rhétorique, le jeu de puissance consistant à s'approprier la défense du plus élevé, se glisser dans le rôle de celui qui garde l'intérêt général, comme l'administration sait l'affirmer, ce qui met en position rhétorique définitivement négative celui qui se bat pour l'intérêt particulier* »[1527]. Lorsque

---

[1519] M.-A. FRISON-ROCHE, « Critère des intérêts et secret professionnel », *in Les entretiens du Palais*, *Gaz. Pal*., 18 février 2005, pp.78-81.
[1520] *Ibid.*, p. 78.
[1521] *Ibid.*
[1522] *Ibid.*
[1523] B. PY, « Le secret professionnel : le syndrôme des assignats ? », *AJ pénal* 2004, p. 133.
[1524] V. par exemple J.-H. ROBERT, « Secrets professionnels », *JCP G*, n° 47 hors-série, 19 Novembre 2012, ; E. VERNY, « La notion de secret professionnel », *RDSS* 2015, p. 395 ; Concernant le secret professionnel médical, mais traitant à la fois de la question de l'opposabilité et des faits justificatifs : M. BÉNEJAT-GUERLIN, « Que reste-t-il de la protection pénale du secret médical ? », *AJ pénal* 2017, p. 368 ; D. HOUSSIN, « Le secret médical dans les nouvelles pratiques et les nouveaux champs de la médecine » *D.* 2009, p. 2619 ; C. BERGOIGNAN-ESPER, « La confidentialité des informations de santé peut-elle tenir face à la protection d'autres intérêts légitimes ? », *D.* 2008, p. 1918.
[1525] M.-A. FRISON-ROCHE, « Critère des intérêts et secret professionnel », *op. cit.*, p. 79.
[1526] *Ibid.* p. 80.
[1527] *Ibid.*

l'intérêt général est *porté* par un outil efficace, l'on conçoit que le compromis se fasse, davantage encore, au détriment du secret professionnel en tant qu'institution et des secrets professionnels en fonction de leur domaine.

C'est au regard de ces objectifs de conciliation mus en compromis par les enjeux de pouvoir, que s'analyse le rapport entre le traitement des données et les secrets professionnels dans le domaine de la santé.

329. L'influence de la Cnil. Il apparaît que, dès les premiers temps de la loi informatique et liberté, le traitement informatique des informations – notamment des informations issues de la relation médicale – par l'Etat et l'administration est sollicité. La CNIL, présentée comme un contre-pouvoir face à l'Etat[1528], est investie d'une mission de conseil au regard de laquelle elle rend des avis[1529] en vertu de l'ancien article 15 de la loi informatique et libertés. Si elle n'a pas

---

[1528] La CNIL a en effet été conçue comme « *l'organe de la conscience sociale face à l'emploi de l'informatique* », (A. LUCAS, *Le droit de l'informatique*, PUF, 1987, p. 176).

[1529] L'avis est défini comme un *« conseil donné par un organe délibératif qui détient le pouvoir d'édicter la norme pour l'inviter à prendre une telle décision* » (S. GUINCHARD, G. MONTAGNIER, *Lexique des termes juridiques*, 17ème éd., Dalloz, 2009, *V°* « avis »). Ces actes consultatifs, sont « *les catégories connues du droit administratif : avis simple, avis obligatoire, avis conforme* » (S. GERRY-VERNIERES, *Les « petites » sources du droit. A propos des sources étatiques non contraignantes*, préf. N. MOLFESSIS, coll. Recherches Juridiques, Economica, 2012, n° 293), les avis de la CNIL n'interviennent pas tous dans le cadre de prérogatives identiques. Dans les premiers temps de la loi informatique et libertés, l'article 15 de la loi prévoyait : « *Hormis les cas ou ils doivent être autorisés par la loi, les traitements automatisés d'informations nominatives opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité territoriale, ou d'une personne morale de droit privé gérant un service public, sont décidés par un acte réglementaire pris après avis motivé de la commission nationale de l'informatique et des libertés* », l'avis était donc obligatoire pour certains traitements. La CNIL doit désormais être consultée en amont de la mise en œuvre du pouvoir règlementaire ou légal 8-4 a) : « *Elle est consultée sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données. Elle peut également être consultée par le Président de l'Assemblée nationale, par le Président du Sénat ou par les commissions compétentes de l'Assemblée nationale et du Sénat ainsi qu'à la demande d'un président de groupe parlementaire sur toute proposition de loi relative à la protection des données à caractère personnel ou au traitement de telles données. Outre les cas prévus aux articles 31 et 32, lorsqu'une loi prévoit qu'un décret ou un arrêté est pris après avis de la commission, cet avis est publié avec le décret ou l'arrêté* ». C'est à ce titre qu'elle est notamment consultée par les pouvoirs publics dans le domaine de la santé pour toutes les modifications ayant trait à la protection des données (elle a ainsi récemment été consulté sur le projet de loi relatif à la transformation du système de santé (Délibération n° 2019-008 du 31 janvier 2019 portant avis sur un projet de loi relatif à l'organisation et à la transformation du système de santé). Enfin, la CNIL rend également des avis simples : elle peut en effet être sollicitée par les personnes publiques ou privées et par les juridictions à propos d'un projet de traitement de données (art. 8-2 e) LIL). Outre ces avis qui constituent un conseil, la CNIL exerce également une forme de conseil *a priori* à la mise en œuvre des fichiers par l'Etat ou pour le compte de celui-ci. Même si ces avis sont parfois décrits comme un « contrôle », ils ne lient pas le demandeur (S. GERRY-VERNIERES, *Les « petites » sources du droit. A propos des sources étatiques non contraignantes, op. cit.*, n° 293). Malgré leur caractère obligatoire, ils ne sont pas toujours sollicités, ce que la CNIL dénonce parfois (sur ce point, concernant les fichiers de police v. V. GAUTRON, Rép. pén. *V°* « Fichiers de police », avril

pour rôle d'évaluer le caractère général de l'intérêt présenté par un traitement mis en œuvre par l'Etat ou l'administration, elle y procède néanmoins lorsqu'elle se prononce sur les finalités du traitement de données. Ces avis, rendus en amont des traitements autorisés par actes règlementaires ou sur les traitements de données à caractère personnel mis en œuvre par l'Etat nécessitant un décret en Conseil d'Etat[1530] ainsi que les avis rendus en vertu d'une obligation procédurale de consultation pour tout projet de loi ou de décret ou toute disposition relatifs à la protection des données s'intègrent au processus normatif[1531]. Dès lors qu'ils sont suivis par l'exécutif, il est possible d'affirmer, en dépit du caractère consultatif de ces avis, que la Commission a « *un rôle quasi-normatif de facto* »[1532]. Or, nous avons pu voir que la CNIL avait

---

2015 (act. Mars 2019, spéc. n° 35), certains traitements qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ; ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté (art. 31 de la LIL).

[1530] Il ne s'agit plus, désormais, que des traitements de données de santé comportant le NIR (art. 30 de la LIL), ceux mis en œuvre pour le compte de l'Etat, agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes (art. 32 de la LIL).

[1531] Jacques Raynard souligne que les avis en amont de la loi sont intégrés « *au processus d'élaboration de la prescription* » (J. RAYNARD, « Domaines et thèmes des avis », *in* Th. REVET (ss. la dir.), *L'inflation des* avis, coll. Etudes juridiques, Economica, 1998, p. 11, spéc. p. 14). Evoquant l'avis – sans viser spécifiquement celui des AAI – sollicités en amont de la loi, Philippe Jestaz explique que les avis sur des projets de loi servent *« à exercer un contrôle de correction juridique, l'émetteur se comportant à la façon d'un professeur qui corrige la thèse de son étudiant*. […] *il s'agit d'un avis-inspection* » (Ph. JESTAZ, « Rapport de synthèse », *in* Th. REVET, *L'inflation des avis*, *op. cit.*, p. 113, spéc. p. 116). Monsieur Mouchette considère que les avis obligatoires sont des instruments incitatifs de ce qu'il nomme la « magistrature d'influence » des AAI (J. MOUCHETTE, *La magistrature d'influence des autorités administratives indépendantes*, Préf. de P. WACHSMANN, *coll. Bibliothèque de droit public*, LGDJ, 2019, n° 485 et svt.) selon lui ces instruments ne peuvent être « rangés » dans la catégorie fourre-tout du droit souple, qu'il critique par ailleurs, et considère que le « *phénomène recommandationnel* » appartient au « *contexte du droit sans toutefois pouvoir les assimiler au droit* » (*Ibid.* n° 522 et svt.).

[1532] L'expression est utilisée par Rémy Libchaber pour désigner le pouvoir de l'autorité de la concurrence dont il affirme que les « *lois récentes se sont appropriées le contenu de certaines recommandations* » (R. LIBCHABER, « L'autorité des recommandations de la Commission des clauses abusives », *RTD civ.* 1997, p. 791). En outre, une analogie est possible entre la doctrine (comprise comme « *la pensée des auteurs. Par extension l'ensemble des auteurs* », S. GUINCHARD, G. MONTAGNIER, *Lexique des termes juridiques*, 17ème éd., Dalloz, 2009, *V°* « doctrine ») et les travaux de la CNIL et particulièrement les avis qu'elle rend à l'occasion de sa mission de conseil. Si la doctrine est une source, au moins indirecte du droit (Ph. JESTAZ, Ch. JAMIN, *La doctrine*, coll. Méthodes du droit, Dalloz, 2004), elle n'agit que par « *voie d'influence* » (*Ibid.* p. 6), l'on peut par exemple rappeler son « *rôle d'expert institutionnel* » (*Ibid.* p. 236) lorsqu'elle est sollicitée par les décideurs sur un projet de loi. Les AAI en général, et la CNIL en particulier, de par les instruments de conseil dont elles disposent, peuvent consistuer, bien que nous l'évoquons avec réserve, une doctrine, et leurs productions peuvent sans doute s'analyser comme une doctrine non pas au sens administrativiste du terme (le terme de *doctrine administrative* étant surtout employé en matière fiscale pour désigner le pouvoir d'instruction ministériel à la destination des services v. J.-J. BIENVENU, « Naissance de la doctrine administrative », *in RF fin. pub.* 2001, n° 75, p. 11) mais comme « *la littérature du droit* » (D. ALLAND et S. RIALS, *Dictionnaire de culture juridique*, Quadrige, Lamy-PUF, 2003, *V°* « doctrine »). Les AAI partagent, avec la doctrine, une indépendance (qui peut être relativisée) et un statut d'expert (bien que cette expertise ne soit pas *savante*, elle consiste, pour la CNIL, en une connaissance de la technique informatique, de la loi informatique et liberté, c'est en raison de cette expertise qu'elle porte son discours vers ce qui est souhaitable). A la grande différence que la CNIL bénéficie d'instruments incitatifs par lesquels son

parfois autorisé la transmission d'informations couvertes par le secret en dépit de textes justificatifs[1533], s'assurant par ailleurs de l'existence de garanties pour assurer la confidentialité des informations[1534]. Elle n'a toutefois pas manqué de souligner, à de multiples reprises, l'importance d'une intervention du législateur afin d'assouplir le secret professionnel, tandis que certains faits justificatifs ont parfois été prévus par décret ou par la loi. Ces aménagements peuvent être analysés au regard des finalités des traitements.

330. A propos des faits justificatifs. Les faits justificatifs de la violation du secret professionnel sont nombreux et disparates. Outre le premièrement du premier alinéa de l'article 226-14 du Code pénal qui prévoit une permission générale de révéler[1535], les autres alinéas concernent uniquement les autorisations offertes aux professionnels de santé. De plus, certaines causes générales d'irresponsabilité pénale s'appliquent à la révélation d'informations par des personnes soumises au secret[1536]. Les textes ayant fonction de justification se trouvent éparpillés dans les codes et les textes législatifs et règlementaires et leur champ d'application se limitent souvent à un secret en particulier[1537]. Ensuite, certains faits justifiant la violation du

---

pouvoir s'exerce. Nous nous garderons ici de qualifier les contrôles *a priori* de la CNIL. Si les décisions rendues dans le cadre de son pouvoir d'autorisation sont susceptibles de recours devant le Conseil d'Etat et appartiennent donc à la catégorie classique des actes décisoires unilatéraux, il n'en va pas de même pour les avis obligatoires. Nous renverrons pour une étude complète nous renverrons notamment aux travaux de Monsieur Mouchette (envisageant ces instruments comme la marque d'un pouvoir d'influence n'appartenant pas au droit) ainsi qu'à ceux de Monsieur Gérry-Vernières (qui les appréhende comme des sources du droit) : J. MOUCHETTE, *La magistrature d'influence des autorités administratives indépendantes*, *op. cit.* ; S. GERRY-VERNIERES, *Les "petites" sources du droit : à propos des sources étatiques non contraignantes*, *op. cit.*

[1533] V. *supra* n°242 et svt.

[1534] V. *supra Ibid.*

[1535] « *A celui qui informe les autorités judiciaires, médicales ou administratives de privations ou de sévices, y compris lorsqu'il s'agit d'atteintes ou mutilations sexuelles, dont il a eu connaissance et qui ont été infligées à un mineur ou à une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son incapacité physique ou psychique* » (CP, art. 226-14, al. 1).

[1536] Il en est ainsi de l'état de nécessité (CP, art. 122-7) qui semble pouvoir justifier la révélation du secret professionnel (Par exemple : À propos du secret professionnel bancaire : J. LASSERRE-CAPDEVILLE, « La détection du délit d'abus de faiblesse par le banquier », *AJ pénal* 2018, p. 223 et *Rép. pen.*, *V°* « Banque », n° 275 ; A propos du secret professionnel médical : Y. MAYAUD, « Des mauvais traitements sur mineurs de quinze ans et de leur retombées, en terme de secours et de dénonciation, sur les professionnels de la santé et de l'assistance », *Rev. sc. crim.* 1998, p. 320 ; B. PY, « Le secret professionnel : une obligation de parler », *Jurisassociations* 2008, p. 15 ; A propos de la prévention des infractions terroristes et du secret professionnel médical : D. VIRIOT-BARRIAL, « Secret médical et terrorisme », *RDSS* 2019 p. 236) ; Posant la question de l'application du fait justificatif pour un médecin qui révèlerait la séropositivité de son patient au conjoint de ce dernier, cette question étant posée par l'auteur suite à la condamnation d'un prévenu pour administration de substance nuisible, en l'espèce la transmission volontaire du VIH (M. BENILLOUCHE, « Les incertitudes juridiques entourant la contamination volontaire par le VIH », *AJ pénal* 2012, p. 388).

[1537] CP, art. 226-14, al. 1, 2°, 3°.

secret professionnel ne visent que les révélations faites par les médecins[1538]. Il s'agira d'analyser les aménagements concédés aux secrets professionnels afin de traiter et faire circuler les données issues de la relation de soin.

2 - Les aménagements opérés dans le domaine de la santé

331. Dans le prolongement de l'extension du champ d'application de l'infraction sanctionnant la violation du secret professionnel, c'est en faveur de la recherche dans le domaine de la santé et des statistiques publiques qu'ont été opérés les aménagements les plus importants **(a)**. La maîtrise des dépenses de santé constitue également un intérêt au profit duquel le secret professionnel doit céder **(b)**.

a - Recherche dans le domaine de la santé et statistiques

332. La transmission des informations couvertes par le secret à l'INSEE. Le premier aménagement notable du secret professionnel dans le domaine de la santé et pour les besoins du traitement de données concerne les statistiques. Tandis que les statistiques publiques peuvent être mises en œuvre par le biais d'enquêtes auprès des personnes et permettant à l'INSEE de collecter des informations relatives à la santé des personnes, il demeurait que les données collectées par les administrations et les établissements publics ne pouvaient être transmises à l'institut. Par une loi du 23 décembre 1986, le législateur est venu prévoir une justification spéciale à la violation du secret professionnel afin de permettre la transmission par une administration, un établissement public ou une personne morale de droit privé gérant un service public, des informations nominatives à l'INSEE[1539]. Cette exception ne concerne donc pas seulement le secret professionnel médical. La Commission avait d'ailleurs eu l'occasion de rappeler, à plusieurs reprises, que le partage de données nominatives entre des administrations distinctes ne pouvait être autorisé en raison du secret professionnel[1540]. La transmission des

---

[1538] Pour citer quelques exemples : La déclaration obligatoire des naissances, des décès, des maladies contagieuses dont la liste est fixée par décret, la transmission des certificats d'hospitalisation.

[1539] Loi n° 86-1305 du 23 décembre 1986 portant modification de la loi 51-711 du 07 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques (*JORF* du 26 décembre 1986 p. 15596). Cette exception s'est accompagnée de la soumission au secret professionnel de tous les agents de l'INSEE : v. *supra* n° 297.

[1540] Rappel formulé à l'occasion de l'édiction d'un norme simplifiée (n° 26) concernant les traitements statistiques, dans lequel la CNIL a confirmé l'impossibilité de partager les informations couvertes par le secret entre les admnistrations : « *Le problème de la transmission d'informations entre administrations est controversé. Il a cependant été mis fin à cette controverse juridique dans le sens de l'interdiction faite aux administrations de se communiquer leurs secrets. La jurisprudence a toujours interprété l'obligation au secret professionnel de façon*

informations nominatives impliquait donc une intervention du législateur. Le projet de loi en ce sens a été soumis à la CNIL qui, dans son avis, a souligné que « *la transmission d'informations nominatives couvertes par le secret professionnel et relevant en particulier du secret médical, prévue par le projet de loi doit s'opérer conformément aux lois précitées du 7 juin 1951 et du 6 janvier 1978 ; qu'elle constitue une nouvelle exception aux dispositions de l'article 378 du Code Pénal* »[1541]. Il avait été prévu, en guise de *compensation*, des garanties renforcées pour les données issues de la relation de soin puisque toute transmission devait faire l'objet d'un acte réglementaire après avis motivé de la CNIL.

333. La transmission des informations couvertes par le secret et la recherche dans le domaine de la santé. Le problème de la transmission des informations couvertes par le secret professionnel à des organismes de recherche s'est posé, nous l'avons évoqué, dès les années 1980. En 1985, la CNIL, le Comité consultatif national d'éthique (CCNE) et l'Ordre national des médecins avaient sollicité le législateur dans le sens d'un assouplissement du secret professionnel médical[1542]. Les raisons de ce souhait exprimé par les deux institutions tiennent notamment à l'existence, avant la promulgation de la loi informatique et libertés, de registres relatifs aux cancers et dont certains ont été postérieurement déclarés à la CNIL. En 1985, la Commission avait posé les données du problème au sujet duquel une concertation entre les deux institutions précitées et l'Institut national de la santé et de la recherche médicale (INSERM) avait donné lieu : la tenue des registres nécessitait l'adhésion des médecins mais plus encore, elle imposait de leur part la communication d'informations normalement couvertes par le secret

---

rigoureuse. Dans son avis rendu en 1965, traitant des demandes de renseignements émanant d'autorités ou de services poursuivant un objet dépourvu de rapport avec celui qui est interrogé (en l'espèce, les organismes de Sécurité sociale), le Conseil d'Etat a estimé que « la règle du secret professionnel fait obstacle, en l'absence de disposition législative expresse permettant d'y déroger, à la communication des renseignements sollicités... ». *De même, dans des arrêts ultérieurs* (Crochette, 11.2.1972), *il a considéré que* « à l'intérieur de l'administration, les informations couvertes par le secret professionnel ne sont communicables qu'aux administrations et agents ayant compétence pour assumer la mission pour laquelle les renseignements sont recueillis... » ». Par exemple à propos des fichiers de population des municipalités, la CNIL souligne « *Quant à l'utilisation statistique de données nominatives, détenues par des services de la municipalité, il convient d'interpréter de façon stricte l'obligation de secret professionnel établie par l'article 378 du code pénal, qui exclut tout partage du secret entre services publics distincts. Ainsi, chaque service est habilité à détenir les seules informations nominatives qui lui sont nécessaires pour l'exercice de ses missions* » (CNIL, *Rapport d'activité* 1985, p. 154).

[1541] Délibération n° 86-42 du 8 avril 1986 portant avis, au sens de l'article 1er du décret n° 78-774 du 17 juillet 1978, sur le projet de loi tendant à autoriser l'INSEE à recevoir communication d'informations recueillies sous le couvert du secret par d'autres administrations, en vue de l'élaboration de statistiques.

[1542] CNIL, *Rapport d'activité 1985*, p. 89.

professionnel, à des fins épidémiologiques. Nous avons mentionné la timide critique de la CNIL à ce sujet[1543]. Elle avait par ailleurs reconnu, dans un rapport annuel, que l'informatisation était une nécessité dans la mesure où elle « *permet et permettra de plus en plus une meilleure gestion de la société, de l'économie, des administrations, de l'Etat. En ce domaine, le retard se paie cher* […] »[1544] et d'ajouter qu'« *un exemple a été donné tout au long du second semestre 1984 par l'étude des problèmes des registres du cancer* […]. *La nécessité de concilier les progrès de la recherche* […] *ne peut avancer sans informatisation, le respect du malade et les devoirs du médecin traitant* […] »[1545]. C'est donc guidée par la logique de compromis que la CNIL a recommandé une intervention du législateur dans le sens d'un assouplissement du secret professionnel médical[1546]. Il faudra néamnoins attendre 1994[1547] pour que le législateur se saisisse du problème et prévoit, par une modification de la loi informatique et libertés et la création d'un chapitre dédié, l'aménagement au secret professionnel, non pas seulement médical, mais des professionnels de santé[1548]. Notons que le texte en question est passé relativement inaperçu en comparaison de l'importance des débats publics dont avaient été l'objet les deux autres lois du triptyque des lois dites *bioéthiques*. Aussi, si la loi relative au respect du corps humain[1549] et celle relative à l'utilisation des éléments et produits du corps humain, à l'assistance médicale à la procréation et au diagnostic prénatal[1550] ont été examinées par le Conseil constitutionnel[1551], ce ne fut pas le cas de celle modifiant la loi informatique et liberté[1552]. Dans l'intervalle, la Commission avait parfois autorisé des traitements de données pour des finalités de recherche en composant avec les outils juridiques et techniques à sa

---

[1543] V. *supra* n° 224.
[1544] CNIL, *Rapport d'activité 1983-1984*, p. 5.
[1545] *Ibid.*
[1546] « *La Commission estime qu'il convient de compléter les dispositions de l'article 378 du Code pénal en vue d'autoriser les transmissions de données médicales nominatives entre médecins et organismes de recherche dans les conditions qu'elle indique dans la recommandation* » (CNIL, *Rapport d'activité 1985*, p. 89).
[1547] Loi n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recheche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[1548] Ancien art. 40-3 de la LIL ; Actuel article 68 de la LIL qui dispose en son premier alinéa : *« Nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre au responsable d'un traitement de données autorisé en application de l'article 66 les données à caractère personnel qu'ils détiennent*. »
[1549] Loi n° 94-653 relative au respect du corps humain, *JO* du 30 juillet 1994.
[1550] Loi n° 94-654 relative au don et à l'utilisation des éléments et produits du corps humain, à l'assistance médicale à la procréation et au diagnostic prénatal, *JO* du 30 juillet 1994.
[1551] Cons. const., 27 juillet 1994, n° 94-343/344 DC.
[1552] I. DE LAMBERTERIE et H.-J. LUCAS, *Informatique, libertés et recherche médicale*, coll. CNRS Droit, CNRS éditions, 2001, n° 50.

disposition afin que, faute de respect du secret professionnel, la confidentialité fût néanmoins assurée. Le texte prévoyant cette permission de révéler est désormais prévu à l'article 68 de la loi informatique et libertés. Le périmètre de cette exception est aujourd'hui particulièrement flou et potentiellement étendu puisque cet aménagement concerne désormais tous les traitements de données à caractère personnel dans le domaine de la santé ayant une finalité d'intérêt public[1553].

b - Evaluation et maîtrise des dépenses de santé

334. L'évaluation des dépenses des établissements publics et le partage des informations pour l'évaluation de l'activité des établissements. Avant la loi informatique et libertés, les établissements de santé publics comme privés avaient déjà mis en œuvre des traitements automatisés de données ayant pour finalité l'évaluation de l'activité des établissements publics ou privés. Le traitement informatisé des résumés de sortie a fait l'objet d'un arrêté pendant l'année 1985. La CNIL s'y est donc intéressée avec, pour question centrale, la « *protection du secret médical* »[1554]. Dans son avis rendu à propos du projet de décret, elle a précisé que certaines garanties devaient entourer la circulation des données issues de la relation de soin[1555]. Sans que cela ne soit explicite, il a été admis une exception au secret professionnel dès lors que l'arrêté prévoit la communication des informations, par les médecins prenant en charge les patients, à un médecin extérieur à la relation de soin qui sera désigné pour assurer la correspondance entre le numéro d'hospitalisation et le numéro anonyme du résumé de sortie standardisé[1556]. Obligation a ensuite été faite aux établissements publics et privés d'évaluer leur

---

[1553] Nous avons développé ce point lorsque nous avons envisagé l'assujettissement au secret professionnel des personnes accédant aux données sur le fondement de l'article 68 de la LIL, V. *supra* n° 298.

[1554] A. DEBET, J. MASSOT, N. METALLINOS (ss. la dir.), *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, coll. Les intégrales, Lextenso, 2015, n° 2632.

[1555] ; « *Le respect du secret médical et de l'anonymat des malades devait être garanti par l'adoption, non seulement de dispositifs particuliers de sécurité, mais, également, d'une procédure spécifique de circulation et d'exploitation de données médicales* » (Délibération n° 85-39 du 10 septembre 1985 portant avis sur le projet d'arrêté du Ministère des Affaires Sociales et de la Solidarité Nationale relatif à l'informatisation dans les établissements hospitaliers des résumés de sortie standardisés (RSS) élaborés dans le cadre du projet de médicalisation du système d'information (PMSI) ; CNIL, *Rapport d'activité 1985*, p. 101).

[1556] Les RSS anonymisés pouvant ensuite être transmis à des tiers (art. 3 et 4 de l'arrêté du 3 octobre 1985 autorisant l'informatisation des résumés de sortie standardisés dans les établissements d'hospitalisation publics et privés participant au service public hospitalier (abrogé)) et notamment aux organismes d'assurance maladie et à l'Etat (Arrêté du 20 septembre 1994 relatif au recueil et au traitement des données d'activité médicale et de coût, visées à l'article L. 710-5 du Code de la santé publique, par les établissements de santé publics et privés visés aux articles

activité (PMSI)[1557]. Une circulaire du 24 juillet 1989 a prévu la création du département d'information médicale, puis l'importance du traitement et le passage à la tarification à l'activité[1558] a rapidement nécessité d'y inclure des personnes n'étant pas professionnels de santé. Depuis 2009, la transmission consiste en une obligation pour les praticiens hospitaliers, dont le manquement peut entraîner une sanction[1559].

3 - Les aménagements opérés hors du secteur sanitaire : sécurité et ordre public

335. Le secret professionnel médical, ennemi de la sécurité et de l'ordre public ? L'opposition entre la sécurité publique et le secret professionnel médical[1560] se cristallise dans une spécialité médicale en particulier : la psychiatrie[1561]. Les personnes atteintes de troubles

---

L. 714-1, L. 715-5 du Code de la santé publique et aux articles L. 162-23, L. 162-23-1 et L. 162-25 du Code de la sécurité sociale et à la transmission aux services de l'Etat et aux organismes d'assurance maladie d'informations issues de ces traitements ; Arrêté du 22 juillet 1996 relatif au recueil et au traitement des données d'activité médicale, visées à l'article L. 710-6 du Code de la santé publique, par les établissements de santé visés à l'article L. 710-16-2 du même code et à la transmission, visée à l'article L. 710-7 du Code de la santé publique, aux agences régionales de l'hospitalisation, aux organismes d'assurance maladie et à l'Etat d'informations issues de ce traitement).

[1557] Loi n° 91-748 du 31 juillet 1991 portant réforme hospitalière.

[1558] Loi n° 2003-1199 du 18 décembre 2003 de financement de la sécurité sociale pour 2004.

[1559] Depuis la loi HPST de 2009 (Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires) les praticiens des établissements publics qui ne transmettent par les données relatives au soin sont susceptibles d'une sanction administrative (CSP, art. L. 6113-7, al. 8).

[1560]Opposition ancienne puisque dans son ouvrage sur la jurisprudence de la médecine en France publié en 1763, Jean Verdier expliquait « *Autrefois, la plûpart des crimes demeuroient impunis, par l'asile que trouvoient les coupables dans les lieux sacrés. Pour pallier cet abus, les anciennes Ordonnances prescrivoient aux Chirurgiens et Barbiers, d'avertir le Prévôt de Paris, des bléssés qu'ils y auroient pansé. Le même devoir est renouvellé pour les Chirugiens, par un grand nombre d'Ordonnance, et des Status qui leur enjoignent d'avertir les Commissaires du Châtelet, des blessées qu'ils auront pansés dans les 24 heures, sous peine d'amende et d'interdiction, et plusieurs ont été punis pour n'y avoir satisfait* » (J. VERDIER, *Essai sur la jurisprudence de la medecine en France, ou Abregé historique et juridique des etablissemens, reglemens, police, devoirs, fonctions, récompenses, honneurs, droits, & privilèges des trois corps de médecine ; avec les devoirs, fonctions et autorité des juges à leur égard*, Malassis le jeune, Prault père, 1763, p. 288-289). L'édit de 1666 prévoyait par exemple cette obligation pour les chirurgiens qui auraient pansé des individus blessés lors de duels. Par les ordonnances des 17 ventôse an IX, 16 mars 1805 et 26 aout 1806, « *la législation d'Ancien Régime sur les limites posées au secret au nom de l'ordre public fut renouvelée durant la Révolution et l'Empire* » (A. LECA et J.-C. CAREGHI, « Le secret médical, au crible d'une analyse historique », *Les cahiers de droit de la santé du Sud-Est* 2012, Actes du XI[e] colloque du centre de droit de la santé d'Aix-Marseille, 30 novembre 2011, *Le secret médical*, n° 15, p. 15, spéc. p. 17).

[1561] Outre l'aspect relatif à la sécurité publique, la psychiatrie est largement sollicitée par le juge judiciaire et particulièrement en matière pénale puisque les troubles mentaux peuvent constituer une cause personnelle d'irresponsabilité pénale. Dans ce cas, il est fait appel à des experts spécialement mandatés, leur mission ne constitue pas un acte de soin : « *L'expert judiciaire a pour mission de rendre compte de ses constatations à l'autorité judiciaire qui l'a commis. Ce faisant, il ne s'expose pas lui-même à se voir reprocher une violation du secret professionnel, en rapportant des informations, fussent-elles de nature secrètes. Il n'est pas un confident de la personne expertisée mais un professionnel investi d'une mission de justice* » (B. PY, *Rep. pén.*, *V°* « Secret professionnel », fév. 2003, act. fév. 2017). Par ailleurs le médecin psychiatre tient un rôle tant au stade de la mise

mentaux constituent, au sein de notre société, des sources de risque pour les personnes et pour l'ordre public. Aussi, le pouvoir étatique s'est-il toujours préoccupé d'identifier ces malades afin de pouvoir les surveiller[1562]. Les obligations de révéler faites aux médecins quant à l'existence de pathologies psychiatriques, si elles ne sont pas nombreuses, sont régulièrement au cœur des débats. Le secret professionnel est alors présenté, au gré des faits divers, comme un ennemi de la sécurité des personnes[1563]. L'enjeu est d'autant plus important lorsque ce sont des personnes condamnées qui sont atteintes de ces troubles. L'enfermement agit comme catalyseur des suspiscions à l'égard du secret professionnel des soignants intervenant en établissement pénitentiaire. L'on sait que de nombreuses personnes détenues souffrent de troubles psychiatriques, qui sont parfois développés à l'occasion de l'enfermement[1564]. Ils

---

en œuvre de la sanction pénale que de sa détermination (sur ce point v. J.-P. VAUTHIER, *Le psychiatre et la sanction pénale*, Thèse dact., ss. la dir. de B. PY, soutenue le 13 déc. 2013, Université de Lorraine).

[1562] M. FOUCAULT, *Surveiller et punir*, Gallimard, 1975. A propos d'un fichier automatisé que nous évoquerons ultérieurement, Bruno Py explique le processus actuel au regard de la pensée de Michel Foucault : « *Foucault développe l'idée d'un système de police et de quadrillage de la population sur le modèle de la surveillance au temps de la peste. Le fou et le délinquant représentent le mal social, le modèle qui en résulte est donc logiquement calqué sur le modèle de l'épidémie. Il faut repérer les porteurs du mal, pour les surveiller, voire les enfermer* » (B. PY, « Ficher les fous. Au sujet du traitement automatisé de données à caractère personnel dénommé « Redex » (répertoire des expertises) », *RDS* juillet 2018, n° 84, p. 611.

[1563] En référence à l'exemple précédemment évoqué : A propos de l'écrasement de l'avion A320 de la Germanwings provoqué par son pilote qui souffrait de troubles psychiatriques, la question s'est rapidement posée d'obliger les médecins de pilotes de vols commerciaux de révéler les affections d'ordre psychiatrique dont ces derniers pouvaient souffrir (Question écrite sur la possibilité de lever le secret médical pour certaines professions à risque 14e législature n° 15605 de M. Alain Houpert, *JO Sénat* du 2 avril 2015, p. 726). C'est d'ailleurs la demande qui avait été faite par le Bureau d'enquêtes et d'analyses pour la sécurité de l'aviation civile dans son rapport (Rapport final, Accident survenu le 24 mars 2015 à Prads-Haute-Bléone (04) à l'Airbus A320-211 immatriculé D-AIPX exploité par Germanwings, spéc. p. 114). Concernant enfin le terrorisme, la question d'obliger les médecins et notamment les psychiatres à collaborer avec le ministère de l'intérieur et les services de police est régulièrement remise à l'ouvrage. A la suite de l'attentat de Barcelone du 17 août 2017, Gérard Collomb, alors ministre de l'intérieur, avait évoqué une telle possibilité, provoquant de vives réactions de la part des psychiatres et du corps médical qui rappelant qu'il n'y avait pas de lien entre maladie mentale et terrorisme (CNOM, *Risque terroriste et secret professionnel du médecin*, janvier 2017 ; D. GOURION, « Terrorisme : « les psychiatres n'ont pas vocation à collaborer avec le ministère de l'intérieur », *Le Monde*, 21 août 2017).

[1564] Les rapports et études sur ces questions sont nombreux, de manière non exhaustive et concernant uniquement la France, l'on peut citer : B. FALISSARD (dir.), *Enquête de prévalence sur les troubles psychiatriques en milieu carcéral*, Étude pour le ministère de la Santé (Direction générale de la santé) et le ministère de la Justice (Direction de l'administration pénitentiaire), décembre 2004 ; « Étude épidémiologique sur la santé mentale des personnes détenues en prison », *Expertise psychiatrique pénale*, Rapport de la commission d'audition, 25-26 janvier 2007 ; G. BARBIER, C. DEMONTÈS, J.-R. LECERF et J.-P. MICHEL, *Prison et troubles mentaux : Comment remédier aux dérives du système français ?*, Rapport d'information n° 434 (2009-2010) fait au nom de la commission des lois et de la commission des affaires sociales, déposé le 5 mai 2010 ; L. PLANCKE, A. SY, T. FOVET, F. CARTON, J.- L. ROELANDT, I. BENRADIA, A. BASTIEN, A. AMARIEI, T. DANEL, P. THOMAS, « La santé mentale des personnes entrant en détention », Lille, F2RSM Psy, novembre 2017 ; Rapport n° 808 en conclusion des travaux des groupes de travail sur la détention, *Repenser la prison pour mieux réeinsérer*, Assemblée nationale, 21 mars 2018.

présentent alors un risque *a priori* difficilement prévisible pour l'administration pénitentiaire tant pour la sécurité des établissements[1565] que pour eux-mêmes[1566]. Sous l'angle de la *dangerosité*, leur état mental intéresse encore pour *prévoir* les risques de récidive[1567]. Le traitement des données relatives à la santé des détenus peut alors servir efficacement la sécurité carcérale et l'ordre public.

[1565] Les médecins sont régulièrement sollicités afin de délivrer des informations, par exemple dans le cadre du prononcé d'une mise à l'isolement, un décret qui avait fait l'objet d'une annulation par le Conseil d'Etat (CE, 31 oct. 2008, n° 293785) prévoyait que le prolongement de l'isolement pouvait avoir lieu sur décision du directeur interrégional des services pénitentiaires après avis du médecin. Si le moyen tiré de la violation du secret professionnel n'est pas celui retenu par le Conseil d'Etat, la confusion des rôles du médecin, selon qu'il soigne ou qu'il revêt un statut d'expert, à été mise en exergue (Sur ce point v. M. HERZOG-EVANS, « Isolement carcéral : un arrêt du Conseil d'Etat révolutionnant les sources du droit pénitentiaire », *D.* 2009, p. 134). La tension entre la sécurité carcérale et le secret professionnel est constante, en témoigne notamment l'instauration de la commission pluridisciplinaire unique (CPU) qui a notamment vocation de permettre une évaluation de la *dangerosité* des détenus (Circulaire du 18 juin 2012, relative aux modalités de fonctionnement de la commission pluridisciplinaire unique, NOR : JUSK1140048C). En milieur fermé (CPP, art. D. 90), il s'agit d'instaurer une forme de « secret partagé » (M. MEDJKANE, « Le partage des informations à caractère secret », *AJ pénal* 2017, p. 371 ; A. BONNE-HARBIL, *Les droits de la personne détenue en matière de santé*, thèse dact., ss. la dir. de B. PY, soutenue le 12 déc. 2016, n° 195 et svt) entre les différents intervenants du parcours d'execution de la peine. Est ainsi invité à y participer « *un représentant des équipes soignantes de l'unité de consultations et de soins ambulatoires ou du service médico-psychologique régional désigné par l'établissement de santé de rattachement* » (*Ibid.*).

[1566] La France a été condamnée à plusieurs reprises par la CEDH pour violation de l'article 2 de la Convention à la suite de suicides de détenus (CEDH, 16 oct. 2008, n° 5608/05, *Renolde* c/ *France* ; *AJDA* 2008, p. 1983 ; *AJ pénal*, p. 609, obs. J.-P. CERE ; *D.* 2008, p. 2723, obs. M. LENA ; *ibid.* 2009, p. 123, obs. G. ROUJOU DE BOUBEE, T. GARE et S. MIRABAIL ; *ibid.*, p. 1376, obs. J.-P. CERE, M. H-EVANS et E. PECHILLON ; *AJ pénal* 2009, p. 41, obs. J.-P. CERE ; *RDSS* 2009, p. 363, obs. P. HENNION-JACQUET ; *RSC* 2009, p. 173, obs. J.-P. MARGUENAUD ; *ibid.,* p. 431, chron. P. PONCELA ; CEDH, 19 juill. 2012, n° 38447/09, *Ketreb c/ France*, *AJ pénal* 2012, p. 609, obs. J.-P. CERE ; CEDH, 8 oct. 2015, n° 32432/13 *Sellal c/ France* ; CEDH, 4 févr. 2016, n° 58828/13*, Isenc c/ France*, *AJDA* 2016, p. 232 ; *D.* 2016, p. 1220, obs. J.-P. CERE, M. HERZOG-EVANS et E. PECHILLON ; *AJ pénal* 2016, p. 158, obs. J.-P. CERE). La détection des populations pénales présentant un risque pour elles-mêmes est donc devenue un enjeu important pour l'administration pénitentiaire (A. HENRY « Un suicide qui dérange : le suicide en prison », *AJ pénal* 2010, p. 437 ; V. VIOUJAS, « Les soins psychiatriques aux détenus : des modifications mineures pour une problématique de santé publique majeure », *RDSS* 2011, p. 1071). Les CPU font alors double emploi puisqu'elles sont également instituées pour évaluer la vulnérabilité des détenus (Circulaire du 18 juin 2012, relative aux modalités de fonctionnement de la commission pluridisciplinaire unique, *op. cit.*).

[1567] Dans cette optique la psychiatrie et, du fait des progrès de la science, les neurosciences, sont mobilisées (sur la place des neurosciences dans le droit pénal, v. M. PELTIER-HENRY, *Le droit pénal et les neurosciences*, thèse en cours, ss. la dir. de B. PY, Université de Lorraine; sur la place de la psychiatrie dans l'évaluation de la dangerosité dans le but de prévoir la récidive v. notamment *AJ pénal* 2012, numéro spécial n° 2, *Prévenir la récidive, évaluer la dangerosité* ; P.-J. DELAGE, « La dangerosité comme éclipse de l'imputabilité et de la dignité », *RSC* 2007, p. 797 ; C. LAZERGES, « Le choix de la fuite en avant au nom de la dangerosité : les lois 1, 2, 3, 4, 5, etc. sur la prévention et la répression de la récidive », *RSC* 2012, p. 274 ; Sur la notion de dangerosité : A. COCHE, *La détermination de la dangerosité des délinquants en droit pénal. Etude de droit français*, PUAM, 2005 ; On peut encore mentionner la prise en charge pluridisciplinaire de la population pénale *radicalisée* dans laquelle la psychiatrie tient une place importante (F. HABOUZIT, « L'usage de la notion de radicalisation dans le champ pénitentiaire (suite) : Existe-t-il un statut *sui generis* des personnes « radicalisées » ? », *RSC* 2018, p. 541).

336. Le traitement des données de santé des détenus, les « *outils de communication* ». La commission pluridisciplinaire instituée par un décret[1568] portant application de la loi pénitentiaire[1569] est un « *outil de communication* »[1570] devant favoriser le partage d'informations entre les professionnels de santé et le personnel pénitentiaire[1571]. La permission de révéler offerte aux soignants des unités de consultation et de soins ambulatoires (UCSA) et des services médico-psychologiques régionaux (SMPR) par le décret a provoqué de vives réactions de la part de ces derniers. Le Conseil national de l'ordre des médecins a d'ailleurs appelé ses membres à ne pas se rendre aux réunions[1572]. Le guide méthodologique prévoyant les modalités d'échange d'information « […] *a eu pour conséquence de dissuader les médecins de participer aux commissions pluridisciplinaires uniques* »[1573], et a en outre fait l'objet d'un recours pour excès de pouvoir introduit par l'Observatoire international des prisons qui a argué, entre autres, d'une atteinte au « secret médical »[1574]. Ce premier *outil de communication*

[1568] Décret n° 2010-1635 du 23 décembre 2010 portant application de la loi pénitentiaire et modifiant le Code de procédure pénale (troisième partie : Décrets), *JORF* n° 0300 du 28 décembre 2010, p. 22796, texte n°13, art. 7.
[1569] Loi n° 2009-1436 du 24 novembre 2009, *JORF* n° 0273 du 25 novembre 2009 p. 20192.
[1570] Circulaire interministérielle du 30 octobre 2012 relative à la publication du guide méthodologique sur la prise en charge sanitaire des personnes placées sous main de justice, NOR : AFSH1238354C.
[1571] « *La qualité de la prise en charge sanitaire des personnes détenues repose sur une dynamique partenariale entre les acteurs concernés du monde de la santé et de la justice. Ce partenariat, indispensable pour un bon fonctionnement, doit pouvoir s'instaurer en dépassant les clivages issus de cultures et d'approches différentes et dans le respect des domaines de compétences et des cadres professionnels de chacun* » (*Ibid.*).
[1572] CNOM, « Prisons : Menace sur le secret médical », *Bulletin d'information de l'ordre national des médecins*, n° 18, juill.-août 2011, p. 22.
[1573] Contrôleur général des lieux de privation de liberté, *Rapport d'activité 2013*, p. 132. « *Par crainte d'éventuelle pressions exercées par le personnel pénitentiaire pour obtenir des informations à caractère médical, les médecins justifient leur refus par des raisons tenant à la préservation du secret professionnel du médecin* » (A. BONNE-HARBIL, *Les droits de la personne détenue en matière de santé*, *op. cit.*, n° 196).
[1574] CE, 22 oct. 2014, n° 362681 ; *AJ pénal* 2014, p. 595, obs. E. PECHILLON ; *RPDP* 2014, p. 891, obs. E. PECHILLON. Afin d'expliquer cet arrêt, nous avons repris, en partie, des développements que nous avions rédigé à l'occasion de son commentaire (V. OLECH, « Soins médicaux en milieu carcéral : confusion des rôles et partage des secrets », *RDS* 2015, n° 63, Pp. 96-99.) : Sur la légalité externe, l'OIP avait soulevé l'incompétence des auteurs de la circulaire, invoquant le caractère règlementaire de celle-ci. Ce moyen est écarté par le Conseil d'Etat pour qui cette circulaire ne fait que préciser « *l'interprétation qu'il convient d'adopter des dispositions régissant les informations susceptibles d'être partagées entre professionnels de santé* […] *et professionnels de l'administration pénitentiaire et de la protection judiciaire de la jeunesse* », ainsi que les modalités selon lesquelles les professionnels de santé doivent participer à la CPU. Il est toutefois permis de douter de cette analyse puisque la circulaire en question pose bel et bien le cadre d'un « secret partagé » entre professionnels de santé et agents de l'administration pénitentiaire. Ce partage n'est prévu ni par la loi, ni par le décret du 23 décembre 2010. La lecture de la circulaire suffit à s'en convaincre puisque celle-ci contient un tableau intitulé « partage de l'information opérationnelle entre les acteurs pénitentiaires et les acteurs de santé », dans lequel on trouve une liste importante d'informations concernant la santé des patients détenus et les modalités de leur partage. D'emblée, le terme « informations opérationnelles » interroge. Y aurait-il donc des informations couvertes par le secret et des informations opérationnelles qui, elles, pourraient, ou devraient, être communiquées ? Au titre de la légalité

s'accompagne d'un fichier informatisé constituant un traitement de données à caractère personnel : le cahier électronique de liaison (CEL). Celui-ci constitue un module intégré à un traitement de données à caractère personnel relatif à la gestion informatisée des détenus en établissement (GIDE) crée par un décret du 6 juillet 2011[1575]. La CNIL a rendu un avis[1576]

---

interne, l'OIP invoquait une atteinte illégale au *secret médical*. Elle arguait, entre autres, de ce que la circulaire prévoyait le partage de la découverte de « maladies à déclarations obligatoire ou maladies contagieuses » dans le cadre des CPU. Si les articles D. 3113-6 et D. 3113-7 du Code de la santé publique dressent la liste des maladies à déclaration obligatoire, le terme de « maladies contagieuses » est bien plus large. La loi n'impose, ni même ne permet de telles révélations (sauf dans de rares cas, comme par exemple pour la grippe), qui pourraient avoir des conséquences désastreuses pour les patients détenus. Pour rester dans la limite de ce que prévoit la loi, la formulation « *maladies contagieuses à déclaration obligatoire* » aurait peut-être été préférable. Dans de tels contextes, l'emploi d'un mot ou d'un autre revêt une importance considérable. Un autre argument soulevé par l'OIP concernait le signalement par les professionnels de santé, lors des réunions des CPU, de l'existence de « *risques sérieux pour la sécurité des personnes* ». L'article L. 6141-5 du Code de la santé publique, prévoit bien une exception au secret professionnel dans cette hypothèse encore que, selon la loi, le destinataire de l'information est le directeur de l'établissement, ce que rappelle d'ailleurs le Conseil d'Etat. Dans le cadre de la circulaire, le directeur d'établissement n'est donc plus le seul destinataire de cette information, qui devrait maintenant être communiquée lors des réunions de la commission. La haute juridiction administrative balaie l'argument en rappelant qu'il ne s'agit là que d'une possibilité (donc d'une permission de révéler), qu'elle découle de l'obligation des services publics pénitentiaires d'assurer la protection effective de l'intégrité physique des personnes détenues et qu'il appartient au directeur de veiller à ce qu'elles ne soient communiquées, lors des CPU, qu'aux seules personnes ayant besoin d'en disposer pour accomplir leurs missions. Plusieurs observations s'imposent : d'abord, on ne peut que constater que l'on est passé d'une obligation d'information au directeur d'établissement à une possibilité de partage d'informations, ce qui constitue une extension de la portée du fait justificatif. D'un point de vue pratique, on imagine mal comment se déroulerait une commission dont il faudrait faire sortir certains membres dès lors que le professionnel de santé prendrait la parole. Sur quels critères serait-il décidé que l'un ou l'autre n'a pas besoin d'avoir accès à des informations qui concerneraient sa propre sécurité ? L'application d'une telle mesure paraît difficile à mettre en œuvre. La circulaire prévoyait, en outre, que doivent être signalés, dans le cadre des CPU, les cas de maltraitance avec l'accord de la personne majeure. Cette exception figurant dans le Code pénal est d'ailleurs rappelée par le Conseil d'État. L'article 226-14 du Code pénal prévoit la permission de révéler pour le médecin « *qui, avec l'accord de la victime, porte à la connaissance du procureur de la République les sévices ou privations qu'il a constatés* ». Le destinataire n'est donc plus le procureur de la République mais l'ensemble des membres de la CPU. Le Conseil d'État considère une fois encore qu'il ne s'agît là que d'une possibilité pour le soignant et qu'en conséquence, il n'y a pas d'atteinte illégale au secret professionnel. En conclusion, il faut rappeler une fois encore que le secret professionnel médical est institué dans l'intérêt du patient et non des tiers dont le personnel pénitentiaire fait partie. Il s'impose au médecin et ne concerne pas uniquement les informations de nature médicale ou ayant trait au diagnostic, le Code de déontologie médicale énonce à l'article R. 4127-4 CSP que « *le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris.* » C'est pourquoi, bien qu'il soit compréhensible, dans une certaine mesure, que les professionnels de santé partagent des informations nécessaires à l'adaptation des conditions de détention des détenus ou relatives à la réalisation des visites médicales réglementaires, il semble dangereux d'admettre qu'une circulaire puisse fixer le cadre de ce partage et les informations qu'il concerne.

[1575] Décret n° 2011-817 du 6 juillet 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion informatisée des détenus en établissement (GIDE), *JORF* n° 0157 du 8 juillet 2011 p. 11842. GIDE est un fichier ayant pour but le suivi du détenu pendant sa détention, l'un des objectifs est notamment de prévenir les suicides des détenus et d'assurer leur sécurité ainsi que celle des agents des services pénitentiaires. Pour ce faire, le décret GIDE prévoit que les membres du personnel soignant renseignent le CEL, fichier intégré au GIDE qui permet de gérer l'accueil des détenus, le traitement de leurs requêtes ainsi que leur accompagnement et orientation, et dont l'accès est ouvert à une liste de personnes prévue par le décret.

[1576] Conformement aux anciens article 8 et 26 de la LIL. Le premier portant sur les données sensibles et le second prévoyant que les traitements « *qui portent sur des données mentionnées au I de l'article 8 sont autorisés par*

concernant le projet de décret autorisant le traitement. Constatant qu'il est prévu un accès au CEL lors des réunions pluridisciplinaires[1577], elle a estimé que les données relatives à la santé ne devaient pouvoir être consultées qu'en présence d'un représentant de l'équipe de soins[1578]. Elle a également souhaité « *qu'il appartienne à ces personnels médicaux de déterminer librement les données qui pourront être communiquées au cours de la CPU, compte tenu de la présence de personnels non médicaux* »[1579]. Tandis que l'outil constitué par la commission pluridisciplinaire unique impliquait une autorisation de révéler des informations, le CEL ne nécessite plus que le soignant *parle* mais simplement qu'il enrichisse le fichier. L'accès au CEL permis lors de CPU s'apparente à un partage des informations au sens du Code de la santé publique[1580].

337. De la permission de révéler au partage, au profit de la sécurité carcérale : Panoptisme numérique[1581] ? Le passage d'une permission de révéler des informations précises à une personne identifiée en raison d'un contexte précis, tel que le prévoit par exemple l'article 226-14 du Code pénal, à progressivement cédé la place à une logique de partage des informations. Ce glissement n'est pas anodin. Si la CNIL a pu souhaiter qu'un certain nombre de précautions soient prises afin d'éviter les accès aux informations relatives à la santé traitées

---

décret en Conseil d'Etat pris après avis motivé et publié de la commission ; cet avis est publié avec le décret autorisant le traitement ».

[1577] « *Aux termes de l'article 90 du code de procédure pénale, la CPU est présidée par le chef d'établissement. Elle comprend en outre, le directeur du service pénitentiaire d'insertion et de probation, un responsable du secteur de détention du détenu dont la situation est examinée, un représentant du service du travail, un représentant du service de la formation professionnelle, et un représentant du service d'enseignement* » (Délibération n° 2011-021 du 20 janvier 2011 portant avis sur un projet de décret en Conseil d'Etat portant création d'un traitement de données à caractère personnel relatif à la gestion des personnes écrouées dénommé « gestion informatisée des détenus en établissement » (GIDE) (avis n° 10024143)).

[1578] « *Elle estime que les données relatives à la santé du détenu ne devraient être examinées que dans la mesure où ont été convoqués les personnes énumérées à l'article D.90 du code de procédure pénale, à savoir le psychologue en charge du parcours d'exécution de la peine, un représentant des équipes soignantes de l'unité de consultations et de soins ambulatoires ou du service médico-psychologique régional désigné par l'établissement de santé de rattachement* » (*Ibid.*).

[1579] *Ibid.*

[1580] Le partage *« consiste à mettre à disposition de catégorie de professionnels fondés à en connaître des informations dans les conditions prévues au présent code, respectant les conditions de confidentialité et de sécurité* » (Arrêté du 25 novembre 2016 fixant le cahier des charges de définition de l'équipe de soins visée au 3° de l'article L. 1110-12 du code de la santé publique, Annexe, *JORF* n°0280 du 2 décembre 2016).

[1581] Developpant l'idée d'un panoptisme généralisé à l'echelle de la société (nous précisons que l'article autant que la revue défendent une position axiologique qui n'est pas neutre, la revue étant celle du *mouvement anti-utilitariste dans les sciences sociales*. Nous n'en partageons pas l'entier point de vue) : Ch. LAVAL, « Surveiller et prévenir. La nouvelle société panoptique », *Revue du MAUSS* 2012/2, n° 40, p. 47.

au sein du CEL hors la présence d'un professionnel de santé, le décret du 6 juillet 2011 a fait l'objet d'un recours pour excès de pouvoir formé, entre autres, par le Conseil national de l'ordre des médecins[1582].

Le CNOM contestait notamment la légalité du décret en ce que le CEL portait une atteinte illégale au « secret médical » tel que prévu à l'article L. 1110-4 du Code de la santé publique. Etait visé le fait que le cahier électronique comporte une rubrique « *entretien avec les services médicaux* » dans laquelle se trouvent des items[1583] auxquels les professionnels de santé sont invités à répondre par oui/non/ne ne se prononce pas. Le Conseil d'Etat affirme, sur ce point, la légalité du décret. Il rappelle d'abord que les alinéas 3 et 4 de l'article L. 6141-5 du Code de la santé publique prévoient une exception au secret professionnel médical et que, dès lors qu'il existe « *un risque sérieux pour la sécurité des personnes au sein des établissements publics de santé destinés à l'accueil des personnes incarcérées ou des établissements pénitentiaires, les personnels soignants ayant connaissance de ce risque sont tenus de le signaler dans les plus brefs délais au directeur de l'établissement en lui transmettant, dans le respect du secret médical, les informations utiles à la mise en œuvre des mesures de protection* ». Plusieurs remarques sont à faire sur ce point : Si la loi prévoit une obligation de révéler, celle-ci semble particulièrement encadrée. Il s'agit en effet de révéler au « *directeur de l'établissement pénitentiaire* » les « *informations utiles* » concernant un « *risque sérieux* ». Or, on constate que ce qui est prévu par le décret dépasse largement ce cadre tant au niveau des

[1582] Deux requêtes ont été formées puis jointes, contre ce même décret : CE 11 avr. 2014, n° 352473, *Ligue des droits de l'homme et autres* ; CE 11 avr. 2014, n° 355624, *Union générale des syndicats pénitentiaires CGT [UGSP-CGT]* ; *AJ pénal* 2014, p. 255, obs. M. Herzog-Evans ; *JCP Adm.* 2014, Act., p. 373 ; *RDS* 2014, n° 60, Pp. 1455-1458, comm. O. Valérie.

[1583] « *Antécédents placement SMPR (services médicaux psychologiques régionaux), antécédents placement UMD (unités pour malades difficiles), antécédents d'hospitalisation d'office, nécessite un suivi somatique, suivi psychologique ou psychiatrique antérieur ou en cours, régime alimentaire particulier, grève de la faim ou de la soif, prescription d'une douche médicale, automutilations graves, fumeur, addictions, aptitude au sport, aptitude au travail* » (*Ibid.*).

destinataires de l'information[1584], que de la nature des informations[1585]. Quant à la notion de « risques sérieux », elle disparaît, il est désormais question de renseigner le CEL pour *tous* les détenus. Sur le fondement de l'article D. 382 du Code de procédure pénale, le Conseil d'Etat rappelle encore que les médecins « *délivrent aux autorités pénitentiaires des attestations écrites contenant les renseignements strictement nécessaires à l'orientation du détenu ainsi qu'aux modifications ou aux aménagements du régime pénitentiaire que pourrait justifier son état de santé* »[1586]. Le Conseil d'Etat précise encore que le nombre important de personnes ayant accès aux informations se justifie par l'accès limité au besoin qu'ils ont d'en connaître dans le cadre de leurs missions. Il n'en demeure pas moins que l'on est bien loin du cadre des révélations autorisées ou obligées par les textes mentionnés. La Haute Juridiction indique enfin que la collecte des données de santé n'entache pas le décret d'illégalité dès lors qu'elle ne comporte aucune « *motivation médicale* » mais, faut-il le rappeler, cela ne libère en rien le médecin de son obligation au secret puisque les informations couvertes par celui-ci n'ont pas uniquement trait à la santé du patient ou au diagnostic médical. Enfin, il est expliqué que les restrictions apportées au « secret médical » sont nécessaires à la protection de l'intégrité de la personne détenue et du personnel pénitentiaire, mais également à l'individualisation des peines et du régime de détention. C'est sans doute cette affirmation qu'il importe de retenir : le décret met en place une dérogation au « secret médical » et l'utilisation du CEL est justifiée par un intérêt légitime qui n'est pas uniquement celui des détenus, d'autant que la consultation du CEL est possible durant la commission pluridisciplinaire unique, laquelle a également vocation à

[1584] La CNIL regrettait d'ailleurs que la liste des destinataires des informations contenues dans le module CEL du GIDE soit très étendue (un autre module qui ne concerne pas notre étude était également intégré au traitement de donné) : *« A titre de remarque liminaire, la Commission relève que les deux nouveaux modules ont été expérimentés sans que son avis préalable ait été recueilli comme le prévoit la loi du 6 janvier 1978 modifiée en août 2004. Les modifications qui lui sont soumises étendent considérablement les destinataires, ainsi que la liste des données, dont certaines relèvent de la catégorie des données sensibles énumérée à l'article 8 de la loi informatique et libertés* » (Délibération n° 2011-021 du 20 janvier 2011 portant avis sur un projet de décret en Conseil d'Etat portant création d'un traitement de données à caractère personnel relatif à la gestion des personnes écrouées dénommé « gestion informatisée des détenus en établissement » (GIDE) (avis n° 10024143)).

[1585] « *La Commission considère que les observations du personnel médical ne devraient pas être portées dans le CEL dès lors qu'elles peuvent relever du secret médical et figurer dans le dossier médical du détenu. Seules les prescriptions médicales devraient figurer dans le CEL sans pouvoir être consultables sans habilitation spécifique du chef de l'établissement et dans la seule mesure où cela correspond à une nécessité* » (*Ibid.*). S'il semble avoir été en partie tenu compte des remarques de la CNIL en ce que le décret prévoyait finalement que les professionnels de santé appelés a renseigner le CEL devaient simplement apporter des réponses fermées, la question des habilitations est plus problématique dès lors que sa consultation est possible durant les CPU.

[1586] CPP, art. D. 382, al. 3.

évaluer la *dangerosité* des détenus. L'utilisation conjointe des *outils de communication* permet un glissement subtil d'une obligation ponctuelle de révéler, vers un partage étendu des informations couvertes par le secret. La mise en œuvre du traitement GENESIS par un décret du 30 mai 2014[1587] a permis de remplacer le précédent traitement. Dans son avis, la CNIL a relevé que les données traitées dans GENESIS étaient similaires à celles traitées dans GIDE[1588]. Elle a aussi remarqué que les destinataires étaient nombreux, bien qu'ils soient, pour la plupart, déjà destinataires des données contenues dans le précédent traitement[1589]. Le décret a fait l'objet d'un recours pour excès de pouvoir sur requête du Conseil national de l'Ordre des médecins. A cette occasion, la violation du « secret médical » a encore été alléguée, mais l'annulation partielle n'a été prononcée qu'à raison de la disproportion de la durée de conservation des données[1590]. L'argument invoqué par le CNOM ne pouvait aboutir dès lors que les données traitées dans le CEL étaient identiques à ce que prévoyait le décret précédent, de même que la liste des destinataires. Il s'agissait sans doute pour le Conseil de tenter de faire obstacle, une fois encore, aux outils que sont le CEL et la CPU. A propos du premier, la CNIL a d'ailleurs relevé que si « *le CEL est présenté par l'administration comme ayant pour finalité une prise en charge individualisée permettant la mise en œuvre d'un parcours de détention adapté à chaque détenu, elle considère toutefois que ce dernier poursuit une double finalité : la prévention des comportements à risques et la prévention des éventuelles mises en cause de la responsabilité de l'administration* »[1591]. Cet aveu a sans doute motivé les actions du CNOM : l'inquiétude tient à l'utilisation qui est faite, dans la pratique, des informations partagées. En définitive, la transparence de l'informatique est notable, l'intérêt du traitement des données n'est pas discuté, il *s'incorpore* à l'intérêt hiérarchiquement supérieur, au détriment du secret professionnel.

[1587] Décret n° 2014-558 du 30 mai 2014 portant création d'un traitement de données à caractère personnel relatif à la gestion nationale des personnes détenues en établissement pénitentiaire, *JORF* n° 0125 du 31 mai 2014, p. 9066.

[1588] Délibération n° 2013-405 du 19 décembre 2013 portant avis sur un projet de décret portant création d'un traitement de données à caractère personnel relatif à la gestion nationale des personnes détenues en établissement pénitentiaire dénommé GENESIS (avis n° 13032517).

[1589] « *Si ces destinataires peuvent apparaître nombreux et divers, il convient de relever que, pour la plupart, ils figurent dans le décret du 6 juillet 2011, d'une part, et correspondent aux différents intervenants en prison ou dans le processus de mise à exécution d'une décision judiciaire, d'autre part.*
La commission considère toutefois que le nombre et la diversité des destinataires du traitement imposent la mise en œuvre de mesures adaptées de nature à garantir des accès restreints aux seules données strictement nécessaires à l'accomplissement de leurs missions » (*Ibid.*).

[1590] CE, 9 nov. 2015, n° 383313 ; *AJDA* 2016, p. 527.

[1591] Délibération n° 2011-021 du 20 janvier 2011 portant avis sur un projet de décret en Conseil d'Etat portant création d'un traitement de données à caractère personnel relatif à la gestion des personnes écrouées dénommé « gestion informatisée des détenus en établissement » (GIDE) (avis n° 10024143).

§ 2 - Evolution du rôle du consentement de la personne concernée

338. Le rôle du consentement de la personne comme justification à la violation du secret professionnel paraît être contradiction avec le mouvement qui s'opère dans la législation relative au traitement des données à caractère personnel **(B)**, pour le comprendre, il faut au préalable s'attarder sur la place du consentement de la victime du délit de violation du secret professionnel **(A)**.

A - Considérations d'ordre général

339. Le consentement justificatif en droit pénal. Le rôle de la volonté de la victime dans la détermination des infractions est classiquement étudié en droit pénal général au sein des développements consacrés aux causes objectives d'irresponsabilité dans le cadre de l'étude de l'infraction ou de la responsabilité pénale[1592]. Le refus ou non d'admettre le consentement comme cause justificative de l'infraction dépend de la théorie de l'infraction que l'on adopte.

[1592] La doctrine pénaliste a proposé diverses constructions des causes de justification. La doctrine classique considère que la justification consiste dans la disparition de l'élément légal (R. MERLE et A. VITU, *Traité de droit criminel*, 4ème éd., t. 1, Editions Cujas, n° 396 ; P. CONTE , P. MAISTRE DU CHAMBON et J. LARGUIER, *Droit pénal général*, 23ème éd., coll. Mémentos, Dalloz, 2018, p. 40 ; B. BOULOC, *Droit pénal général*, coll. Précis, Dalloz, 25e éd., n° 408) c'est la conception légaliste traditionnellement admise. Une partie de la doctrine refuse d'admettre l'élément légal comme un élément constitutif de l'infraction (X. PIN, *Droit pénal général*, 11ème éd., coll. Cours Dalloz, série Droit privé, 2019, n° 226) ; pour certains auteurs les faits justificatifs sont alors un obstacle à la qualification de l'infraction car le fait justificatif rend l'acte incriminé licite, d'autres considèrent encore que l'absence de causes justificatives objectives est un élément négatif de l'infraction (M.- L. RASSAT, *Droit pénal* général, 4ème éd., coll. Cours magistral, ellipses, 2017,p. 364 ; E. DREYER, *Droit pénal général*, 5e éd., 2019, LexisNexis, n° 1226 et svt. ; Y. MAYAUD, *Droit pénal général*, coll. Droit fondamental, 6e éd., PUF, 2018, n° 400), il s'agit d'une conception négative de l'élement injuste. Certaines constructions sont parfois *hybrides*, il est donc difficile d'en dresser un panorama complet. Mais la question qui sous-tend ces conceptions tient à la reconnaissance ou non de l'existence d'un élément injuste comme élément de l'infraction (qu'il soit nié, selon une vision légaliste ou qu'il soit admis comme élément négatif). Xavier Pin explique par ailleurs que s'il est encore entendu négativement, « *il est possible de présenter l'élément injuste également avec un contenu positif, en avançant que l'infraction n'est constituée que si le fait incriminé* porte atteinte à un intérêt protégé. *Cette présentation théorique axiologique est rarement suivie dans notre pays de tradition plutôt légaliste mais elle correspond pourtant à la réalité, puisque l'agent peut toujours contester, devant les tribunaux, le caractère illicite de son geste, en démontrant soit que l'intérêt protégé n'a pas été lésé, soit que son geste était justifié par la sauvegarde d'un intérêt supérieur, sous la forme d'une immunité ou d'un fait justificatif* » (X. PIN, *Droit pénal général*, coll. Cours, 10e éd., Dalloz, n° 218 ; M. LACAZE, *Réflexions sur le concept de bien juridique protégé par le droit pénal*, LGDJ-Fondation Varenne, t. 39, 2010 ; J. WALTHER, *L'antijuridicité en droit pénal comparé franco-allemand*, Thèse dact., ss. la dir. de J.- F. SEUVIC et H. JUNG, soutenue le 28 juin 2003, Université de Nancy II, p. 152 et svt). Une analyse complète de ces conceptions des causes justificatives a été proposée par Julien Walther, dans sa thèse portant sur l'antijuridicité en droit pénal comparé franco-allemand (J. WALTHER, *L'antijuridicité en droit pénal comparé franco-allemand*, *op. cit.*).

Si l'on considère que le fait infractionnel ne peut être qualifié que s'il est injuste – c'est-à-dire que l'on reconnaît l'élément injuste comme un élément de l'infraction –, il est alors possible de s'interroger sur la place du consentement de la victime dans la mesure où celui-ci empêcherait la lésion de l'intérêt, qui est alors dit *disponible*[1593]. Si l'on considère, comme la majorité de la doctrine française, que le droit pénal est d'ordre public et qu'il protège, en toute hypothèse, l'intérêt général, le consentement ne peut pas être une cause justificative de l'infraction [1594] : « *si l'on considère les faits justificatifs comme des dérogations particulières aux textes repressifs, le consentement de la victime ne saurait, à lui seul, être un fait justificatif car pour déroger à une incrimination – comme à toute norme –, il faut en avoir la force. Or les incriminations étant des normes d'ordre public, elles ne sauraient être suspendues par l'effet d'une permission individuelle* »[1595]. Toutefois, la théorie selon laquelle certaines incriminations protègeraient avant tout des intérêts privés, donc disponibles, n'est pas sans influence sur la doctrine actuelle, et la jurisprudence de la CEDH contribue à maintenir l'intérêt d'une telle thèse, en particulier concernant les atteintes à la vie et à l'intégrité physique. En effet, au regard de l'émergence du droit à disposer de son corps – ou droit à l'autodétermination –, l'inefficacité du consentement de la victime paraît devoir être relativisée[1596]. Néanmoins, comme l'explique Monsieur Pin, quand bien même l'on admettrait la disponibilité du corps humain, il faudrait

---

[1593] X. PIN, *Droit pénal général*, coll. Cours, 10e éd., Dalloz, n° 218-2019.

[1594] Le silence des textes et la jurisprudence imposent en effet la prudence et ne permettent pas d'affirmer que le consentement serait une cause justificative. La doctrine majoritaire admet que l'adage ancien *volonti non fit injuria* n'est pas opérant en matière pénale car la distinction entre délits privés et délits publics n'a jamais réellement convaincu (X. PIN, *Le consentement en matière pénale*, préf. P. MAISTRE DU CHAMBON, Bibl. sc. crim., t. 36, LGDJ, 2002, n° 15). Les tenants de cette conception arguent notamment de ce que l'article 6 du Code civil prévoit qu'« *on ne peut déroger par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs* » (E. DREYER, *Droit pénal général*, *op. cit.*, n° 1240). La Cour de cassation a ainsi affirmé, en matière d'atteinte à la vie, que « *La protection assurée aux personnes par la loi constitue une garantie publique* » (Crim. 23 juin 1838, *S.* 1838, 1, p. 626).

[1595] X. PIN, *Le consentement en matière pénale*, *op. cit.*, n° 223. Cela explique également que la doctrine majoritaire ne reconnaisse pas plus la portée justificative du mobile légitime (X. PIN, *Droit pénal général*, *op. cit.*, n° 254).

[1596] S'agissant de l'atteinte à l'intégrité corporelle, l'émergence d'un droit à l'autodétermination, issu de la théorie allemande (qui admet l'existence d'un élément injuste comme élément constitutif de l'infraction et d'une liberté des individus sur le corps, v. X. PIN, « La théorie du consentement de la victime en droit pénal allemand – Elements pour une comparaison », *RSC* 2003, p. 259), s'est traduite, dans la jurisprudence de la CEDH, par une reconnaissance progressive du droit des personnes à disposer de leur corps (CEDH, 29 avr. 2002, *Pretty c. Royaume-Uni*, n° 2346/02 ; CEDH, 17 févr. 2005, *K.A et A.D c. Belgique*, *D.* 2005 chron., p. 2973, M. FABRE-MAGNAN ; *RTD civ.* 2005, p. 345, obs. J.-P. MARGUENAUD. Sur la libre disposition de soi, v. D. ROMAN, « A corps défendant (la protection de l'individu contre lui-même) », *D.* 2007, Chron., p. 1284 ; sur le droit à l'autodétermination v. S.-M FERRIE, *Le droit à l'autodétermination de la personne humaine : essai en faveur du renouvellement des pouvoirs de la personne sur son corps*, Préf. de G. LOISEAU, coll. Bibliothèque de l'Institut de Recherche Juridique de la Sorbonne-André Tunc, Vol. 92, IRJS Editions, 2018).

encore faire preuve de nuance chaque fois que l'ordre public est atteint[1597]. Concernant l'infraction de violation du secret professionnel, la question du rôle du consentement s'est posée avec d'autant plus de force que son fondement et, partant, l'intérêt qu'il protège, a toujours fait l'objet de controverses.

340. Le secret professionnel médical, secret relatif. Controverse à propos du consentement. Il est désormais admis que le secret professionnel médical n'est pas absolu[1598] et la controverse doctrinale qui tentait de trouver les limites du secret professionnel[1599] en déterminant son fondement[1600] s'est tarie. Si, à la suite de l'arrêt *Watelet*[1601], la majorité de la doctrine[1602] a défendu la théorie d'un secret fondé sur le seul ordre public, et bien qu'une partie de la doctrine continue encore de le désigner comme tel en raison d'une certaine constance de la jurisprudence[1603], la conception relativiste a également trouvé application dans la jurisprudence. Elle a été admise, par exemple, pour reconnaître au médecin la possibilité de témoigner en justice[1604]. Elle a également trouvé appui dans la multiplication des dérogations

---

[1597] X. PIN, *Droit pénal général*, *op. cit.*, n° 222, *spéc.* p. 225-226.

[1598] L. MENNELEC, « Vers une relativisation du secret médical », *JCP* 1979, I, 2936. Sur ce point Monsieur Pin constate qu'il s'opère un rapprochement avec la conception allemande du secret professionnel médical (X. Pin, *Le consentement en matière pénale*, *op. cit.*, n° 204 ; H. JUNG, « Introduction au droit médical allemand », *RSC* 1996, p. 41).

[1599] Le principal enjeu de cette question portait sur la possibilité, pour le déposant, de lever le secret, c'est-à-dire d'autoriser le déposant et en particulier le médecin, à révéler une information le concernant.

[1600] Question qui a opposé les tenants d'un secret professionnel fondé sur le contrat et les partisans d'un secret professionnel fondé sur la profession du déposant (sur ce point v. la synthèse produite par M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.* n° 12 et svt.) : « *A bien des égards, la logomachie qui voit s'affronter un secret absolu reposant sur l'ordre public et un secret relatif reposant sur le contrat apparaît comme une querelle relativement vaine. Ce n'est donc pas en invoquant à l'envi l'un ou l'autre, sans chercher les significations implicites mais réelles qu'ils véhiculent, qu'on découvrira la réponse aux nombreuses questions soulevées par le secret* » (*Ibid.* n° 39).

[1601] Cass. crim., 19 déc. 1885, *S.* 1886, I, p. 86, rapp. TANON.

[1602] V. *contra* R. SAVATIER, note ss. Cass. 1ère civ., 22 janv. 1957, II, 9818 ; *D.* 1957, p. 445. Sur ce point v. encore les travaux précités de Monsieur Couturier (M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*).

[1603] Cass. crim., 8 mai 1947, *Bull. crim.* n° 128 ; *D.* 1948, p. 109, note P. GULPHE ; *JCP* 1948, II, 4141, note A. LEGAL ; *S.* 1947, 1, p. 106 ; Cass. crim. 22 déc. 1966, *D.* 1967, p. 122, rapp. R. COMBALDIEU ; *JCP* 1967, II, 15126, note R. SAVATIER ; *RSC* 1967, p. 463, obs. G. LEVASSEUR ; Cass. crim., 8 avr. 1998 : *Bull. crim.* n° 136 ; *Dr. pén.* 1998, comm. n° 113, obs. M. VERON ; *D.* 1999, somm. p. 381, obs. J. PENNEAU ; *Procédures* 1998, comm. n° 228, obs. J. BUISSON. Il en est de même de la jurisprudence du Conseil d'Etat et encore récemment, v. F. DIEU, concl. sur CE, 26 sept. 2018, n° 407856 et 410550 ; *RDSS* 2018 p. 1035. Le rapporteur public rappelle à cette occasion le caractère absolu du secret professionnel au regard d'une jurisprudence ancienne du Conseil d'Etat (CE, 12 avr. 1957, *Devé*, *Rec. Lebon*, p. 266).

[1604] Depuis un arrêt Cass. crim., 22 fév. 1828 : *S.* 1928, I, p. 41 ; Puis Cass. crim., 24 mai 1862 : *D.* 1862, I, p. 545 ; Cass. crim., 20 mai 1899 : *S.* 1901, I, p. 64 ; *D.* 1900, I, p. 25. S'agissant de la possibilité, pour le médecin de témoigner afin d'assurer sa défense, l'arrêt le plus connu est celui dit du *Roi des Gitans* (Crim. 20 déc. 1967 :

spéciales prévues à l'article 226-14 du Code pénal et, en ce qui concerne le secret professionnel dans le domaine de la santé, dans le Code de la santé publique. C'est au regard de ces limites que Monsieur Beignier a défendu la possible conciliation entre « *une limite au secret professionnel et son caractère absolu* »[1605], ce que Madame Delmas-Marty avait déjà expliqué, utilisant une métaphore souvent reprise pour figurer la limitation du secret professionnel[1606]. Le succès de cette possible complémentarité s'est ensuite confirmé[1607]. Elle a été parfaitement résumé par Monsieur Sargos, selon lequel la portée de l'affirmation du caractère absolu du secret professionnel constitue « *pour le médecin, une excuse, au sens juridique du terme, qui le dispense de l'obligation de témoigner en justice* […] »[1608], ce que l'auteur nomme *principe d'immunité*, tandis qu'au regard d'un *principe de légitimité*, « *la révélation d'informations relevant du secret médical doit poursuivre une finalité légitime fondée sur des raisons pertinentes et suffisantes et ne pas être disproportionnée par rapport au but létitime poursuivi* »[1609]. En somme, même s'il ne fait plus de doute que le secret professionnel connaît des limites, ces évolutions n'ont pas permis de résoudre la question tenant au caractère justificatif du consentement. Puisque la doctrine majoritaire refuse d'admettre l'existence, au sein de l'infraction, d'un élément injuste et donc « *d'envisager l'intérêt protégé, dans la structure de l'incrimination* »[1610], il serait risqué, sinon erroné, d'évoquer le *consentement de la victime* comme étant, à lui seul, un fait justificatif[1611].

Bull. n°338, *D.* 1967, p. 309 note E. LEPOINTE, *RSC* 1968, 343, obs. G. LEVASSEUR). V. B. PY, *Rep. pén.*, *V°* « secret professionnel », fév. 2003 (act. fév. 2017), n° 165 et svt.

[1605] B. BEIGNIER, *L'honneur et le droit*, préf. J. Foyer, Bibl. dr. privé, t. 234, LGDJ, 1995, spéc. p. 119 et svt.

[1606] Selon l'auteur, le secret est « *bien autre chose que l'expression d'un simple devoir de se taire. Reposant sur un jeu plus subtil entre parole et silence, il est avant tout un rythme, mouvement, comme un mouvement repiratoire* » (M. DELMAS-MARTY, « A propos du secret professionnel », *D.* 1982, chron., p. 267).

[1607] P. SARGOS, « Les principes d'immunité et de légitimité en matière de secret professionnel médical », *JCP G*, n° 50, 8 Décembre 2004, doctr. 187 ; M. COUTURIER, « Que reste-t-il du secret médical ? », *in Mélanges en l'honneur de Gérard Mémeteau. Droit médical et éthique médicale : regards contemporains*, LEH Édition, 2015, p. 351-360 ; Y. LAMBERT-FAIVRE, *Droit du dommage corporel - Systèmes d'indemnisation*, Précis Dalloz, 4e éd., 2000, spéc. n° 47.

[1608] P. SARGOS, « Les principes d'immunité et de légitimité en matière de secret professionnel médical », *op. cit.*, n° 11.

[1609] *Ibid.* n° 13.

[1610] X. PIN, *Le consentement en matière pénale*, *op. cit.*, n° 198.

[1611] Quelques auteurs se sont toutefois risqués dans cette voie, sans trouver réllement écho dans la doctrine (X. PIN, *Le consentement en matière pénale*, *op. cit.* n° 3) et notamment, pour ne mentionner que l'ouvrage le plus souvent cité : A.-F. ABDOU, *Le consentement de la victime*, Bibl. sc. crim. , t. 11, LGDJ, 1971.

341. Distinction entre consentement exclusif et consentement justificatif en matière pénale. Monsieur Pin, traçant les contours de ce qu'il nomme *consentement permissif*[1612] et évoquant ces différentes illustrations, explique que toute infraction, quand bien même elle comporte une victime, « *nuit à la collectivité* »[1613]. La victime est toujours « *l'instrument d'une lésion qui la dépasse* »[1614], pour savoir si le consentement peut ou non être permissif il faut alors savoir quel *intérêt est protégé en priorité*[1615]. Il s'en suit que si l'intérêt protégé en priorité est un intérêt particulier, c'est-à-dire « *la liberté de certaines personnes d'exercer ou de ne pas exercer un droit ou une faculté* »[1616], alors la prohibition est relative et non absolue. En conséquence, selon l'auteur, le consentement peut avoir un *effet permissif*. Dans ce cas, l'incrimination est disponible. Deux hypothèses sont alors distinguées par l'auteur : soit le consentement « *se déduit du texte d'incrimination, il procède par exclusion de l'infraction, c'est un* consentement exclusif »[1617]*,* soit *« il est prévu par un texte dérogatoire, afin de rendre licite un acte objectivement infractionnel, il s'agira d'un* consentement justificatif »[1618]. C'est au regard de cette typologie qu'il convient d'analyser l'évolution des rapports entre secret

---

[1612] Ce terme désigne, selon Monsieur Pin « *l'action de permettre ; c'est-à-dire à la fois l'acte qui lève un empêchement (le permis s'oppose à l'interdit), et l'acte qui du même coup offre une possibilité (le permis s'oppose à l'obligatoire, à l'imposé)* » (X. PIN, *Le consentement en matière pénale*, *op. cit.*, n° 57) l'auteur s'emploie ensuite à démontrer que cet acte est de même nature que les actes d'autorisation du droit privé (B. THUILLIER, *L'autorisation, étude de droit privé*, Bibl. de droit privé, t. 252, LGDJ, 1996). Il en déduit, s'agissant de la nature du consentement, qu'il « *importe peu que le consentement soit un obstacle à la constitution de l'infraction (consentement exclusif) ou une conditions exceptionnnelle à sa justification (consentement justificatif), dans les deux cas, l'interdit pénal est levé par un acte qui présente la même nature* » (X. PIN, *Le consentement en matière pénale*, *op. cit.*, n° 113). Ce qui explique également que l'auteur n'emploie pas le vocable « consentement la victime », car dans la première hypothèse il n'existe pas de victime puisque l'infraction n'est pas constituée. Sur le plan du régime l'auteur explique, après en avoir fait la démonstration, que « *l'existence du consentement permissif est enfermé dans de strictes limites, constituées,* d'une part*, par la loi qui le prévoit, et* d'autre part*, par la disponibilité de l'objet protégé par l'incrimination qu'il suspend : le consentement permissif bute sur l'intérêt général et l'intérêt des tiers*. *En outre, le consentement n'est efficace que s'il est exprimé* avant la réalisation de l'infraction ou simultanément*, et s'il émane d'une personne raisonnable, qui se décide* liberment et en connaissance de cause » (X. PIN, *Le consentement en matière pénale*, *op. cit.*, n°173).

[1613] *Ibid.* n° 175.

[1614] *Ibid.*

[1615] *Ibid.* Il est patent que certaines infractions comportant une victime protègent en priorité l'ordre public, c'est notamment le cas, au moins en droit français, des infractions sanctionnant des actes de nature brutale (X. PIN, *Droit pénal général*, *op. cit.*, n° 222). On peut notamment souligner une certaine résistance du juge français à la jurisprudence de la CEDH concernant les pratiques sadomasochistes (CA Grenoble, 1re ch. app. corr., 11 mars 2009 : JurisData n° 2009-002946 ; *JCP G*, n° 27, 29 Juin 2009, 65, obs. A.-G. ROBERT ; Cass. crim., 2 déc. 2009, n° 09-82.447 ; *CCC* 2010, comm. 28, obs. A. LEPAGE).

[1616] X. PIN, *Droit pénal général*,

[1617] X. PIN, *Le consentement en matière pénale, op. cit.*, n° 175.

[1618] *Ibid.*

professionnel dans le domaine de la santé et les dispositions relatives au traitement des données. C'est plus particulèrement sur le consentement permissif justificatif que nous porterons notre analyse car s'agissant de l'incrimination de violation du secret professionnel, le consentement ne peut se déduire du texte d'incrimination[1619].

B - Le rôle du consentement *permissif justificatif* : mouvements contradictoires

342. Tandis que le consentement est érigé en *principe* matriciel du droit de la protection des données **(1)** c'est davantage un droit d'opposition qui accordé aux personnes concernées par les données **(2)**.

1 - L'affirmation du rôle croissant du consentement

343. Traitement des données, consentement justificatif et secret professionnel dans le domaine de la santé. En l'état actuel du droit français, si le consentement ne peut justifier la révélation d'une information à caractère secret par un professionnel qui y est soumis, il n'en est pas moins un élément de la justification, une *cause de justification*[1620]. Les dérogations particulières prévues par un texte – en principe législatif selon l'article 122-4 du Code pénal– autorisant la révélation d'une information à caractère secret sont nombreuses et le consentement de la personne concernée apparaît régulièrement comme l'une des *conditions* permettant de faire jouer la justification. Il en est ainsi du fait justificatif prévu à l'article 226-14 du Code pénal, qui autorise le médecin ou le professionnel de santé à révéler à des personnes désignées « *les sévices ou privations qu'il a constatés, sur le plan physique ou psychique, dans l'exercice de sa profession et qui lui permettent de présumer que des violences physiques, sexuelles ou psychiques de toute nature ont été commises* »[1621] dans les hypothèses où la personne concernée est en mesure de donner son consentement[1622]. La possibilité de partager ou d'échanger des

---

[1619] Nous avons veillé en amont a démontrer que le critère de la soumission au secret professionnel était désormais celui de la source des données (des données couvertes par un secret professionnel que l'on pourrait qualifier d'originel) et non leur nature, ce qui constitue une indication en ce sens.

[1620] L'exemple représentatif est celui du consentement cause de justification de l'acte médical. Pour l'une des premières études sur la question, v. B. PY, *Recherches sur les justifications pénales de l'activité médicale*, ss. la dir. de J.-F. SEUVIC, Nancy II, 1993.

[1621] CP, art. 226-14, 2°.

[1622] La capacité à consentir est entendue plus strictement qu'en matière civile. Elle dépend en partie du jugement du professionnel puisque le texte prévoit notamment que l'accord de la personne n'est pas nécessaire lorsqu'il s'agit d'un mineur ou d'une personne qui n'est pas en mesure de se protéger en raison de son âge ou d'une incapacité physique ou psychique. Or, en droit civil, la capacité, une fois la majorité civile atteinte, ne connaît plus

informations entre professionnels prenant en charge une même personne dans le cadre de son parcours de santé est prévue à l'article L. 1110-4 du Code de la santé publique[1623]. Ce texte prévoit une hypothèse dans laquelle le consentement de la personne est exigé, souvent présenté comme une cause de justification de la violation du secret professionnel, bien qu'il ne s'agisse pas, selon nous, de justifier la violation du secret professionnel.

Il n'existe, à notre connaissance, aucun texte portant justification de la révélation d'une information à caractère secret dans le cadre d'un traitement de données et prévoyant, pour seule cause justificative, le consentement de la personne[1624].

Notons toutefois que Monsieur Pin semble interpréter en ce sens l'ancien article 226-18 du Code pénal qui prévoyait que les données concernant des prélèvements biologiques ne pouvaient être transmises qu'avec le consentement exprès et éclairé de l'intéressé[1625]. Il nous semble toutefois que l'auteur interprète de manière critiquable en raison de l'autorisation de transmettre l'information à des fins de recherche créée par la loi du 1er juillet 1994. Le texte d'incrimination précité ne faisait que sanctionner le fait de ne pas recueillir le consentement dans certaines hypothèses. Autrement dit, le consentement est l'une des causes de justification,

---

de seuil d'âge mais dépend uniquement de l'altération des facultés mentales, lesquelles vont permettre la mise en place de mesures de protection.

[1623] CSP, art. L. 1110-4. Les autres *conditions* du partage et de l'échange ont été évoquées en amont v. *supra* n°234.

[1624] La question s'est également posée en droit belge. Comme en droit pénal français, le consentement de la personne n'est pas un fait justificatif de la violation du secret professionnel. Dans une analyse relative à l'articulation du secret professionnel et du règlement général sur la protection des données (RGPD), deux auteurs expliquent : « *Le principal enjeu de ce débat consistait à savoir si, dans ce nouveau contexte législatif, l'obtention du consentement d'une personne aux fins de légitimer, en tout ou en partie, le traitement de données à caractère personnel relatives à sa santé permettait, en outre, de libérer le praticien professionnel* […] *de son obligation au secret* […]. *En effet, dans une vision pénale classique, il n'était pas admis que le patient puisse libérer le dépositaire de ses secrets sauf dans la mesure (pas nécessairement si limitée en toute hypothèse) de ce qui lui était reconnu dans la littérature et la jurisprudence, sans oublier les situations dans lesquelles la loi elle-même conférait un droit à la personne en ce sens. La réponse était évidente : la protection des données n'a jamais eu pour objectif de modifier les règles relatives au secret médical, que ce soit au niveau belge ou européen*. […] *Deux arguments principaux soutenaient cette interprétation. D'abord, la directive elle-même faisait référence à l'existence des règles relatives au secret médical sans pour autant prétendre les régir. Il ne pouvait qu'en être déduit que ces dernières existaient indépendamment de la protection des données. Ensuite, l'obligation de traiter licitement les données a été interprétée comme incluant aussi l'obligation de se conformer aux règles particulières qui pouvaient régir le type de données en cause ce qui, dans notre cas, renvoyait au respect des règles relatives au secret médical* » (J. HERVEG, J.-M. VAN GYSEGHEM, « Titre 16 - L'impact du Règlement général sur la protection des données dans le secteur de la santé » *in* C. DE TERWANGNE et K. ROSIER (ss. la dir.), *Le règlement général sur la protection des données* (RGPD/GDPR), Bruxelles, Larcier, 2018, p. 703-704).

[1625] X. PIN, *Le consentement en matière pénale*, *op. cit.*, n° 206.

pour certaines données, mais, dans cette hypothèse, la condition première reste la finalité du traitement. Ce texte a ensuite été remplacé par l'article 226-19-1 du même code, sanctionnant le fait de traiter des données caractère personnel ayant pour fin la recherche dans le domaine de la santé « *malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne* ». La formulation entre les deux versions de l'article demeure la même. La CNIL apporte un éclairage sur ce point : rappelant l'exception posée par l'article 56 de la loi informatique et libertés, elle précise : « *Lorsque la recherche, l'étude ou l'évaluation nécessite le recueil de prélèvements biologiques identifiants permettant d'en extraire des données génétiques, la loi « Informatique et Libertés » impose le recueil par écrit du consentement de la personne concernée (ou de ses représentants légaux) préalablement à tout traitement* »[1626]. Il faut donc entendre le traitement dans son sens le plus large : il s'agit autant du recueil que de la transmission des données, laquelle est donc, en plus de la finalité, subordonnée au consentement de la personne concernée.

344. Le consentement, condition essentielle de la liciété du traitement. Si le consentement est l'une des conditions de licéité du traitement des données à caractère personnel[1627], il est aussi la première cause de justification de l'interdiction de traiter des données sensibles, dont les données de santé à caractère personnel[1628]. En toute hypothèse, le consentement n'est jamais l'unique condition de licéité des traitements, d'ailleurs une seule des incriminations sanctionnant une atteinte aux droits des personnes résultant des fichiers ou des traitements informatiques prévoit l'absence de consentement comme élément constitutif de l'infraction[1629]. Le consentement de la personne tient néanmoins une place centrale dans la loi informatique et

---

[1626] CNIL, *Les données génétiques*, coll. point Cnil, La documentation française, 2017, chapitre « Recherche génétique et pratique médicale ».

[1627] Un traitement de données à caractère personnel n'est en effet licite que si le responsable du traitement respecte l'une des conditions énoncées à l'article 6 du RGPD (LIL, art. 5). Le consentement est la première de ces conditions, il ne peut être passé outre le recueil du consentement que lorsque le traitement respecte l'une des autres conditions énoncées : « *Le respect d'une obligation légale incombant au responsable du traitement ; La sauvegarde de la vie de la personne concernée ; L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ; L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ; La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée* » (LIL, art. 5).

[1628] Art. 9 du RGPD.

[1629] Seul l'article 226-19 sanctionne la collecte des données dites sensibles, en dehors des possibilités de collecte sans le consentement des personnes (art. 9 RGPD), effectuée sans le consentement des personnes.

libertés depuis la transposition de la directive 95/46/CE par la loi du 6 août 2004[1630] et dans le RGPD[1631]. Les difficultés liées au respect de la condition d'obtention du consentement intéressent particulièrement la doctrine[1632], et la CNIL est particulièrement vigilante quant à sa validité[1633]. Outre l'exigence première de consentement, c'est la maîtrise de l'individu sur ses données qui est revendiquée, tant dans le discours politique que dans la doctrine.

345. L'affirmation d'une maîtrise de la personne sur ses données personnelles. *Empowerment* et *autodétermination informationnelle*. Clarification. Pour évoquer la maîtrise de ses données par l'individu, le terme *empowerment*, importé des Etats-unis, est parfois utilisé par la doctrine[1634]. Il désigne un phénomène social qui n'est pas propre au numérique. La notion a une origine relativement ancienne[1635] mais connaît un renouvellement idéologique à partir des années 1970, rattachée à des mouvements sociaux qui participent au « *décentrement de l'action revendicative du monde de la production vers de nouveaux enjeux comme la libération des femmes, la question raciale, les droits des homosexuel-les, les identités*

[1630] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* n° 182 du 7 août 2004, p. 14063.

[1631] En ce sens également, v. A. LECOURT, « RGPD : nouvelles contraintes, nouvelles stratégies pour les entreprises », *Dalloz IP/IT* 2019, p. 205. Aussi, le considérant 32 du RGPD précise les qualités que devrait revêtir le consentement et les conditions de sa validité, tandis que les considèrants 40 et suivants précisent les conditions dans lesquelles le consentement peut être « libre » et « éclairé ».

[1632] Les difficultés apparaissent de manière plus aiguë s'agissant du recueil de ce consentement sur internet : J. ROCHFELD, « Le « contrat de fourniture de contenus numériques » : la reconnaissance de l'économie spécifique « contenus contre données » », *Dalloz IP/IT* 2017, p. 15 ; Sur le consentement et le *smart contract* porté par le dispositif de *blockchain* v. M. MEKKI, « Le smart contract, objet du droit (Partie 2) », *Dalloz IP/IT* 2019, p. 27.

[1633] V. la sanction de la Commission à l'encontre de Google : CNIL, formation restreinte, délib. SAN-2019-001, 21 janv. 2019, *Dalloz act.* 28 janvier 2019, obs. N. MAXIMIN, *Dalloz IP/IT* 2019. 165, obs. E. NETTER ; *CCE* 2019. Comm. 32 et 43, obs. N. METALLINOS ; *JCP E* 2019. 1059, note J. DEROULEZ.

[1634] Par exemple : C. ZOLYNSKI, « Les nouveaux contours de l'action de groupe et de l'action collective au lendemain de la loi pour la protection des données : un *empowerment* renforcé », *Dalloz IP/IT* 2018, p. 470 ; L. CLUZEL-METAYER et E. DEBAETS, « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA 2018*, p. 1101 ; N. OCHOA, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA* 2015, p. 1157 ; A. BENSAMOUN et G. LOISEAU, « L'intégration de l'intelligence artificielle dans certains droits spéciaux », *Dalloz IP/IT* 2017, p. 295 ; F. EON, « Hôpital public et données personnelles des patients », *RDSS* 2015, p. 85 ; G. GALUSTIAN, « La protection des données personnelles à l'épreuve du numérique », *RDP* 2018, p. 1389 ; A. BENSAMOUN et C. ZOLYNSKI, « Big data et privacy : comment concilier nouveaux modèles d'affaires et droits des utilisateurs ? », *LPA* 18 août 2014, p. 8.

[1635] M.-H. BAQUÉ et C. BIEWENER, « L'empowerment, un nouveau vocabulaire pour parler de participation ? », *Idées économiques et sociales* 2013/3, n° 173, n° 4 et svt.

régionales ou l'écologie »[1636]. Sa portée émancipatrice se traduit dans sa double définition : « L'empowerment *articule deux dimensions, celle du pouvoir, qui constitue la racine du mot, et celle du processus d'apprentissage pour y accéder. Il peut désigner autant un état (être empowered) qu'un processus. Cet état et ce processus peuvent être à la fois individuels, collectifs et sociaux ou politiques – même si, selon les usages de la notion, l'accent est mis sur l'une de ces dimensions ou au contraire sur leur articulation* »[1637]. La notion est ensuite intégrée au discours politique français dans le courant des années 2000[1638]. Dans le domaine de la protection des données à caracatère personnel, elle est mise en avant par le Forum économique mondial[1639], puis reprise par le Conseil national du numérique pour viser la maîtrise des données à caractère personnel comme condition de la transformation numérique[1640]. Si le terme d'*empowerment* connaît un certain succès, remarquons qu'il est souvent rattaché à un autre terme, celui *d'autodétermination informationnelle*[1641]. Les deux termes ne visent toutefois pas les mêmes concepts, bien qu'ils s'inscrivent tous deux dans une idéologie libérale[1642]. L'*empowerment* est sous-tendu par l'idée de donner plus de pouvoir à l'individu ou à un groupe d'individus pour qu'il puisse agir dans la société. L'idée de participation prédomine et s'inscrit dans un contexte social. Quant à l'*autodétermination* de la personne – qu'elle concerne ses informations ou son corps –, elle consiste à faire de l'autonomie

---

[1636] *Ibid.* n° 10.
[1637] *Ibid.* n° 1.
[1638] *Ibid.*
[1639] World Economic Forum, « *Unlocking the Value of Personal Data : From Collection to Usage* », 2013.
[1640] Le terme empouvoirement est aussi utilisé : CNNum, *Rapport au premier ministre,* « Ambition numérique. Pour une politique française et européenne de la transition numérique », juin 2015 ; CNNum, *Rapport remis à la Ministre des Affaires sociales, de la Santé et des Droits des femmes,* « La santé, bien commun de la société numérique. Construire le réseau du soin et du prendre soin », oct. 2015. L'une des propositions du Conseil consistait à « *Concrétiser* l'empowerment *individuel et collectif sur les données de santé, en termes de protection, de maîtrise et de mobilisation à la faveur de nouveaux usages* » (*Ibid.* p. 16).
[1641] Où la notion d'*empowerment* est utilisée pour parler de la maîtrise des données à caractère personnel et vise l'autodétermination informationnelle, dans le discours politique : CNNum, *Rapport remis à la Ministre des Affaires sociales, de la Santé et des Droits des femmes*, « La santé, bien commun de la société numérique. Construire le réseau du soin et du prendre soin », *op. cit.* ; dans le discours de la doctrine où il est souvent affirmé que l'empowerment consiste dans la reconnaissance de droits subjectifs : J.-P. FOEGEL, « *Le Conseil d'Etat, héraut de la révolution numérique ? Protection des données personnelles (Conseil d'Etat)* », *La revue des droits de l'Homme*, *Actualité Droits-Libertés*, déc. 2014 ; G. GALUSTIAN, « La protection des données personnelles à l'épreuve du numérique », *op. cit.* ; E. GEFFRAY, « Quelle protection des données personnelles dans l'univers de la robotique ? », *Dalloz IP/IT* 2016, p. 295 ; L. CLUZEL-METAYER et E. DEBAETS, « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA* 2018, p. 1101.
[1642] S'agissant de *l'empowerment*, v. M.-H. BAQUÉ et C. BIEWENER, « L'empowerment, un nouveau vocabulaire pour parler de participation ? », *op. cit.*, n° 25 ; concernant le droit à l'autodétermination, v. notamment M. FABRE-MAGNAN, *L'institution de la liberté*, PUF, 2018.

de la volonté, et donc du consentement, le fondement et les conséquences de la liberté[1643]. Le concept d'autodétermination n'a donc pas de dimension collective, il ne s'agit que de consacrer le pouvoir de la personne sur son corps et sur les éléments de sa personnalité[1644].

Nous pensons que l'usage du terme *empowerment* pour parler de la maîtrise de ses données par la personne constitue un raccourci, voire un leurre. Une comparaison avec le processus à l'œuvre en matière de santé suffit à s'en convaincre. Dans le domaine de la santé, l'on évoque en effet l'*empowerment* du patient face au pouvoir médical, afin de conceptualiser le passage d'une médecine paternaliste à une médecine dont les patients sont acteurs, l'aspect individuel ne pouvant être isolé de l'aspect collectif[1645]. La fin du paternalisme médical a aussi consisté à offrir une place à la participation des groupes d'usagers dans le débat public, c'est l'idée même de la démocratie sanitaire portée par la loi du 4 mars 2002. La création des Commissions des relations avec les usagers et de la qualité de la prise en charge[1646], l'émergence progressive du statut de *patient expert*[1647], la place grandissante des

---

[1643] On trouvera, dans l'ouvrage de Muriel Fabre-Magnan, une synthèse éclairante de ces rapports et de l'évolution de notre conception de la liberté désormais fondée sur la volonté de l'individu (*Ibid.*). L'autodétermination est issue de la théorie allemande des droits de l'Homme. Un droit à l'autodetermination informationnelle est reconnu, dès 1983 par la Cour constitutionnelle allemande (*Bundesverfassungsgerichsthof*, 15 déc. 1983, BVerfGE 65, 1) comme « *la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* » (traduction de Y. POULLET et A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du le développement personnel. Une réevaluation de l'importance de la vie privée pour la démocratie » *in* K. BENYEKHELF et P. TRUDEL (ss. la dir.), *Etat de droit et virtualité*, Thémis, 2009, p. 157 svt.).

[1644] Les développements de Madame Ferrié à propos de l'autodétermination de la personne humaine peuvent être transposés pour définir l'autodétermination informationnelle : « *Le principe d'autodétermination conduit* […] *à reconnaître à l'individu la possibilité de choisir comment traiter son corps, y compris si cela doit le conduire à porter atteinte à son intégrité physique ou psychique.* […] *C'est dire que la source de tout acte d'autodétermination est une manifestation de volonté individuelle et que l'objet de tout acte d'autodétermination est le corps de la personne ayant exprimé cette volonté* » (S.-M. FERRIÉ, *Le droit à l'autodétermination de la personne humaine. Essai en faveur du renouvellement des pouvoirs de la personne sur son corps*, *op. cit.*, n° 841).

[1645] D. CRISTOL, « L'usager dans la stratégie nationale de santé : la démocratie en santé en quête d'un nouveau souffle », *RDSS* 2018, p. 413 ; « Le droit à la participation dans les lois des 2 janvier et 4 mars 2002 », *RDSS* 2012, p. 453 ; M. DUTOIT, « Entre injonction et impératif de coopération, les nouveaux modes d'organisation des personnes " usagers " », *in* M. JAEGER (dir.), *Usagers ou citoyens ? De l'usage des catégories en action sociale et médico-sociale*, Dunod, 2011, p. 162.

[1646] Art. R. 1112-79 CSP.

[1647] Il s'agit de partager la connaissance entre patients, ce qui diminue le déséquilibre informationnel inhérent à la relation patient-soignant. On voit notamment émerger des formations de patient-experts, une université des patients (<https://universitedespatients.org/>) ; M. JACOT, Faire de l'expérience de la maladie son métier, Le Monde, 22 avr. 2018 ; M. BERTHOD-WURMSER, F. BOUSQUET et R. LEGAL, « Patients et usagers du système de santé : l'émergence progressive de voix qui commencent à compter », *Revue française des affaires sociales* 2017/1, p. 5.

aidants-familiaux dans la prise en charge[1648], sont autant de marqueurs d'un pouvoir d'agir collectivement et personnellement sur un domaine de la société. Aussi, il nous semble que si l'autonomie de la personne est une des conditions de l'*empowerment*, ce n'est que dans son aspect individuel, or, pour que les individus constituent un pouvoir, la dimension collective ne peut être exclue[1649]. Cette dimension participative et collective qui sous-tend l'*empowerment* n'est pas prégnante dans les dispositions relatives à la protection des données[1650], les textes qui fondent la protection des données à caractère personnel octroyant davantage de prérogatives individuelles. Historiquement, elle trouve une première application dans la reconnaissance du droit d'accès, par l'individu, à ses dossiers personnels, peu importe le support, dont le dossier médical[1651]. Par la suite seront reconnues diverses prérogatives : le consentement à toute opération de traitement, le droit à l'oubli – ou effacement[1652] –, le droit à la portabilité des données[1653], le droit de rectification[1654], et le droit à l'information[1655], bien qu'ils soient limités

---

[1648] S. GUÉRIN, « Les aidants, cœur du système social », *Revue Projet* 2012/1 (n° 326), p. 47 ; Les nommant proches mais évoquant leur mission d'aide et se positionnant pour la reconnaissance d'un statut des proches dans la mesur où « plus que jamais le proche devient un acteur incontournable de la prise en charge globale du patient » : B. BEVIERE-BOYER, « Le proche du patient, un statut complexe, des améliorations possibles », *RDS*, n° 41, 2011, Pp. 230-243.

[1649] L'*empowerment* ne peut exister que dans le cadre d'une participation collective : P. TÜRK, « La citoyenneté à l'ère numérique », *RDP* 2018, p. 623 ; P. TÜRK et C. VALLAR, « La souveraineté numérique », Mare&Martin, 2018. Le Conseil d'Etat distingue également l'*autodétermination informationnelle* de l'*empowerment :* Conseil d'Etat*, Étude annuelle 2014 : le numérique et les droits fondamentaux,* La Documentation française, 2014.

[1650] On en trouve tout de même une manifestation au travers de l'action de groupe, ce que Mesdames Rochfeld et Zolynski identifient clairement comme participant de l'*empowerment* (Judith Rochfeld n'utilise toutefois pas le terme) : C. ZOLYNSKI, « Les nouveaux contours de l'action de groupe et de l'action collective au lendemain de la loi pour la protection des données : un empowerment renforcé », *op. cit.* ; J. ROCHFELD, *Quelle politique européenne en matière de données personnelles ?*, New Deal Foundation, Rapport d'étude septembre 2015.

[1651] Le droit d'accès aux dossiers est successivement reconnu par la loi informatique et libertés du 6 janvier 1978, puis par celle du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal. Ce que la CNIL qualifiera, dès 1980, « *d'habeas data* » répondant à un souci de transparence de l'administration (CNIL, *Rapport* « bilan et perspective », 1978-1980). S'agissant du dossier médical, le droit d'accès s'exerce d'abord par l'intermédiaire d'un médecin avant qu'il ne soit reconnu un accès direct par la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

[1652] Le terme de droit à l'effacement permet de ne pas opérer de confusion avec un droit qui consisterait à pouvoir « *s'opposer à la reprise sans leur consentement d'informations qui dans leur temps furent licitement révélées au public mais dont l'actualité ne justifie plus la diffusion* » (A. LEPAGE, « Droit à l'oubli : une jurisprudence tâtonnante », *D.* 2001, p. 2079). En matière de traitement de données il s'agirait plutôt du droit à l'effacement de ses données à caractère personnel ayant fait l'objet d'un traitement (RGPD, art. 17).

[1653] RGPD, art. 20.

[1654] RGPD, art. 16.

[1655] Le contenu de l'information et les modalités de celle-ci diffèrent selon que les données sont collectées directement auprès de la personne (RGPD, art. 13) ou pas (RGPD, art. 14).

dans certaines hypothèses, sont autant d'élements tendant à la reconnaissance d'un *droit à l'autodétermination informationnelle*[1656].

346. Des conséquences attendues du droit à l'autodétermination informationnelle sur le rôle du consentement comme fait justificatif. L'on pourrait penser que la volonté de donner à l'individu une maîtrise de ses données à une influence déterminante sur la justification de la violation du secret professionnel des professionnels intervenant dans le système de santé, dans la mesure où les prérogatives accordées à l'individu existent indépendamment de la source des données. L'autonomie accordée à l'individu ne devrait-elle pas se traduire, au travers des normes dérogatoires, par un rôle accru du consentement comme élément justificatif ? D'un point de vue technique, la question se pose de manière plus évidente puisque la notion de traitement recouvre une multitude d'opérations dont des opérations consistant à communiquer des données[1657]. Ainsi, certains auteurs ont pu affirmer que « *la transmission des données sensibles à des tiers doit évidemment se faire avec le consentement exprès des personnes concernées* »[1658]. Cette affirmation n'est que partiellement conforme au droit positif puisqu'elle ne se vérifie pas en qui concerne les données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou d'un suivi social et médico-social. L'examen des textes spéciaux justifiant la transmission des données par des professionnels soumis au secret doit nous permettre de le confirmer.

347. Le domaine de la santé, l'exclusion de la logique du *tout consentement*. Le partage de certaines informations hors du cadre de l'équipe de soins est prévu par décret et, outre les conditions tenant à la qualité des personnes pouvant partager et à la finalité[1659], le consentement de la personne est également exigé. Le partage correspondant à une *mise à disposition*[1660], sa traduction dans le vocabulaire de la loi informatique et libertés et du RGPD est une opération de traitement : *l'accès*. L'article L. 1111-17 du Code de la santé publique prévoit ainsi qu'un

---

[1656] L'expression n'est utilisée qu'une seule fois dans le RGPD, ce que regrette d'ailleurs un auteur, estimant qu'il s'agit d'une reconnaisse timide : N. MARTIAL-BRAZ, « Le renforcement des droits de la personne concernée », *Dalloz IP/IT* 2017, p. 253.
[1657] Comme nous avons pu le souligner, le traitement des données ne consiste pas dans le seul fait de collecter et de mettre les données en mémoire, toute opération sur les données est susceptible d'être qualifiée de traitement (v. *supra* n° 157). Ainsi, la transmission des données vers un autre responsable ou un sous-traitant, constitue une opération de traitement dont les conditions de licéité sont inscrites au sein de la LIL et du RGPD.
[1658] M. VIVANT, B. WARUSFEL et N. MALLET-POUJOL, *Lamy droit du numérique*, n° 404.
[1659] V. *supra* n° 237.
[1660] *Ibid.*

professionnel de santé ayant accès au dossier médical partagé du patient « *recueille, après avoir informé la personne concernée, son consentement pour qu'un autre professionnel de santé à qui il serait nécessaire de confier une partie de la prestation accède à son dossier médical partagé et l'alimente* ». L'article R. 1111-41 du même code précise ensuite les modalités de cet accès. Si ce consentement est ordinairement présenté comme une cause justificative, nous ne partageons pas cet avis. Dès lors qu'il ne s'agit pas d'autoriser le professionnel à communiquer les informations mais bien à la personne concernée d'autoriser un accès à ses données personnelle de santé, il s'agit selon nous, d'une manifestation de l'autodétermination informationnelle. Outre cet exemple, le consentement n'est pas le maître mot du traitement des données à caractère personnel dans le système de santé. Il nous semble que la place secondaire du consentement en la matière correspond à une double volonté : protéger la personne et permettre l'utilisation des données pour des finalités d'intérêt public. Nous aurons l'occasion de revenir sur le second aspect, il nous faut évoquer rapidement le premier.

Nous rejoignons, à propos du consentement et particulièrement du consentement en matière de traitement des données à caractère personnel dans le domaine de la santé, les propos plus généraux de Madame Fabre-Magnan et, dans le domaine du numérique et plus particulièrement de l'internet, ceux de Madame Frison-Roche et de Monsieur Yves Poullet. A l'occasion d'un ouvrage remarqué au-delà du monde universitaire et du droit, Madame Fabre-Magnan a expliqué comment la logique du « *tout consentement* »[1661] aliénait l'individu. Concernant le traitement des données, certains auteurs prônent une redéfinition de la vie privée au regard de ce seul consentement. Le fait que les personnes partagent de plus en plus volontairement des informations sensibles serait un argument pour laisser à l'individu une liberté sans bornes sur ses données, vision que l'on peut qualifier de libérale. C'est l'individu qui est alors entièrement responsable de ses choix. Pourtant, comme l'explique Monsieur

---

[1661] Pour illustrer « les leurres du tout-consentement » l'auteur prend, entre autres exemples, celui du consentement en matière de traitement des données à caractère personnel : « *Tous les* « progrès » *technologiques du présent et de l'avenir pourront être analysés selon les mêmes principes : les personnes ayant consenti (à autoriser l'accès à leurs données personnlles, à utiliser les programmes et les algorithmes qui leur sont proposés, à se faire installer des puces corporelles, à prendre place dans des automobiles à pilotage automatique, à se faire injecter des paquets de gènes thérapeutiques, à utilisr des objets connectés ou des robots, ect.), elles ne pourront s'en prendre qu'à elles-mêmes. Dès lors qu'elles auront été informées des risques, elles seront entièrement responsables de toutes les conséquences éventuellement dommageables pour elles.* […]. *En définitive, le sésame du consentement nous vante et nous vend, dans le même sac, la liberté de travailler sans limite de temps (vers le haut) ou de salaire (vers le bas)* […], *ou encore la liberté de céder ses données personnelles* » (M. FABRE-MAGNAN, *L'institution de la liberté*, PUF, 2018, pp. 75-76).

Poullet, « *l'exigence de vie privée ne se fonde pas sur le présupposé d'un individu capable a priori d'une maîtrise de son environnement via son consentement ou par l'exercice de ses droits, mais sur une approche collective et un Etat qui, dans un contexte sociétal donné, doit permettre, y compris par son intervention vis-à-vis des acteurs privés, l'épanouissement des personnes comme acteurs sociaux de changement* »[1662]. Madame Frison-Roche dénonce, à propos du RGPD, « *la fable du consentement* »[1663]. Selon cet auteur, dans le monde numérique, le consentement n'est pas « *le meilleur des outils, alors qu'on le présente souvent comme l'alpha et l'omega* »[1664]. Il nous semble que l'on peut voir, dans le refus de considérer le consentement comme fait justificatif du secret professionnel – en dépit de son importance au sein du RGPD –, une volonté de protéger la personne qui ne maîtrise pas et ne pourra pas maîtriser l'usage qui est fait de ses données à caractère personnel recueillies et traitées lors de sa prise en charge. L'exploitation dynamique des données le justifie[1665]. C'est alors un droit d'opposition qui est offert aux individus. Il ne faut toutefois pas faire preuve de trop d'angélisme, car le droit d'opposition révèle d'autres desseins qu'il faut mettre en lumière.

2 - L'absence d'opposition comme cause justificative

348. Du consentement comme cause justificative à la *l'absence d'opposition*. Malgré la prééminence donnée au consentement dans le RGPD, cette cause justificative a été évacuée de certaines autorisations légales permettant une transmission des données issues d'informations couvertes par le secret par un professionnel qui y est soumis. C'est notamment le cas s'agissant de l'hébergement des données de santé. Tandis que la loi du 4 mars 2002 prévoyait la possibilité de recourir à un hébergeur agréé pour l'hébergement des données des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de

---

[1662] Y. POULLET, *La vie privée à l'heure de la société numérique*, Editions Larcier, 2019, p. 182.
[1663] M.-A. FRISON-ROCHE (propos recueillis par O. DUFOUR), « Gouvernance d'internet : « Nous sommes face à un enjeu de civilisation », *LPA*, 18 juill. 2019 : l'auteur développe les raisons de cette réserve à l'égard du consentement en matière de traitement de données dans un rapport au Ministre en charge du Numérique : M.-A. FRISON-ROCHE, *L'apport du droit de la compliance à la gouvernance d'internet*, Rapport commandé par Monsieur le Ministre en charge du Numérique, Avril 2019.
[1664] M.-A. FRISON-ROCHE (propos recueillis par O. DUFOUR), « Gouvernance d'internet : « Nous sommes face à un enjeu de civilisation », *op. cit.*
[1665] Evoquant une exploitation désormais « dynamique, cinétique » des données en raison des *Big Data* : A. BENSAMOUN et C. ZOLYNSKI, « Cloud computing et big data. Quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux* 2015/1, n° 189, Pp. 103 à 121.

diagnostic ou de soins, cette possibilité de transmettre les données à un tiers était en outre *conditionnée* à l'obtention du consentement de la personne concernée par les données[1666]. La loi de modernisation de notre système de santé[1667] a modifié ce texte : le recours à un hébergeur n'est plus subordonné qu'à une obligation d'information à l'égard de la personne concernée et s'accompagne d'un droit d'opposition, cette opposition devant, en outre, intervenir pour un motif légitime. Dans la rédaction d'origine, le législateur n'avait pas même prévu la possibilité de s'opposer, c'est à la demande de la CNIL qu'il a finalement concédé une modification en ce sens[1668]. Plutôt qu'un consentement permissif c'est l'absence d'opposition qui justifie en partie la transmission des données issues d'informations couvertes par le secret.

Monsieur Pin considère que l'absence d'opposition consiste dans une *présomption de consentement permissif*[1669]. Si nous signalons le point de vue de cet auteur, il nous semble que l'assimilation entre *absence d'opposition* et *présomption de consentement* ne peut être admise. Au sujet du prélèvement *post mortem* qui est l'exemple mis en avant par l'auteur, la doctrine s'est davantage employée à montrer les lacunes de l'assimilation. Madame Thouvenin insiste particulièrement sur l'importance de distinguer entre ces deux notions et sur les conséquences de leur confusion[1670]. Selon Monsieur Loiseau « *la loi prévoit dans* […] *que, sauf opposition*

[1666] Le consentement était surtout analysé comme une condition de validité du contrat d'hébergement (en ce sens, I. VACARIE, « *L'hébergement des données de santé : entre contrat et statut », RDSS* 2002, p. 695), d'autres ont pu considérer qu'il s'agissait d'un contrat tripartite (F.-J. PANSIER et C. CHARBONNEAU, « La dématérialisation des données médicales et les enjeux de leur hébergement », *Gaz. Pal.* 17 déc. 2002, n° 351, p. 23), tandis qu'il a pu être évoqué la qualification de stipulation pour autrui (C. ZORN-MACREZ, « L'hébergement des données de santé sur support informatique », *Droit médical et hospitalier*, Litec, fasc. 10, 2013, n° 23). Il a ainsi pu lui être dénié toute portée justificative de la violation du secret professionnel (*Ibid.* n° 20). Ce n'est pas notre point de vue, dès lors que la transmisson des données entraîne nécessairement un accès à ces dernières pour des nécessités techniques, ce qui a notamment justifié la soumission au secret professionnel des hébergeurs et du personnel placé sous leur autorité. V. *supra* n° 292 et svt.. Il s'agit donc bien d'une permission spécifique prévue par la loi.

[1667] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

[1668] Rapport n° 2673 fait au nom de la commission des affaires sociales sur le projet de loi relatif à la santé, p. 485. En ce sens v. également L. TILMAN, *L'utilisation des technologies de l'information et de la communication à l'hôpital face au droit*, Th. de droit public, ss. la dir. de J. SAISON-DEMARS, Université de Lille II Droit et santé, soutenue le 28 septembre 2017, n° 232.

[1669] Sur les cas de présomptions de consentement permissif v. X. PIN, *Le consentement en matière pénale*, préf. P. MAISTRE DU CHAMBON, Bibl. sc. crim., t. 36, LGDJ, 2002, n° 165 et svt. Selon cet auteur une présomption de consentement permet notamment le prélèvement d'éléments du corps humain et la collecte de ses produits (CSP, art. 1211-2). Ce consentement présumé justifie l'atteinte sanctionnée à l'article 225-17 qui punit l'atteinte à l'intégrité du cadavre. Il en est de même pour les organes prélevés lors d'une opération chirurgicale, pratiquée dans l'intérêt de la personne, qui peuvent être utilisés à des fins thérapeutiques ou scientifiques, sauf opposition de la personne concernée (CSP, art. 1235-2) et les tissus et cellules (CSP, art. 1245-2).

[1670] Sur cette question, la thèse de Monsieur Zagury (V. ZAGURY, *Regards sur le droit d'opposition extrapatrimonial : contribution à l'etude de la volonté en droit prive*, th. dact., ss. la dir. de F. BELLIVIER,

exprimée par la personne concernée, les éléments et produits prélevés à l'occasion d'une intervention chirurgicale pratiquée dans l'intérêt de celle-ci ou les organes prélevés après la mort de la personne peuvent être utilisés à des fins thérapeutiques ou scientifiques. Mais ***ce n'est pas alors la volonté de l'intéressé qui rend le prélèvement possible****, l'idée d'un consentement présumé à défaut d'opposition exprimée étant* ***un leurre juridique****. C'est en réalité la loi qui, dans* ***une politique favorisant le recueil d'éléments et produits du corps humain, permet leur utilisation*** *tout en réservant la possibilité, par une réactivation de la volonté individuelle, d'y faire barrage* »[1671].

Indépendamment des seules hypothèses de traitement de données, le consentement à l'échange et au partage d'informations dans le cadre de l'équipe de soins est, par exemple, présumé[1672]. Il n'en est pas de même du fait justificatif prévoyant la possibilité de révéler une

---

Université Paris Ouest- Nanterre la Défense (Paris X), soutenue le 1 juil. 2009, spéc. n° 301 et suivant) dans laquelle l'auteur explique les arguments en faveur d'une distinction entre présomption de consentement et opposition, rejoint les travaux de Madame Thouvenin (notamment D. THOUVENIN, « L'obtention des organes : le don comme finalité et le prélèvement comme modalité », *in* B. FEUILLET-LE MINTIER (ss. la dir.), *Les lois « bioéthique » à l'épreuve des faits. Réalités et perspectives*, PUF, 1999 ; *Consentement présumé ou droit d'opposition au prélèvement d'organes sur personne décédée : un exemple de conflit entre représentations communes et règles juridiques*, Rapport ronéotypé à l'Établissement français des greffes, mars 2004). Madame Thouvenin considère notamment que le rapprochement de l'opposition et de la présomption de consentement par la référence au *don* a pour but de donner l'illusion d'un rôle de la volonté de la personne : « *L'avantage d'une telle présentation tient à ce que c'est la personne elle-même qui est le moteur de l'obtention des organes, les médecins qui effectuent le prélèvement apparaissant comme les exécutants fidèles de sa volonté. On comprend mieux dès lors l'utilité d'évoquer le « consentement présumé* », *car cette formulation se référant implicitement à la volonté de la personne, maintient un rôle actif et premier à cette dernière. Il permet ainsi de rendre secondaire le rôle du médecin…* » (*Ibid.* p. 29 – *Adde* V. ZAGURY, *Regards sur le droit d'opposition extrapatrimonial : contribution à l'étude de la volonté en droit privé*, *op. cit.*, n° 304). Cet auteur ajoute que le don « *qui est présenté comme fondé sur la volonté individuelle a pour fonction de masquer la nécessité du prélèvement opéré par des médecins dans des conditions bien peu respectueuses des droits pourtant reconnus à toute personne par le Code civil* » (*Ibid.* p. 77 – *Adde* V. ZAGURY, *Regards sur le droit d'opposition extrapatrimonial : contribution à l'étude de la volonté en droit privé*, *op. cit.*, n° 304). Pour Monsieur Zagury, « *L'assimilation opérée entre l'opposition et la présomption de consentement est révélatrice d'un glissement à la fois méthodologique (au lieu de définir positivement la notion d'opposition, l'on insiste sur les conséquences attachées à son non-exercice), symbolique (l'on entretient l'illusion d'une volonté qui décide) et technique (l'on procède à la confusion du silence et de la volonté tacite)* » (*Ibid.,* n° 307).

[1671] G. LOISEAU, « Le contrat de don d'éléments et produits du corps humain. Un autre regard sur les contrats réels », *D.* 2014, p. 2252.

[1672] CSP, art. L. 1110-4, III, al. 1. Le texte précise en effet que les informations sont *réputées confiées* à l'ensemble de l'équipe. La présomption de consentement est explicite. Madame Thouvenin explique notamment que l'examen des articles du Code civil permet de mettre en exergue les caractéristiques de la présomption de consentement « […] *leurs énoncés précisent explicitement que tel fait ou telle situation juridique sont présumés être conformes à celles qu'ils décrivent* […]*; et chaque fois le texte dit "la loi présume que", "est présumé", "est réputé", est "censé", "est tenu pour" ceci ou cela; chaque texte est rédigé sur le mode affirmatif* » (D. THOUVENIN, *Consentement présumé ou droit d'opposition au prélèvement d'organes sur personne décédée : un exemple de*

information, en cas de pronostic ou de diagnostic grave, à la famille, aux proches ou à la personne de confiance du malade, *sauf opposition de sa part*[1673].

S'agissant spécifiquement du traitement des données, nous avons pu expliquer qu'un *décloisonnement* majeur a été prévu par l'une des lois formant le triptyque des lois bioéthiques[1674], entre les activités de soin et la recherche ayant une finalité autre que l'intérêt direct de la personne concernée. Les relations entre recherche, soin et traitement des données de santé à caractère personnel sont en réalité infiniment plus complexes[1675]. Sous l'angle de notre développement, le texte portant justification est prévu à l'article 68 de la LIL tandis que l'article 75, s'appliquant uniquement au traitement à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé prévoit que la personne concernée peut « *s'opposer à la levée du secret* »[1676]. Par ailleurs, l'article R. 1461-9 du Code de la santé publique précise le domaine d'application de ce droit d'opposition s'agissant de l'accès au SNDS. Il ne s'applique que pour les traitements ayant des finalités de recherche, d'étude ou d'évaluation répondant à un motif d'intérêt public (art. L. 1461-3 CSP) ou à des finalités prévues au III de l'article L. 1461-1 du même Code[1677]. Or, il importe de relever qu'il ne s'agit pas d'une hypothèse de

---

conflit entre représentations communes et règles juridiques, *op. cit.* p. 69). On en trouve un exemple dans le Code pénal à l'article 226-1 *in fine* prévoyant une présomption de consentement à la captation d'image ou de parole dans un cadre privé : « *Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé* ».

[1673] CSP, art. L. 1110-4-V, al. 2.

[1674] Loi n°94-654 du 29 juillet 1994 relative au don et à l'utilisation des éléments et produits du corps humain, à l'assistance médicale à la procréation et au diagnostic prénatal ; Loi n° 94-653 du 29 juillet 1994 relative au respect du corps humain ; Loi n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[1675] V. *supra* n° 302. La frontière, poreuse, entre recherche et soin pose des questions d'ordre éthique qui se traduisent en droit, ce qu'explique notamment Madame Supiot dans l'article précité. Mais elle pose également des questions plus éloignées du droit et qui relèvent de la mise en conformité à la loi informatique et libertés, la *compliance*. Les acteurs du monde de la santé cherchent des solutions principalement techniques et organisationnelles pour assurer une mise en conformité, avant même l'entrée du règlement européen (A. BURGUN, A.-S. JANNOT, B. RANCE, M.-F. MAMZER, « Partage des données patients pour la recherche : aspects organisationnels et éthiques », *Ethics, Médecine and Public Health* 2016, n° 2, p. 435-441).

[1676] Ce texte est issu de la loi du 20 janvier 2018, auparavant aucun droit d'opposition n'était prévu.

[1677] « *1° A l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité ;*
2° A la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale ;
3° A la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales ;
4° A l'information des professionnels, des structures et des établissements de santé ou médico-sociaux sur leur activité ;
5° A la surveillance, à la veille et à la sécurité sanitaires ;
6° A la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale. »

transmission mais *d'accès*. Le fait, souligné plus avant[1678], que le régime de la loi informatique et libertés réponde à la nature des données et non aux opérations de traitement crée ici une confusion. L'*accès* aux données n'est pas le fait du professionnel soumis au secret. Il n'a pas la maîtrise des données auxquelles les chercheurs accèdent par le biais du SNDS. Il faut donc distinguer : dans le cas où le professionnel soumis au secret *transmet* à un organisme de recherche les données personnelles de santé qu'il recueille à l'occasion de son activité, il s'agit bien d'une permission légale telle que prévue à l'article 68 de la LIL ; dans le cas d'un *accès*, la question est autre. L'absence d'opposition, dans le premier cas, est un élément de justification de l'infraction de violation du secret professionnel, tandis que dans le second cas, il s'agit d'un droit d'opposition à l'accès, ce que nous envisagerons ultérieurement.

349. Le choix entre consentement et droit d'opposition : un instrument de hiérarchisation des intérêts. Plutôt qu'un affermissement du rôle du consentement comme élément justifiant la violation du secret professionnel, nous constatons une affirmation croissante du droit d'opposition[1679] à la transmission des données issues des activités de prévention, de diagnostic, de soins ou d'un suivi social et médico-social. Les fonctions du droit d'opposition ont été mises en exergue par Monsieur Zagury[1680]. Cet auteur a démontré que le droit d'opposition, dans sa dimension fonctionnelle, visait à procéder à une hiérarchisation des intérêts. Plus encore, c'est le choix entre *consentement* et *opposition* qui révèle de la hiérarchisation des intérêts en jeu. L'auteur explique que l'intérêt de l'*opposant* est secondaire par rapport à l'intérêt de celui contre lequel s'exerce l'opposition, à savoir, en ce qui nous concerne, le responsable du traitement, qu'il s'agisse d'une personne publique ou privée.

[1678] V. *supra* n° 141.

[1679] Monsieur Zagury explique notamment que l'opposition ne peut être qualifiée ni de « faculté », ni de « pouvoir », ni de « liberté ». Il explique : « *L'opposition extrapatrimoniale est une prérogative juridique qui permet à son titulaire d'interdire, par le biais d'une manifestation de volonté purement négative et distincte du consentement, la réalisation d'une pratique déterminée. L'acte d'opposition qui assure la mise en mouvement de ce droit subjectif d'opposition extrapatrimonial peut d'abord être qualifié d'acte juridique unilatéral. La manifestation de volonté du seul titulaire de la prérogative d'opposition permet en effet de créer une obligation de ne pas faire à la charge d'un individu ou d'un groupe d'individus devenus débiteurs d'une abstention d'agir. Il peut ensuite être qualifié d'acte prohibitif en ce sens qu'il vient poser un interdit et contrecarre la réalisation d'une activité précisément déterminée dont la réalisation était jusque-là envisageable. Enfin, l'acte d'opposition par lequel le droit d'opposition se réalise peut être qualifié d'acte accessoire affecté à la réalisation d'un droit substantiel de nature extrapatrimoniale dont il favorise la réalisation effective* » (V. ZAGURY, *Regards sur le droit d'opposition extrapatrimonial : contribution à l'etude de la volonté en droit privé*, *op. cit.*, n° 352).

[1680] *Ibid.*

Concernant la fonction de l'opposition en matière de traitement de données à caractère personnel, il affirme qu'elle conduit à favoriser l'impératif de circulation des données[1681]. Ceci est particulièrement vrai dans le système de santé. L'objectif de compromis, décrit plus avant, se trouve donc également servi par le droit d'opposition en ce qu'il traduit – s'agissant spécifiquement de la recherche scientifique dans le domaine de la santé – la volonté de trouver un équilibre « *entre l'utilité collective pour la recherche et pour l'économie de la santé des données individuelles et la défense des droits de la personne* »[1682]. Toujours selon Monsieur Zagury, cela « *justifie par conséquent cette orientation législative particulière, la consécration d'un droit d'opposition, et le rejet corrélatif qu'elle porte en germe : la mise à l'écart du consentement* »[1683].

350. Le choix entre consentement et droit d'opposition : un instrument au service de l'efficacité des dispositifs techniques servis par les données. Le glissement de la nécessité d'obtenir le consentement de la personne à la transmission de ses données vers un simple droit de s'opposer s'explique aussi par l'avantage pratique que cela recèle. C'est ce qui ressort notamment des travaux préparatoires de la loi de modernisation de notre système de santé, à propos de l'hébergement des données de santé : « *dès lors qu'un médecin ou un hôpital a décidé de sous-traiter l'hébergement de son système d'information, il lui est raisonnablement impossible en pratique de stocker chez lui le dossier d'un patient qui refuserait l'hébergement* »[1684]. Lorsque le législateur favorise l'opposition au consentement, il admet comme étant supérieure l'efficacité du dispositif par rapport à l'autonomie de la personne. L'individu qui souhaiterait que ses données ne soient pas transmises à un hébergeur ne peut s'y opposer que pour un motif légitime. La recherche d'un équilibre se traduit ici par un compromis dont l'autonomie personnelle sort perdante, au profit de l'effacité du dispositif technique. Ce choix est encore plus perceptible s'agissant de l'accès aux données issues de la relation de soin, ce dont nous devons traiter à présent.

351. Un choix politique généralisé en matière de traitement de données à caractère personnel dans le domaine de la santé. Si nous nous éloignons de la question du secret professionnel, il apparaît que le consentement n'est pas au fondement des règles juridiques qui

---

[1681] *Ibid.* n° 411 et svt.
[1682] Rapport n° 3526 déposé le 9 janvier 2002 par Monsieur G. GOUZES, p. 70.
[1683] V. ZAGURY, *Regards sur le droit d'opposition extrapatrimonial : contribution à l'etude de la volonté en droit prive*, *op. cit.*, n° 419.
[1684] Rapport n° 2673 fait au nom de la commission des affaires sociales sur le projet de loi relatif à la santé, p. 485.

guide le traitement des données à caractère personnelle dans le domaine de la santé. Le traitement et la réutilisation des données dans ce domaine sont principalement accompagné d'un droit d'opposition de la personne. Le CCNE, dans son avis n° 129 préalable à la révision de la loi bioéthique, opère un parallèle entre l'opposition au traitement des données dans le domaine de la santé et l'opposition au prélèvement d'organes « *La création d'une plate-forme nationale sécurisée de collecte et de traitement des données de santé constitue une piste intéressante pour articuler entre eux les différents enjeux éthiques afférents aux données de santé. La définition du mode d'alimentation de cette plate-forme relèverait d'un niveau législatif si le choix était fait de mettre en œuvre un mécanisme de consentement présumé dans le cas d'un intérêt public pour la santé du type de celui existant en matière de prélèvement d'organes. Un tel choix permettrait plus de lisibilité et d'efficacité dans le fonctionnement du dispositif dans son ensemble* »[1685]. Notons par ailleurs que le Comité postule de l'intérêt d'un traitement accru des données, du développement de l'intelligence artificielle à partir de celles-ci et les potentialités pour la médecine personnalisée[1686].

352. Conclusion de section. Les limites du secret professionnel, l'intérêt public, l'intérêt général. La force de la norme pénale est l'objet de conciliations qui se traduisent par de multiples dérogations légales, qu'il s'agisse de permissions ou d'obligations de révéler. Par ailleurs, le rôle de la volonté de la personne dans les textes justifiant la révélation semble aller à rebours du mouvement favorable à une autodétermination informationnelle, sans pour autant

---

[1685] CCNE, Avis n° 19, *Contribution du comité consultatif national d'éthique à la révition de la loi bioéthique*, 18 sept. 2018, p. 103.

[1686] « *Le développement du numérique, dont la diffusion s'accélère dans tous les secteurs de la santé, est un fait majeur pour la santé, la recherche et l'organisation des soins* » (*ibid.* p. 10). A propos de ce rapport Madame Beviere-Boyer met justement en balance le discours timoré sur le consentement « *le rapport envisage la pertinence du consentement des personnes concernant le recueil, le stockage, l'accès et l'exploitation des données de sante à l'égard de leur traitement, notamment concernant la recherche medicale et le développement d'algorithmes. En termes de restriction de l'accessibilite de telles données, particulièrement dans le cadre des maladies orphelines, il estime que ce serait pénalisant pour la recherche. Il note toutefois qu'il existe, en parallele, de possibles pressions au détriment des individus concernés* » et celui sur l'apport de la réutilisation accrue des données « *toutefois, en parallèle le rapport note l'importance de l'innovation par la collecte et le traitement des données de santé qui ne devrait pas être trop restreinte dans la mesure ou peuvent en decouler des applications profitables a la sante des citoyens. A ce titre, la valorisation des donnees de sante reste un enjeu majeur, laquelle peut être envisagée par la creation d'un health data hub national, nouvelle plateforme des données plus accessibles au profit de la recherche et de l'innovation* » (B. BEVIERE-BOYER, « Bioethique : la creation du health data hub national peut-elle contribuer à renforcer la protection des donnees sensibles de sante ? », avril 2019, disponible sur : <https://managersante.com/2019/04/15/les-potentialites-demultipliees-des-donnees-sensibles-de-sante-necessitant-une-protection-renforcee/>).

préserver le secret professionnel. Cela ne signifie pas que la personne ne dispose pas de prérogatives sur les données issues de sa prise en charge et donc couvertes par le secret –là n'est pas notre propos –, mais lorsqu'il s'agit de favoriser la circulation de celles-ci, cette volonté n'est pas prégnante. C'est l'intérêt servi par la circulation des données qui prime. Si nous avons, jusqu'ici évoqué indifféremment l'intérêt public et l'intérêt général, ou plutôt que nous avons considéré que l'intérêt public et l'intérêt général se rejoignaient, nous avons également reproduit les propos particulièrement critiques de Madame Frison-Roche à propos de la distribution entre intérêt général et intérêt particulier, qui considère que « *le jeu de puissance* » consiste « *à s'approprier la défense du plus élevé* »[1687], au détriment de l'intérêt particulier. L'important n'est pas tant de constater que lorsque la transmission des données couvertes par le secret est justifiée par un intérêt public compris comme général, l'intérêt privé protégé par le secret professionnel est considéré comme secondaire, mais de remarquer que les intérêts qui sont privilégiés s'ils sont publics, ne sont pas toujours généraux, et que l'intérêt privé rejoint l'intêret public. Il en est ainsi de l'impératif de maîtrise des dépenses de santé[1688], de la recherche[1689], du progrès technique[1690]. Pour reprendre les propos de Monsieur Moor :

> « *Il y a derrière chacun de ses éléments* [de l'intérêt public]*, non plus la « volonté générale », la « nation », mais le conglomérat de tous les intérêts privés qui, d'une manière ou d'une autre, y sont liés. Il y a hybridation des divers intérêts publics et des intérêts privés qui, tour à tour, s'y rattachent. Ainsi relativisé, l'intérêt public perd sa majesté et manifeste de qui, de quel groupe, de quel milieu il relève et par qui – outre l'autorité – il est défendu. Sa fonction idéologique unifiante s'est évaporée : la réalité juridique a rejoint la réalité politique. L'intérêt public n'est plus (seulement, ni principalement) ce qui s'oppose aux intérêts privés, et leur distinction ne permet plus de tracer la frontière censément constitutive (et constitutionnelle) entre l'État et la société civile, celui-là ayant pour fonction (intérêt public) de permettre à celle-là (intérêts privés) de se déployer librement en tant qu'elle-même, selon ses propres règles. Bien au contraire : la société est immédiatement intéressée à l'efficacité de l'administration dans la gestion des ressources dont elle a besoin pour être elle-même.*

[1687] V. *supra* n° 327-328.
[1688] V. *supra* n° 334.
[1689] M.-A. FRISON-ROCHE, « Critère des intérêts et secret professionnel », *op. cit.*, p. 80.
[1690] En ce que le développement des technologies n'est pas l'apanage de l'Etat et que les intérêts privés des entreprises se confondent dans l'intérêt public et rejoignent parfois l'intérêt général.

Par définition, il ne peut plus y avoir de frontière. […] *L'intérêt privé ne peut dès lors plus être conçu comme le splendide produit de la conscience d'un sujet en soi et pour soi, qui légitime de par ce seul fait sa propre valeur universelle.* […] *Il ne peut plus se prétendre autonome sous la seule réserve de restrictions que l'État lui imposerait du dehors et qui seraient contraires à sa nature propre. Bien au contraire : ces restrictions – qui ont de leur côté perdu l'apparente virginité de l'intérêt public comme pure référence à la généralité de la collectivité comme un ensemble homogène – sont toujours aussi la manifestation d'un intérêt privé autre. Si le terme d'intérêt général devait conserver un sens au-delà de la phraséologie des discours politiques, ce serait peut-être pour désigner les points de convergences entre les doubles mouvements qui amèneraient intérêts publics et privés (les deux au pluriel !) à se rejoindre pour se confondre plus ou moins transitoirement avant de se disjoindre à nouveau* »[1691].

Section 2 - Des données devenues communes

353. Le domaine de l'opposition du secret professionnel. L'une des spécificités qui rendent l'étude du secret professionnel ardue tient au fait que lorsqu'on évoque le secret professionnel, ce n'est pas uniquement sous son aspect répressif mais également comme une attitude de résistance[1692]. Si l'incrimination sanctionne la révélation, la majorité du contentieux relatif au secret professionnel, et également du secret professionnel médical, relève des juridictions civiles et administratives[1693]. De plus, même devant les juridictions pénales, la problématique porte non pas sur la sanction d'une révélation mais sur le fait de savoir si la personne soumise au secret professionnel peut garder le silence[1694] lorsqu'elle a *opposé* son

[1691] P. MOOR, *Pour une théorie micropolitique du droit*, PUF, 2005, « Chapitre IV. Intérêts publics et intérêts privés », n° 5.7.
[1692] « *Il est assez facile d'exposer au professionnel qu'il lui est presque toujours interdit de prendre l'initiative de révéler à un tiers ce que la confiance de leur interlocuteur lui a permis de connaître, il est plus délicat de définir l'attitude à avoir lorsque la justice ou toute autre administration souhaite avoir accès au secret qu'il détient* » (B. PY, « Secret professionnel : le syndrome des assignats ? », *AJ pénal* 2004, p. 133) ; dans le même sens M.-A. FRISON-ROCHE (ss. la dir.), *Secrets professionnels*, éd. Autrement, 1999, pp. 18-19.
[1693] D. THOUVENIN, *Le secret médical et l'information du malade*, PUL, 1982, p. 107 et svt.
[1694] La dernière étude quantitative relative aux poursuites pour violation du secret professionnel n'est pas récente, mais les poursuites pour violation du secret professionnel

secret professionnel, ce qui a parfois été présenté comme un *droit au silence*[1695]. Il s'est trouvé, et se trouve régulièrement, des hypothèses dans lesquelles le professionnel est sollicité, que ce soit par l'administration, une personne publique, une autorité quelconque telle que la justice, afin qu'il témoigne, déclare ou transmette des informations ou des données. Il faut distinguer ces cas de ceux dans lesquels il existe soit une obligation spécifique[1696] de révéler, celle-ci pouvant parfois donner lieu à des sanctions[1697], soit une simple permission de révéler, le professionnel devant lui-même faire la pesée des intérêts en présence afin de décider de celui qu'il entend sacrifier[1698], la permission justifiant alors la révélation. Dans ce dernier cas il ne pourra être sanctionné ni pour avoir révélé l'information ni pour s'être tu[1699].

Outre ces faits justificatifs spéciaux, des faits de non-dénonciation, qu'il faut également distinguer de ce *droit au silence*, sont par exemple prohibés, à l'exception des personnes soumises au secret professionnel[1700]. Certains auteurs affirment alors que le secret professionnel justifie la commission d'infractions prévoyant une obligation générale de signaler ou de

---

[1695] M. DELMAS-MARTY, « Le droit au silence en procédure pénale », *in Mélanges en l'honneur de Jacques Teneur*, Université du droit et de la santé de Lille, 1977, p. 273. ; J.-L. BAUDOUIN, *Secret professionnel et droit au secret dans le droit de la preuve. Etude de droit québécois comparé au droit français et à la common law*, LGDJ, 1965 ; B. PY, *Rep. pén.*, *V°* « Secret professionnel », févr. 2003 (act. fév. 2017), n° 78 et svt.

[1696] Spécifique, dans la mesure où elles visent expressement une obligation de révéler pour les professionnels soumis au secret.

[1697] C'est par exemple, en matière médicale, le cas des maladies à déclaration obligatoire (CSP, art. L. 3113-1). Il existe néanmoins des incertitudes sur le fait de savoir si la déclaration de certaines maladies consiste en un ordre de la loi et constitue donc une obligation pour le médecin ou une simple autorisation dès lors qu'aucune sanction n'est prévue dans le cas où la transmission n'est pas effectuée (en ce sens, S. HOQUET-BERG et B. PY, *La responsabilité du médecin*, coll. « Droit professionnel », HDF, 2006, n° 303 ; P. MISTRETTA, *Droit pénal médical*, Cujas, 2013, n° 534).

[1698] Ce que la doctrine a désigné sous le terme d'« option de conscience » (F. ALT-MAES, « Un exemple de dépénalisation : la liberté de conscience accordée aux personnes tenues au au secret professionnel », *RSC* 1998, p. 301 ; Y. MAYAUD, « La condamnation de l'évêque de Bayeux pour non-dénonciation, ou le tribu payé à César », *D.* 2001, chron. p. 3453 ; A. LEPAGE, « Droit pénal et conscience », *Dr. pén*. 1999, chron. 1 ; B. PY, *Rep. pén.*, *V°* « Secret professionnel », *op. cit*., n° 154 et svt.

[1699] S'agissant spécifiquement du secret professionnel médical, Monsieur Mistretta explique que la liberté de conscience du médecin s'est accrue au cours des années, les permissions de révéler étant de plus en plus nombreuses. L'auteur souligne que cet accroissement « relativise grandement la portée actuelle du secret professionnel » (P. MISTRETTA, *Droit pénal médical*, Ed. Cujas, 2013, n° 535).

[1700] Il en est ainsi de la sanction prévue pour toute personne qui ne témoignerait pas en faveur d'un innocent (CP, art. 434-11) ou qui refuserait de témoigner après avoir publiquement déclaré connaître les auteurs d'un crime ou d'un délit (CP, art. 434-12). Est également puni le fait de ne pas dénoncer un crime alors qu'il est encore possible d'en prévenir ou d'en limiter les effets ou lorsque les auteurs sont susceptibles d'en commettre de nouveaux qui pourraient être empêchés (CP, art. 434-1). Est encore puni le fait de ne pas informer les autorités judiciaires ou administratives de privations, de mauvais traitements ou d'atteintes sexuelles infligés à des personnes vulnérables (CP, art. 434-3).

communiquer des informations[1701], d'autres soulèvent l'ambiguïté de la jurisprudence, le juge ayant parfois écarté ces dispositions, notamment en ce qui concerne le secret professionnel des ministres du culte[1702]. Enfin, Mesdames Lepage et Matsopoulou soulignent les difficultés d'interprétation découlant des obligations contradictoires de se taire et de révéler, admettant que celles-ci « *paraissent se neutraliser réciproquement, le législateur déléguant ainsi à la conscience de chaque professionnel le soin de faire le choix qui lui paraît le mieux adapté à la situation dont il est à même d'apprécier les tenants et les aboutissants* »[1703].

En dehors des cas dans lesquels une infraction prévoit expressement une justification tirée de la soumission au secret professionnel ou sanctionne une non-dénonciation qui laisse *a priori* le professionnel libre de décider, l'article 109 du Code de procédure pénale énonce : « *Toute personne citée pour être entendue comme témoin est tenue de comparaître, de prêter serment et de déposer sous réserve des dispositions des articles 226-13 et 226-14* »[1704]. En dépit de la formulation laissant penser qu'il existerait une dispense de témoigner pour toutes les personnes soumises au secret[1705], le juge paraît décider au cas par cas des secrets qui entraînent une dispense absolue de témoigner et de ceux où, au contraire, l'obligation de témoigner l'emporte

---

[1701] En ce sens, E. DREYER, *Droit pénal spécial*, coll. Cours magistral, 3e éd., Ellipses, 2016, n° 46 ; Ph. CONTE, *Droit pénal spécial*, coll. Manuel, 4e éd., LexisNexis, 2013, n° 358.

[1702] C'est ainsi que Messieurs Pradel et Danti-Juan interprètent la décision du tribunal correctionnel de Caen de condamner un évêque pour non-dénonciation de mauvais traitements et d'atteintes sexuelles sur mineurs de quinze ans (J. PRADEL et M. DANTI-JUAN, *Droit pénal spécial*, coll. Référence, 7e éd., Editions Cujas, 2017, n° 314). Nous n'adhérons pas à cette interprétation puisque le tribunal avait considéré que les informations que l'évêque tenait d'un tiers à propos d'un prêtre de son diocèse ne pouvait être qualifiées d'informations à caractère secret : « *En refusant la qualité d'informations confidentielles, le tribunal évitait d'ouvrir le débat sur le point de savoir si l'évêque pouvait ou devait signaler les actes connus de lui. D'aucuns pourraient voir dans cette interprétation particulièrement stricte une volonté tacite de contrecarrer la hiérarchie textuelle des valeurs protégées. Admettre que Monseigneur Pican était informé à titre professionnel aurait empêché toutes poursuites pour non-dénonciation de crime car sont exceptées du champ d'application de ces incriminations* « les personnes astreintes au secret dans les conditions prévues par l'article 226-13 » (B. PY, « Secret professionnel : le syndrome des assignats ? », *op. cit.*).

[1703] Les auteurs notent encore qu'il demeure des incertitudes au regard de l'absence de symétrie entre l'article 226-14, 1° du Code pénal et l'article 434-3 du même code (A. LEPAGE et H. MATSOPOULOU, *Droit pénal spécial*, coll. Thémis Droit, PUF, 2015, n° 551).

[1704] CPP, art. 109. Peuvent être intréprétés dans le même sens les articles 326 et 438 du même code (E. DREYER, *Droit pénal spécial*, *op. cit.*, n° 416). Une disposition identique existe en matière civile, à l'article 206 du Code de procédure civile. Cet article prévoit une exception pour un « motif légitime ». Il ne fait pas de doute que le secret professionnel constitue un tel motif (En ce sens M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, th. dact. ss la dir. de A. PROTAIS, soutenue le 17 déc. 2004, Université de Lille II, n° 179).

[1705] La mention des articles 226-13 et de 226-14 du Code pénal envoyant néanmoins « *un signal contradictoire* » au professionnel puisque le premier texte réprime la violation du secret professionnel tandis que le second justifie la révélation de certains fait (A. LEPAGE et H. MATSOPOULOU, *Droit pénal spécial*, *op. cit.*, n° 550).

sur le devoir de garder le silence[1706]. C'est principalement sur ce point que l'on a pu évoquer un *droit au silence* ou une *opposition* du secret professionnel. Pour Madame Larguier, le professionnel devient alors un « *législateur des cas particuliers* »[1707], tandis que Madame Thouvenin qualifie le médecin de « *maître de la qualification de l'élément matériel de l'infraction* » puisqu'il est « *libre de parler ou de ne pas parler* »[1708]. Certaines demandes de l'administration pouvant paraître légitimes interrogent également les limites du silence qu'impose le secret professionnel. L'on pourrait considérer que cela relève du fait et non du droit, puisque cette attitude ne peut alors être qualifiée juridiquement, elle n'est que le respect de son obligation par le professionnel. Il appert toutefois que la résistance du professionnel, dont la revendication d'un droit au silence est contestée devant le juge, a constitué un sujet intarissable pour la doctrine, dans le prolongement de la question du fondement du secret professionnel[1709]. Le législateur ayant pris acte des ces difficultés, certains textes prévoient expressément l'impossibilité, pour le professionnel, d'opposer le secret, soit dans des textes prévoyant spécifiquement un accès aux informations, soit dans les textes de désignation.

Un sentiment général ressort inexorablement de ces quelques remarques : lorsqu'il s'agit d'analyser les limites du silence du professionnel, l'unité qui se dégage de l'étude de l'infraction se délite, le fait d'évoquer *les secrets professionnels* et non *le secret* professionnel retrouve son intérêt didactique. Dans le cadre de nos développements, il s'agira de constater, d'une part, que certaines personnes soumises au secret professionnel pour des raisons techniques, voient leur possibilité d'opposer leur secret réduite **(paragraphe 1)**, d'autre part, que les possibilités, pour

---

[1706] S'il est difficile de trouver une cohérence d'ensemble, les juges ont pu affirmer qu'étaient dispensés de témoigner le notaire (CA Paris, 13 juillet 1973 : *D.* 1974, p. 16, note E.-S. de la MARNIERRE), l'avocat en fonction de son activité, c'est-à-dire selon qu'il exerce les droits de la défense ou non (A. LEPAGE et H. MATSOPOULOU, *Droit pénal spécial*, *op. cit.* n° 550 ; Cass. crim., 25 oct. 1995 : *Bull. crim.*, n° 323), et le médecin (Cass. crim., 8 mai 1947 : *D.* 1948, p. 109, note P. GULPHE, *JCP* 1948, I, 4141, note A. LEGAL ; Cass. crim. 22 déc. 1966, *D.* 1967, p. 122, note R. COMBALDIEU ; *JCP* 1967, II, 15126, note R. SAVATIER ; *RSC* 1967, p. 453, obs. G. LEVASSEUR ; Cass. crim., 5 juin 1985 : *Bull. crim.*, n° 218 ; *D.* 1986, IR, p. 120, obs. J. PRADEL ; *D.* 1988, p. 106, note H. FENAUX). Pour ces trois professions, l'interprétation des décisions fait consensus dans la doctrine : B. PY, *Rep. pén.*, *V°* « Secret professionnel », févr. 2003 (act. févr. 2017), n° 78 et svt ; Ph. CONTE, *Droit pénal spécial*, *op. cit.*, n° 359 ; A. LEPAGE et H. MATSOPOULOU, *Droit pénal spécial*, *op. cit.*, n° 550 ; M.-.L RASSAT, *Droit pénal spécial*, coll. Précis, 8e éd., Dalloz, 2018, n° 515 ; E. DREYER, *Droit pénal spécial*, *op. cit.*, n° 427). Certains auteurs ajoutent à cette liste les assistants sociaux et les ministres du culte (Ph. CONTE, *Droit pénal spécial*, *op. cit.*, n° 359). Il nous semble toutefois que c'est donner une portée exagérée à ces arrêts au regard des particularités de leurs activités (dans le même sens M.-L. RASSAT, *Droit pénal spécial*, *op. cit.*, n° 515).

[1707] A.-M. LARGUIER, *Certificats médicaux et secret professionnel*, Dalloz, 1963, n° 120.

[1708] D. THOUVENIN, *Le secret médical et l'information du malade*, *op. cit.*, p. 83.

[1709] C'est notamment l'objet de la thèse de Monsieur Couturier que nous avons cité à de nombreuses reprises au cours de nos développement, l'on pourra trouver dans ces travaux l'intégralité des théories sur cette question : M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*

l'administration, d'accéder directement à certains traitements de données, contribuent à affaiblir la force du secret professionnel dans le domaine de la santé, en le contournant **(paragraphe 2)**.

§ 1 - Restriction du pouvoir d'opposer le secret professionnel

354. Avant d'envisager le de l'opposabilité du secret professionnel dans le cadre particulier du traitement des données **(B)** il faut revenir brièvement sur l'évolution restrictive de l'opposabilité du secret **(A)**.

A - Les limites du pouvoir d'opposer le secret : généralités et évolutions

355. Si la parole du professionnel soumis au secret ne peut-être forçée, le « secret de l'écrit » est affaibli de longue date **(1)**, à cela s'ajoute une augmentation des textes portant restriction de la possibilité d'opposer le secret professionnel **(2)**.

1 - Faiblesse de l'écrit et preuve

356. Saisies et perquisitions : limites traditionnelles à l'opposition du secret professionnel. La première limitation à la possibilité, pour une personne soumise au secret, d'opposer son *droit au silence* à une demande de communication qui lui serait formulée tient à la nécessité d'enquêter sur les infractions et de poursuivre leurs auteurs. Faute de pouvoir contraindre le professionnel à parler, des moyens juridiques permettent la recherche de la vérité[1710], moyens par lesquels les informations représentées vont être rendues accessibles aux enquêteurs. La jurisprudence considère, de longue date, que le secret professionnel ne peut faire obstacle à la recherche de la vérité lorsque ces moyens juridiques sont employés[1711]. Seule la parole reste donc libre. L'article 81 du Code de procédure pénale prévoit ainsi que le juge d'instruction procède « *à tous les actes d'information qu'il juge utiles à la manifestation de la*

[1710] B. PY, *Rep. pén.*, *V°* « Secret professionnel », *op. cit.*, n° 106 et svt.
[1711] A propos d'une saisie dans un cabinet dentaire : Cass. crim., 8 juin 1966 : *Bull. crim.*, n° 167 ; *D.* 1966, p. 542 ; également à propos de la saisie d'un dossier médical : Cass. crim., 24 avril 1969 : *D.* 1969, p. 637, rapp. F. CHAPAR ; *JCP* 1970, II, 16336, note R. SAVATIER; Cass. crim., 23 mars 1977 : *Bull. crim.,* n° 109 ; *JCP* 1979, II, 19039, note P. CHAMBON ; *RSC* 1977, p. 832, obs. J.-H. ROBERT ; CA Paris, 27 mars 1963 : *D.* 1963, somm. p. 87 ; rappr. Cass. crim., 20 janvier 1976 : *Gaz. Pal.* 1976, 1, p. 308.

vérité. Il instruit à charge et à décharge »[1712]. Une procédure particulière est prévue pour les perquisitions et saisies ayant lieu au cabinet des médecins, notaires et huissiers. En principe, elles s'effectuent « *par un magistrat et en présence de la personne responsable de l'ordre ou de l'organisation professionnelle à laquelle appartient l'intéressé ou de son représentant* »[1713]. Concernant les avocats, la procédure est encore plus encadrée et une opposition peut encore être émise, par l'intermédiaire du référé-bâtonnier[1714]. Par ailleurs, le régime en matière d'instruction préparatoire diffère en fonction de la profession, le secret professionnel des notaires, des avocats, des huissiers et des médecins étant davantage protégé que les autres[1715].

357. Les mesures *ad exhibendum* et secret professionnel médical. En matière civile, et sur la demande d'une partie, le juge peut enjoindre l'autre partie à produire, au besoin à peine d'astreinte, un élement de preuve en sa possession, et peut également enjoindre la production de tout document détenu par un tiers « *s'il n'existe pas d'empêchement légitime* »[1716]. La question s'est posée au juge de savoir si le fait qu'un professionnel soit tenu au secret constituait un empêchement légitime à la production forcée d'une pièce dans le cadre de cette action. Auteur d'une thèse consacrée au secret professionnel, Monsieur Couturier a consacré quelques développements à cette question. Il relève **d'abord** qu'il n'est pas possible, au regard de la jurisprudence, de répondre de manière systématique à cette question : « […] *il est de moins en moins évident que le secret professionnel soit de nature à constituer en soi un empêchement légitime* »[1717] et il apparaît encore que le domaine du secret professionnel revêt une importance particulière pour déterminer s'il constitue ou non un empêchement légitime[1718]. L'auteur relève **ensuite** que le raisonnement du juge semble prendre en considération les fins qui guident l'opposition du secret. Ainsi, le secret professionnel « *ne constituerait donc un empêchement légitime qu'à condition que son invocation soit dictée par la volonté de protéger l'intérêt d'une*

[1712] CPP, art. 81.
[1713] CPP, art. 56-3.
[1714] S. GUINCHARD et J. BUISSON, *Procédure pénale*, coll. Manuel, 11e éd., LexisNexis, 2018, n° 885 et svt.
[1715] CP, art. 99-3. Sur ce point v. C. GUERY et P. CHAMBON, *Droit et pratique de l'instruction préparatoire. Juge d'instruction, chambre de l'instruction*, coll. Dalloz Action, 2018-2019, « Chapitre 542 - Perquisitions et saisies : les procédures particulières », n° 542.41 et svt.
[1716] CPC, art. 11 al. 1.
[1717] M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.,* n° 218.
[1718] En ce sens : « […] *on ne peut pas accorder la même autorité à tous les secrets professionnels et donc,* a fortiori*, leur attribuer une primauté absolue de manière indifférenciée* » (G. LARDEUX, « Le droit à la preuve : tentative de systématisation », *RTD civ.* 2017, p. 1, spéc. II. A. 1. a.).

personne, qu'il s'agisse d'une partie ou d'un tiers au litige »[1719]. **Enfin**, il relève que « *l'on ressent une volonté jurisprudentielle croissante de sanctionner les réticences des professionnels ou même parfois du bénéficiaire du secret lorsque le juge estime que, derrière le refus ou l'opposition à la communication d'une pièce, se dissimule une forme de tactique judiciaire destinée à protéger, au nom de principes louables, des motifs ou des faits blâmables* »[1720]. Certains ont pu en tirer des conclusions quant au caractère justificatif du consentement[1721], mais une telle interprétation ne nous paraît pas pouvoir être admise ni généralisée. Il nous semble qu'il faut ici comprendre le consentement comme l'un des éléments pris en compte pour juger du fait que le secret professionnel n'est pas un empêchement légitime[1722]. Ce qu'il importe surtout de retenir c'est l'affaiblissement patent du secret des informations représentées.

2 - Multiplication des textes portant restriction de l'opposabilité

358. La portée du secret professionnel en cause. C'est à l'occasion d'un article relatif à un mouvement général d'affaiblissement du secret professionnel que Monsieur Py a constaté une augmentation des textes prévoyant expressément l'impossibilité, pour le professionnel soumis au secret, d'opposer celui-ci à certaines autorités[1723]. Ce mouvement est général, il s'observe

---

[1719] M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*, n° 219.
[1720] *Ibid.* n° 220.
[1721] M. CAUCHY et A. DIONISI-PEYRUSSE « Le droit au secret médical et son application en matière d'assurances », *D.* 2005, p. 1313. Si une partie du raisonnement des auteurs nous semble pouvoir être suivie, lorsqu'ils affirment qu'il s'agit, en matière civile, de vérifier la poursuite d'un intérêt légitime pour justifier du fait que le secret profesionnel est un empêchement légitime, nous n'adhérons pas à l'idée selon laquelle « *Les évolutions récentes du droit positif tendent à reconnaître qu'il s'agit d'un droit de la personne. Dès lors, son bénéficiaire pourrait, sous certaines conditions, en avoir la libre disposition* » (*Ibid.*).
[1722] En ce sens : Cass. civ. 1re, 15 juin 2004 : *D.* 2004, p. 2682, note D. DUVAL-ARNOULD ; Cass. civ. 1re, 7 déc. 2004, n° 02-12.539 : *D.* 2005, IR, p. 339 ; Pan. p. 332, obs. N. FRICERO, Pan., p. 403, obs. J. PENNEAU, et Pan, p. 1317, obs. H. GROUTEL ; *AJDA* 2005, p. 167). A l'inverse il a été jugé que le secret professionnel n'est pas un empêchement légitime lorsque l'assuré sollicite lui-même qu'il soit débattu de son état de santé à l'occasion d'un contentieux l'opposant à la CNAMTS. En l'espèce la Cour considère que le secret est un empêchement légitime malgré la demande de la personne concernée par les informations, et ceci au regard de la spécificité du contentieux qui concernait une demande de prestation. Cette solution confirme encore que le consentement n'est qu'un élément parmi d'autres, le fait de solliciter une prestation ne pouvait faire échec à la protection de la profession et donc, au travers d'elle, de la santé publique (Cass. civ. 2e, 13 nov. 2008, n° 07-18.364 : *D.* 2008. AJ, p. 2948 ; *RDSS* 2009, p. 185, obs. T. TAURAN). Un autre arrêt a semblé prendre le contrepied de cette décision : le secret professionnel, en l'espèce, n'a pas été considéré comme un empêchement légitime (Cass., civ. 2e, 22 nov. 2007, n° 06-18.250 : *D.* 2008. AJ, p. 95, et Pan., p. 506, spéc. p. 510, obs. J. PENNEAU), mais il s'agit à notre sens de confirmer, une fois encore, que le consentement n'est qu'un élément d'appréciation.
[1723] B. PY, « Secret professionnel : le syndrome des assignats ? », *AJ pénal* 2004, p. 133.

pour tous les secrets professionnels, aussi bien face aux autorités de police qu'aux magistrats[1724]. A titre d'exemple, pour localiser les prévenus, le procureur de la République peut requérir de toute administration, entreprise, établissement ou organisme de toute nature, qu'elle lui communique tout renseignement en sa possession aux fins de déterminer l'adresse du domicile ou de la résidence du prévenu, sans qu'il soit possible de lui opposer le secret professionnel[1725] . En matière financière et fiscale, plusieurs exemples peuvent être cités et concernent plus spécifiquement le secret professionnel bancaire[1726]. Concernant l'indemnisation des victimes d'infractions, le secret professionnel ne peut être opposé au président aisin qu'aux membres de la commission d'indemnisation des victimes d'infraction (CIVI)[1727]. Quant aux perquisitions et saisies pratiquées lors d'une instruction préalable, certains secrets ne peuvent être opposés au juge d'instruction ou à l'officier de police judiciaire[1728]. Le secret professionnel ne peut pas non plus être opposé aux membres et agents de la CNIL dans l'exercice de leur mission de contrôle[1729]. Dans cette dernière hypothèse, le secret professionnel médical fait figure d'exception dans la mesure où il est prévu qu'il puisse être opposé uniquement pour les informations qui figurent dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé[1730]. Dans ce cas, la communication des données ne peut se faire que sous l'autorité et en présence d'un médecin[1731].

359. Dans le Code de la santé publique, impossibilité d'opposer le secret professionnel dans l'intérêt de la personne. Au sein du Code de la santé publique, plusieurs textes prévoient l'impossibilité d'opposer le secret professionnel à certaines institutions. Il s'agit principalement des restrictions posées afin d'obtenir des informations nécessaires à l'indemnisation des victimes de produits de santé[1732], à l'indemnisation des victimes d'accidents médicaux par la

[1724] *Ibid.*
[1725] CPP, art. 560, al. 4.
[1726] CP, art. 132-22; LPF, art. L. 83; CMF, art. L. 621-9-3 et art. L. 511-33.
[1727] CP, art. 706-6 al. 1.
[1728] CPP, art. 99-3.
[1729] LIL, art. 44.
[1730] Traitement prévu à l'art. 8, 6° LIL.
[1731] LIL, art. 44, III, al. 2.
[1732] CSP, art. L. 1142-24-4 et art. L. 1142-24-11.

commission de conciliation et d'indemnisation des accidents médicaux[1733], et à l'indemnisation des victimes de préjudices directement imputables à la vaccination obligatoire[1734] ou à une transfusion sanguines[1735], par l'office nationale d'indemnisation des accidents médicaux, des affections iatrogènes et des infections nosocomiales (ONIAM). Ces limites à l'opposabilité du secret professionnel font primer l'intérêt de la personne qui demanderait une indemnisation au titre d'un préjudice subi à l'occasion de l'activité de soin ou pour la protection de la santé publique. Il s'agit, ici encore, d'un instrument de hiérarchisation des intérêts.

Le nombre des textes – dispersés dans différents codes et textes non codifiés – incite ainsi à largement relativiser la force du secret professionnel. Il faut admettre, à l'instar de Monsieur Couturier, que « *si les professionnels soumis au secret conservent généralement la maîtrise de leur parole, les écrits qu'ils détiennent s'avèrent de plus en plus accessibles aux investigations des autorités judiciaires et des services administratifs* »[1736]. Cette analyse se vérifie encore au regard des textes de désignation disposant expressément que certaines personnes sont soumises à un secret professionnel *dégradé*.

B - La portée des secrets professionnels fondés sur l'origine des données

360. Une question anecdotique ? Nous avons évoqué, précédemment, que la généralisation de l'utilisation de l'outil informatique et du traitement des données dans le système de santé avait eu pour conséquence d'opérer une transformation des fonctions du secret professionnel, de la protection de la confiance dans la profession vers la constuction de la confiance dans les outils techniques[1737]. C'est également la physionomie générale du secret professionnel qui pourrait en être modifiée, puisqu'en dehors des quelques professions historiquement soumises au secret, il s'agirait désormais d'affirmer que les personnes ne sont plus astreintes au secret au regard de leur profession mais au regard de la source des données[1738]. Une troisième conséquence de l'extension du champ d'application du secret professionnel dans le domaine de la santé peut être envisagée, au regard du *droit au silence* des professionnels. Nous avons, en

---

[1733] CSP, art. L. 1142-12.
[1734] CSP, art. L. 3111-9.
[1735] CSP, art. L. 3122-2 et art. L. 1221-14, al. 2.
[1736] M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*, n° 222 ; dans le même sens B. PY, « Secret professionnel : le syndrome des assignats ? », *op. cit.*.
[1737] V. *supra* n°305.
[1738] V. *Ibid.*

effet, souligné que la question donnait lieu à une importante casuistique. Or, les limites du secret professionnel des personnes qui y sont soumises en raison de la source des données auxquelles ils ont accès– comme par exemple les acteurs techniques, de plus en plus nombreux, de l'information médicale, les hébergeurs de données de santé – sont difficiles à déterminer. Il est, en effet, impossible de savoir dans quelle mesure ils peuvent opposer le secret professionnel. En d'autres termes, la portée de leur secret professionnel est-elle comparable à celle du secret professionnel des professionnels de santé ? Lorsqu'un texte prévoit la possibilité d'opposer le secret pour les médecins, ces professions sont-elles également concernées ?

L'absence de renvoi à l'article 226-14 du Code pénal dans le texte de désignation de ces acteurs laisse supposer que l'option de conscience laissée aux professionnels de la santé et du social n'est pas offerte aux personnes soumises au secret en raison de l'origine des données auxquelles ils accèdent. Cette restriction s'explique, pour les hébergeurs de données de santé au moins, par la particularité de leur activité. Comme le souligne justement Madame Zorn : « *l'hébergeur est un prestataire technique neutre qui ne doit pas avoir accès aux contenus qu'il héberge. Afin de maintenir une possibilité d'accéder aux données de santé en cas de problème technique ou pour faire droit aux demandes d'accès des personnes concernées (comme les y autorise l'article L. 1111-7 du Code de la santé publique), l'hébergeur doit s'adjoindre les services d'un médecin, seul habilité à accéder à l'information médicale* »[1739]. Aussi, la question, si elle mérite d'être évoquée, peut sembler anecdotique puisque ce sont en général les professionnels de santé ou les établissements ou services de soins qui sont responsables du traitement des données, qu'il s'agisse des données personnelles de santé traitées à des fins de prises en charge où de celles qui sont réutilisées à des fins de recherches. Une clarification relative au champ d'application de l'article L. 1110-4 du Code de la santé publique est néanmoins réclamée par les acteurs de terrain[1740]. Ce qui permettrait au moins de distinguer les secrets professionnels ou de les unifier.

En toutes hypothèses, le mouvement d'affaiblissement de la portée du secret professionnel est d'autant plus évident lorsque les informations sont traitées. Si les informations représentées supposent la communication, les données supposent l'accés. On observe

---

[1739] C. ZORN, *L'hébergement des données de santé sur support informatique*. – *Principes fondamentaux*, Fasc. 10, Droit médical et hospitalier, Litec, 2013, n° 17.

[1740] Cette clarification figure parmis les conditions évoquées par Madame Eon pour permettre l'accélération du numérique en santé (F. EON, « L'accélération du numérique en santé : enjeux et conditions de son succès », *RDSS* 2019, p. 55).

désormais de plus en plus d'hypothèses prévoyant un *accès* aux données, constitutives d'une forme de contournement du secret professionnel dans le domaine de la santé.

§ 2 - La mise en commun des données

361. Si la personne ne maîtrise pas le « secret », que les professionnels voient leur possibilité d'opposer le secret se restreindre. Ces derniers perdent également la maîtrise des données **(A)**. Le mouvement qui se dessine est celui d'une mise en commun des utilités des données produites par le système de santé **(B)**.

A - La perte de maîtrise progressive des données

362. Le professionnel ne peut opposer le secret que s'il maîtrise les informations et données dont les tiers cherchent à prendre connaissance **(1)**, au gré des évolutions récentes plusieurs éléments vont dans le sens d'une perte de maîtrise de cette maîtrise **(2)**.

1 - La maîtrise des données, condition de l'opposition du secret professionnel

363. L'opposabilité, manifestation de la maîtrise des informations par les professionnels. A propos de l'opposabilité du secret professionnel médical, Madame Thouvenin remarquait, dans sa thèse de doctorat, que le *droit au silence* des médecins pouvait s'analyser comme la conséquence du statut de gardiens des informations apprises à l'occasion de l'exercice de leur profession[1741]. L'auteur affirmait qu'en tant que « *titulaire d'un pouvoir, le médecin occupe dans les conflits d'intérêts une position-clé* »[1742]. Datée des années 1980, il faut douter que cette analyse pourrait aujourd'hui s'étendre à tous les professionnels désignés par l'article le Code de la santé publique et à ceux, non identifiés, visés par L.1110-4 du Code de la santé publique, elle ne permet plus de décrire l'état du droit positif. La première des raisons tient effectivement à l'extension du champ du secret professionnel provoquant une dilution du pouvoir ; la seconde réside dans le mouvement général d'affaiblissement de l'écrit – sur support papier ou sur support informatique – qui s'accompagne d'une perte de la maîtrise des informations par les professionnels soumis historiquement au secret, ceux de premier rang.

[1741] D. THOUVENIN, *Le secret médical et l'information du malade*, PUL, 1982, p. 107.
[1742] *Ibid.* p. 108.

364. Le professionnel n'a plus la maîtrise des données à caractère personnel et de santé. Il est patent que les professions dont le secret est *véritable* n'ont plus la maîtrise des informations – représentées ou traitées – relatives aux personnes faisant l'objet d'une prise en charge telle que définie au premier alinéa de l'article L. 1110-4 du Code de la santé publique. La première manifestation de cette *perte de maîtrise* tient évidememnt au fait que la personne peut accéder à toutes les informations et données la concernant. L'articulation entre les dispositions relatives aux documents administratifs, celles portant protection des données à caractère personnel et le Code de la santé publique permet de préciser l'étendue de ce droit et les modalités de sa mise en œuvre[1743]. Cette perte de maîtrise des données s'est confirmée, au profit de l'affirmation d'une maîtrise par la personne concernée[1744], particulièrement effective

[1743] L'article L. 1111-7 du CSP précise les modalités d'accès au dossier patient. En cas de refus de l'établissement ou du professionnel, un recours devant la CNIL ou la CADA est possible. S'agissant des dossiers patients, qui sont également des documents administratifs (ceux des établissements publics et des cliniques participant à une mission de service public), la CADA est en principe compétente au regard de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal. Concernant les dossiers médicaux qui constituent des traitements de données mis en œuvre par des professionnels libéraux ou des cliniques privées, la CNIL est compétente. L'apparente simplicité du partage des compétences entre la CNIL et la CADA est trompeuse s'agissant des dossiers patient, d'autant que ces derniers ne sont pas les seuls fichiers ou documents pouvant contenir des informations relatives à la prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social. Un protocole d'accord avait d'abord été pris à la suite de l'arrêt *Bertin* (CE, ass., 19 mai 1983 : *Rec. Lebon,* p. 207) afin de permettre la transmission des demandes d'une commission à l'autre (M. VIVANT, B. WARUSFEL et N. MALLET-POUJOL, *Lamy droit du numérique*, « Partie 2- Numérique et libertés », n° 435). S'agissant du partage des compétences, l'article 311-1 du Code des relations entre le public et l'administration prévoit que la loi informatique et libertés remplace le régime d'accès prévu dans la loi du 17 juillet 1978 (*Ibid.*). Ainsi « *l'accès aux informations nominatives résultant d'un traitement automatisé et contenues dans un fichier, lorsque la demande est formulée par l'intéressé lui-même, en vertu des dispositions de l'article 39 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Dans ce cas, la procédure est entièrement régie par les dispositions de cette dernière loi et fait intervenir la CNIL. Il n'en va pas de même, en revanche, lorsque la demande émane de tiers, en application de l'article 39, I de cette loi. Dans ce dernier cas, ce sont les dispositions de la loi du 17 juillet 1978 qui s'appliquent* » (*Ibid.*). A l'heure actuelle, une grande partie des dossiers patient sont informatisés et constituent des fichiers (LIL, art. 2), si bien que les compétences de la CNIL en la matière sont largement accrues. Par ailleurs, un rapprochement a été effectué entre les deux AAI (bien qu'ayant des statuts différents et beaucoup moins de pouvoir, la CADA est considérée comme telle : J. CHEVALLIER, « Le statut des autorités administratives indépendantes : harmonisation ou diversification ? », *RFDA* 2010, p. 896) à l'occasion de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, qui a modifié la loi informatique et libertés (ancien art. 15 bis LIL devenu art. 14 depuis l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel). Pour des développements complets sur l'articulation entre la LIL et la loi du 17 juillet 1978, v. A. DEBET, J. MASSOT et N. METALLINOS, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, coll. Les intégrales, Lextenso éditions, 2015, n° 94 et svt.

[1744] Nous avons toutefois pu expliquer que cette maîtrise est loin d'être complète v. *supra* n° 348.

s'agissant du Dossier médical partagé puisque la personne peut accéder en ligne à ses données et peut également modifier la liste des professionnels de santé ayant accès au dossier[1745]. Dans le cadre de la stratégie de transformation du système de santé dénommée « Ma santé 2022 », une loi a été adoptée le 24 juillet 2019[1746]. Celle-ci prévoit, suivant les recommandations du comité chargé du pilotage de cette stratégie[1747], la mise en œuvre d'un espace numérique de santé au sein duquel le patient aurait la pleine maîtrise de ses données[1748]. Cet espace comprend le DMP mais également les ordonnances dématérialisées, le carnet de vaccination dématérialisé, la carte de groupe sanguin et la liste des antécédents et des allergies de l'usager. Il contient en outre des données administratives, également relatives à la personne de confiance et les directives anticipées, un agenda de santé, une messagerie sécurisée de santé et les données relatives à l'assurance maladie ainsi qu'éventuellement ses constantes de santé produites par des applications ou des objets connectés référencés au Code de la santé publique ou toute autre donnée de santé utile à la prévention, la coordination, la qualité et la continuité des soins[1749]. Il s'agit de permettre à chaque personne de gérer ses données de santé à caractère personnel, l'espace numérique de santé étant présenté comme un « *nouveau levier au service de la maîtrise des données personnelles de santé* »[1750]. Outre cet outil, l'on constate que la maîtrise sur les données de santé couvertes par le secret n'appartient plus ni aux professionnels intervenant dans la prise en charge, ni à la personne concernée par les données.

2 - Les manifestations de la perte de maîtrise des données

365. La perte de maîtrise des données peut être perçue au travers du mouvement d'accès aux données **(a)** et de la mise en réseau qui conditionne celui-ci **(b)**.

a - L'accès aux données non pseudonymisées

[1745] CSP, art. L. 1111-19.
[1746] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, *JORF* n° 0172 du 26 juil. 2019.
[1747] D. PON et A. COURY, Rapport final : *Accélérer le virage numérique*, disponible sur < https://solidarites-sante.gouv.fr/IMG/pdf/masante2022_rapport_virage_numerique.pdf > (dernière consultation le 21 mai 2019).
[1748] Loi n° 2019-774 du 24 juillet 2019, *op. cit.*, art. 44 et svt. Derrière le discours d'accompagnant et sans verser dans la défiance, il faut souligner qu'il s'agit de maîtriser les données dans cet unique espace. La nature profondemment ubiquitaire des données interdit la généralisation, il n'est pas possible de voir dans ce seul outil la reconnaissance d'une autonomie complète de la personne sur ses données.
[1749] *Ibid.*, art. 45, codifié dans le CSP à l'article L. 1111-13-1.
[1750] F. EON, « L'accélération du numérique en santé : enjeux et conditions de son succès », *RDSS* 2019, p. 55.

366. ***L'accès*****, approche linguistique.** Les termes employés dans les énoncés juridiques ne sont pas toujours définis. Une telle économie se comprend, notamment pour les mots du langage courant, dans la mesure où opérer des définitions en cascade ferait perdre à l'énoncé la clarté qui lui permet d'être compris de tous[1751]. Les énoncés juridiques sont donc en partie construits sur la base d'un « *pari communicationnel* »[1752]. Il importe toutefois de s'interroger sur le sens du terme *accès* que l'on voit fleurir dans les énoncés juridiques, au point qu'il existerait aujourd'hui un *droit d'accès aux documents*[1753] et *aux données*[1754], lequel a pu être qualifié de *nouveau droit fondamental*[1755]. Les enjeux théoriques de l'accès ont fait l'objet de travaux, notamment en droit public et en économie. Nous les aborderons en temps voulu. Il faut, pour l'instant s'arrêter sur sens du terme.

L'accès consiste dans l'« *action ou possibilité d'accéder* »[1756], le verbe *accéder* signifiant le fait d'« *arriver à un terme dont l'approche peut faire difficulté* »[1757]. Dans le vocabulaire informatique, ce mot désigne une « *procédure permettant d'accéder à un élément enregistré dans la mémoire d'un ordinateur* »[1758]. Il nous semble toutefois que, derrière le caractère commun du mot, la définition du verbe *accéder* – dont *l'accès* est l'action – recèle une information centrale pour la compréhension du mouvement qui s'est déployé en droit : accéder suppose une difficulté originaire. Que l'on parle *d'accessibilité* des transports et des lieux aux personnes souffrant d'un handicap[1759], ou encore de l'accès au juge ou à la justice[1760], de l'accès

---

[1751] V. CHAMPEIL-DESPLATS, *Méthodologie du droit et des sciences du droit*, coll. Méthodes du droit, 2e éd., Dalloz, 2016, n° 503.
[1752] V. CHAMPEIL-DESPLATS, *Méthodologie du droit et des sciences du droit*, *op. cit.*, n° 485, 503 et svt. ; Développant l'idée : E. PIC, *Caractérisation de l'anglais des droits de l'Homme en tant que langue de spécialité. Un essai de méthodologie terminologique*, Thèse dact. de linguistique théorique, descriptive et automatique, ss. la dir. de J. HUMBLEY, Université Paris Diderot, 2007, p. 113 et 313).
[1753] V. *supra* n° 49.
[1754] RGPD, art. 15.
[1755] A. GARIN, *Le droit d'accès aux documents : en quête d'un nouveau droit fondamental dans l'Union européenne*, Editions A. Pedone, 2017.
[1756] TLFi, *op. cit.*, *V°* « Accéder ».
[1757] TLFi, *op. cit.*, *V°* « Accès ».
[1758] TLFi, *op. cit.*, *V°* « Accès ».
[1759] Loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées.
[1760] Les travaux sur la question sont innombrables mais l'on peut notamment retenir que le droit à l'accès au juge suppose de lever des obstacles d'ordre économique, juridique, géographique (v. par exemple V. DONIER et B. LAPEROU-SCHNEIDER (ss. la dir.), *Accès au juge : quelles évolutions ?. Recherche sur l'effectivité du droit*, Bruylant, 2013).

aux soins[1761], la mise en œuvre de mesures pour garantir *l'accès* suppose de régler une situation inégalitaire de fait, de lever des difficultés. En cela, l'accès est toujours la condition, pour l'individu, de l'exercice d'autres droits[1762]. Concernant spécifiquement les informations, l'accès aux documents administratifs s'oppose au *secret de l'administration* et constitue une remise en cause de la maîtrise totale de l'administration sur certains documents [1763], tandis que l'accès aux données par les personnes concernées serait une des conditions de l'autodétermination informationnelle, constituant un contre-poids au fait que le responsable traite les données, qu'il soit « *en possession* »[1764] de celles-ci. L'idée étant, selon Jean Foyer, de faire des traitements des « *maisons de verre* »[1765].

A propos de *l'accès aux données*, il a été expliqué, lorsque nous avons évoqué les opérations de traitement, que le terme d'accès pouvait être rapproché de celui de consultation[1766]. Au sein du RGPD, le mot est utilisé de manière générique et participe de syntagmes tels que « *l'accès non autorisé* »[1767], qui vise la consultation illicite des données et au-delà de la consultation, une opération d'ordre technique dont la difficulté dépend de la sécurité des traitements. Egalement, « *l'accès aux données à caractère personnel* »[1768] est utilisé tantôt pour viser *le droit d'accès* que nous venons d'évoquer, tantôt pour désigner le contrôle par le responsable du traitement ou son sous-traitant des personnes pouvant *parvenir* aux données. Enfin, « *l'accès du public aux documents officiels* »[1769] concerne, en France, l'accès aux documents administratifs. En toute hypothèse, le fait de permettre *l'accès* suppose de compenser la maîtrise effective, par le

---

[1761] L'égalité d'accès aux soins, pour être effectif, impose par exemple la mise en œuvre de mesures réduisant les inégalités sociales, géographiques ou la levée d'obstacles juridiques pour accéder à certaines thérapies (sur le droit à l'égal accès aux soins v. B. FEUILLET, « L'accès aux soins, entre promesse et réalité », *RDSS* 2008, p. 713).
[1762] *Ibid.*
[1763] D'où l'idée de *transparence* qui guide les relations entre l'administration et le public depuis la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.
[1764] Comme l'explique Monsieur Netter à propos, spécifiquement, des acteurs de l'internet : « *Les données sont en possession d'entreprises qui les exploitent, et il est trop tard pour s'opposer techniquement à la maîtrise qu'elles exercent. Elles ne relâcheront leur emprise sur ces informations que si elles y sont contraintes par le droit* » (E. NETTER, *Numérique et grandes notions du droit privé*, mémoire présenté pour l'obtention de l'habilitation à diriger des recherches, ss. la dir. de J. ROCHFELD, soutenu le 20 nov. 2017, n° 92).
[1765] Compte-rendu de la séance de l'assemblée nationale du 4 octobre 1977, 1ère séance, première session ordinaire de 1977-1978, n° 79, p. 5783.
[1766] V. *supra* n° 162.
[1767] Nous trouvons cinq occurrences dans le RGPD.
[1768] Nous trouvons huit occurrences dans le RGPD.
[1769] Nous trouvons sept occurrences dans le RGPD.

responsable du traitement, des dispositifs techniques permettant le traitement de celles-ci. Celui qui *accède* ou auquel *l'accès est permis*, est le sujet actif, tandis que la *communication*, la *transmission* d'informations ou de données suppose une action de la part de celui qui est en *possession* des informations. Prenons pour exemple le professionnel de santé : il *accède* aux différents dossiers, dont le patient aurait désormais la maîtrise[1770]. Partant, lorsqu'il est prévu un *accès*, par l'administration, aux données de santé couvertes par le secret, il nous semble qu'il s'agit d'atténuer le *pouvoir* des professionnels et des établissements de santé sur celles-ci en s'assurant qu'ils ne puissent pas opposer le secret. Précisons tout de même que l'*accès aux données* n'implique pas nécessairement un *accès* informatique, il peut également s'agir de permettre l'accès à des documents papier. Il apparaît toutefois que les deux sens du terme, dans le langage commun et informatique, se manifestent en droit : nous constaterons que la *logique d'accès* se déploie pleinement lorsque les données sont *mises en réseaux* ce qui n'est rendu possible que par l'informatique.

367. L'accès aux données couvertes par le « secret médical ». Plusieurs textes mentionnent explicitement un *accès*, par l'administration ou des agences de l'Etat, à des « données couvertes par le secret médical ». Une ordonnance du 19 janvier 2017 prévoit, par exemple, l'accès aux données couvertes par le « secret médical » ou le secret industriel et commercial pour le compte de l'Autorité de sûreté nucléaire et de l'Institut de radioprotection et de sûreté nucléaire (IRSN)[1771]. En vertu de ce texte, les inspecteurs de la radioprotection peuvent accéder aux données couvertes par le « secret médical » ou le secret industriel et commercial dans le cadre des pouvoirs qui leur sont conférés au titre de leur mission d'inspection pour la protection générale de la santé[1772]. L'article L. 1421-3 du Code de la santé publique, cité par l'ordonnance, prévoit notamment que : « *Pour le contrôle des opérations faisant appel à l'informatique, ils ont accès aux logiciels et aux données stockées, ainsi qu'à la restitution en clair des informations propres à faciliter l'accomplissement de leurs*

[1770] CSP, art. L. 1111-17 ; pour les modalités d'accès : art. R. 1111-30 et R. 1111-4 ; concernant le dossier pharmaceutique : art. R. 1111-20-5 ; s'agissant des restrictions d'accès, non plus au dossier médical partagé mais au dossier patient : art. D. 1110-3-1.

[1771] Ordonnance n° 2017-45 du 19 janvier 2017 relative aux conditions d'accès aux données couvertes par le secret médical ou le secret industriel et commercial pour le compte de l'Autorité de sûreté nucléaire et de l'Institut de radioprotection et de sûreté nucléaire et à la mutualisation de certaines fonctions d'agences sanitaires nationales.

[1772] CSP, art. 1333-29.

missions »[1773], tandis qu'il est précisé qu'ils peuvent se faire communiquer tous les documents sur tout support ou procéder à leur saisie. L'accès correspond donc à une forme de saisie informatique. L'emploi du terme *données* s'entend également des informations, sans que soient spécifiquement visées les données faisant l'objet d'un traitement informatique. Il est également prévu que l'IRSN accède, à la demande de l'Autorité de surêté nucléaire, à toute donnée nécessaire à l'expertise demandée par cette dernière. Le texte est passé relativement inaperçu dans la doctrine[1774]. Il s'agissait, ainsi que le relève Monsieur Py, de rendre les secrets visés inopposables[1775]. L'auteur perçoit ce texte comme une manifestation de la tendance contemporaine en matière de sécurité et de veille sanitaire[1776]. Le Code de la santé publique contient, en effet, d'autres dispositions en ce sens. Sans prétendre à l'exhaustivité : en matière de recherches impliquant la personne humaine, outre les personnes les mettant en oeuvre, celles chargées du contrôle qualité de la recherche peuvent accéder aux données couvertes par le « secret médical »[1777] ; l'agence nationale de sécurité du médicament et des produits de santé a également accès aux informations concernant les recherches sur les produits de santé et l'évaluation des soins courants[1778] ; la commission des relations avec les usagers et de la qualité de la prise en charge a, quant à elle, accès, avec l'accord écrit de la personne concernée, « *aux données médicales relatives* [aux] *plaintes ou réclamations* »[1779] ; enfin, pour la certification des établissements, les agents de la Haute autorité de santé n'ont accès « *aux données de santé à caractère personnel que si elles sont strictement nécessaires à l'exercice de leur mission de certification lors de leur visite sur les lieux, dans le respect du secret médical* »[1780].

368. La polysémie du mot *accès* déployée. Au travers des quelques exemples que nous venons d'évoquer, il apparaît que le syntagme « *accès aux données* » ne vise pas toujours les données faisant l'objet d'un traitement automatique. Il nous semble toutefois que l'usage du

---

[1773] CSP, art. L. 1421-3, al. 1.
[1774] Il est néanmoins mentionné par Madame Denizot, au titre des ordonnances modifiant le droit des données de santé : A. DENIZOT, « Droit de la santé : les avalanches de l'hiver 2017 », *RTD civ.* 2017, p. 500 ; B. PY, « Quand la surêté nucléaire atomise un peu plus la notion de secret », *RDS* 2017, n° 77, p. 396.
[1775] *Ibid.*
[1776] *Ibid.* V. encore l'ordonnance
[1777] Art. L. 1121-3 CSP ; également rappelé dans la méthodologie de référence prise par la CNIL concernant le traitement des données pour de telles recherches : Délibération n° 2018-155 du 3 mai 2018 portant homologation de la méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches n'impliquant pas la personne humaine, des études et évaluations dans le domaine de la santé (MR-004), *JORF* n°0160 du 13 juillet 2018.
[1778] CSP, art. L. 1121-1.
[1779] CSP, art. L. 1112-3, al. 3.
[1780] CSP, art. L. 1414-4, al. 6.

terme *accès* est intimement lié au traitement informatisé des données. La mise en réseau, comme forme d'interconnexion entres les traitements et le premier pas vers un **accès aux utilités** des données remplaçant progressivement la logique de reservation du secret professionnel.

b - La mise en réseau condition de la mise en œuvre d'une logique d'accès

369. La mise en réseau des données **(i)** est la condition première d'une généralisation de la logique d'accès **(ii)**.

i - La mise en réseau

370. Les systèmes d'informations informatisés des établissements, première étape. Lorsque nous évoquons le fait de mettre en réseaux les données de santé à caractère personnel au sein des systèmes d'informations informatisés des établissements de santé, nous ne visons pas l'interconnexion des fichiers – dont le potentiel, en termes d'atteinte à la vie privée et à la liberté, à été maintes fois souligné[1781] – ni l'accès aux données au niveau national. Il faut d'abord noter que les systèmes d'information ne sont pas un objet d'étude qui intéresse le droit[1782], il s'agit d'outils de gestion et de management des entreprises et des établissements publics. Les comportements des individus vis-à-vis de ces outils n'emportent pas de conséquences juridiques, et n'intéressent les juristes que lorsqu'il est question de préserver la cybersécurité[1783] ou qu'il est porté atteinte aux systèmes d'information – puisqu'ils entrent dans

---

[1781] Ces « dangers » se trouvent d'ailleurs, selon le récit communémment admis, à l'origine de la loi informatique et libertés et du fichier SAFARI qui « *visait à utiliser un identifiant unique, le « numéro de Sécurité sociale », pour l'ensemble des répertoires et fichiers publics, ce qui ne manquerait pas de favoriser leur « interconnexion* » (CNIL, *Rapport d'activité 1978-1980*, p. 8). Sur la question de l'évolution du débat sur l'interconnexion des fichiers publics v. N. OCHOA, *Le droit des donnees personnelles, une police administrative speciale*, *op. cit.*, p. 110 et svt.

[1782] Relevons tout de même l'existence d'un ouvrage pluridisciplinaire publié par un éditeur juridique au sein duquel, d'ailleurs, le vocable n'est jamais défini : C. HERVE, M. STANTON-JEAN, E. MARTINANT, *Les systèmes informatisés complexes en santé*, coll. Thèmes et commentaires, Dalloz, 2013. Citons également un article dans lequel les systèmes d'information sont analysés afin de souligner leur effet normalisant sur la pratique des soins psychiatriques : C. CASTAING, « Psychiatrie et soins ambulatoires », *RDSS* 2016, p. 77.

[1783] T. DOUVILLE, « L'émergence d'un droit commun de la cybersécurité », *D.* 2017, p. 2255 ; E. GALATRY-ROLIN, « Agence nationale de la sécurité des systèmes d'information (ANSSI) », *JCl. communication*, Fasc. 1000, févr. 2018.

la catégorie des biens[1784] – ou à la protection des données[1785]. Certains systèmes d'information ont toutefois pu faire l'objet d'une attention particulière en raison de leur dimension internationale[1786]. L'importance des systèmes d'information dans la mise en œuvre des politiques de santé est souvent mise en avant et il en est parfois fait mention au détour de recherches en droit public, sans qu'ils ne constituent un sujet d'étude à part entière[1787]. L'étude des conséquences de l'outil et de son usage dans la société, l'entreprise, l'administration ou sur les pratiques professionnelles ne paraît relever pas du droit[1788].

En socio-politique, des recherches sur l'objet *système d'information* ont été entreprises dans les années 1970. Dans un article[1789], puis un ouvrage[1790], les sociologues Pierre Gremion et Haroun Jamous ont envisagé les systèmes d'information comme objet d'étude. Leurs travaux sur le sujet sont désormais datés et ne nous intéressent pas en tous points. Dans leur article dédié aux systèmes d'information dans l'administration publique, ils proposent une analyse des « *déterminants organisationnels et sociaux qui entraînent la participation ou le retrait de*

[1784] V. *supra* n° 50. Les systèmes d'information peuvent en effet être qualifiés de STAD au sens de l'article 323-3 du Code pénal (en ce sens v. C. FERAL-SCHUHL, *Cyberdroit*. *Le droit à l'épreuve d'internet*, coll. Praxis, Dalloz, 2018-2019, n° 712 et svt.).

[1785] Dans le domaine de la santé : J. BOSSI, « Comment organiser aujourd'hui en France la protection des données de santé », *RDSS* 2010, p. 208 ; A. MONNIER, « Le Dossier Médical Personnel : histoire, encadrement juridique et perspectives », *RDSS* 2009, p. 625.

[1786] Par exemple le système d'information douanier (SID) et le système d'information Schengen : A. DEBET, J. MASSOT et N. METALLINOS (ss. la dir.), *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, coll. les intégrales, Lextenso éditions, 2015, n° 2837 et svt, n° 2755 et svt.

[1787] Par exemple : A. LOTH, « Systèmes d'information et cartes de santé », *Droit social* 1996 p. 829 ; M. BORGETTO et C. BERGOIGNAN-ESPER « La loi « Hôpital, patients, santé et territoires », *RDSS* 2009, p. 789 ; M. BORGETTO, « La stratégie nationale de santé », *RDSS* 2018 p. 387 ; F. EON, « L'accélération du numérique en santé : enjeux et conditions de son succès », *RDSS* 2019, p. 55 ; L. CLUZEL-METAYER, « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », *AJDA* 2017, p. 340.

[1788] L'usage des SI en entreprise est étudié en management et au sein des écoles universitaires de cette discipline, l'analyse des usages constitue d'ailleurs le thème d'une revue scientifique (*Systèmes d'information & management*, Editions ESKA). L'objet est étudié dans de nombreuses disciplines, qu'il traverse en tant qu'outil de travail, d'organisation, de gestion, de communication mais également d'information (v. D. COTTE, « Système, information, média, Le SI comme objet des Sciences de l'information et de la communication », *Communication & languages* 2009/2, n° 160, p. 39 ; J. MELESE, *Approches systémiques des organisations, vers l'entreprise à complexité humaine*, Éditions d'organisation, 1990 ; Y. CHEVALIER, *Système d'information et gouvernance*, Eme, 2008). Dans le domaine de la santé c'est sous le prisme de l'économie et de la gestion que leur utilisation est étudiée : P.-L. BRAS, G. de POUVOURVILLE et D. TABUTEAU, *Traité d'économie et de gestion de la santé*, Ed. Presses de Sciences Po – Editions de santé, 2009.

[1789] P. GREMION et H. JAMOUS, « Les systèmes d'information dans l'administration publique », *Revue française de science politique* 1974, n° 2, p. 214.

[1790] H. JAMOUS et P. GREMION, *L'ordinateur au pouvoir. Essai sur les projets de rationalisation du gouvernement et des hommes*, Seuil, 1978.

certains groupes à la mise en place puis à l'utilisation (ou la non utilisation) des systèmes d'information »[1791]. Une partie de leur réflexion porte sur le thème, connu en sociologie et en science politique, de l'information et du pouvoir[1792]. Si les auteurs critiquent la binarité du lien entre information et pouvoir au sein des organisations et de la société, nous relevons d'abord que les rapports entre systèmes d'information, information et pouvoir tiennent à l'une des fonctions des systèmes d'informations, mise en exergue par les auteurs. Ils retiennent en effet que « *les opérations minimales généralement associées aux expressions de* « banques de données » *et de* « systèmes d'information » *visent le rassemblement et l'intégration de données provenant de plusieurs sources (intra ou inter-organisationnelles) et leur mise sous forme automatisée* »[1793]. Le *rassemblement* des informations constitue l'un des éléments centraux de la circulation du pouvoir au sein des organisations et de la société, dans la mesure où le professionnel qui fournit les informations s'en trouverait dépossédé au profit de ceux qui maîtrisent le système d'information[1794]. Si cette vision dichotomique est caricaturale, et en se gardant de toute analyse binaire sur les rapports entre pouvoir, information et résistance à l'utilisation des systèmes d'information, nous en tirons tout de même un enseignement : plus les informations sont *rassemblées* au sein d'un système informatisé, plus leur maîtrise échappe nécessairement aux seuls professionnels qui en sont l'origine. L'évolution des systèmes d'information informatisé n'est pourtant plus à l'heure du rassemblement des données à leur mise en réseau. Il nous faut avancer progressivement dans cette voix, en commençant par évoquer les conséquences, dans un premier temps, du rassemblement des données couvertes par le secret.

371. Des conséquences sur le pouvoir des professionnels originellement soumis au secret. Dès lors que l'opposabilité du secret professionnel peut se concevoir comme la manifestation d'un pouvoir, il devient possible de percevoir le mouvement général qui s'est déployé avec la mise en œuvre des systèmes d'information, dans un premier temps, dans les

---

[1791] P. GREMION et H. JAMOUS, « Les systèmes d'information dans l'administration publique », *op. cit.*, p. 222 et svt.
[1792] Dont une œuvre fondatrice en sociologie des organisations, d'où a été tirée l'expression, devenue un lieu commun, « *l'information c'est du pouvoir* » : M. CROZIER et E. FRIEDBERG, *L'acteur et le système*, Seuil, 1977.
[1793] P. GREMION et H. JAMOUS, « Les systèmes d'information dans l'administration publique », *op. cit.*, p. 214.
[1794] Ce que les auteurs critiquent d'ailleurs à plusieurs égards : P. GREMION et H. JAMOUS, « Les systèmes d'information dans l'administration publique », *op. cit.*, p. 223-224.

établissements de santé publics. Si, comme l'explique Monsieur Couturier, « [...] *le secret* […] *occupe une fonction particulière dans l'ordonnancement social : garantir à ceux qui le détiennent une forme d'autonomie à l'intérieur de la sphère sociale dans laquelle ils évoluent* »[1795], reprenant l'idée développée par le philosophe Georg Simmel selon laquelle le secret est « *constitutif d'un contre-pouvoir, notamment à l'égard du politique mais aussi à l'égard du juge : il est donc un pouvoir. Une charge et un pouvoir* »[1796], alors, toute atteinte à la maîtrise de l'information constitue une atteinte à ce pouvoir. Nous n'affirmons pas que le fait de rassembler les informations issues de la prise en charge donne lieu à une atteinte à la vie privée des personnes – nous verrons que celle-ci est garantie par ailleurs –, mais que si le fait de posséder une information et ainsi de pouvoir la conserver secrète constituent les fondements d'un pouvoir, le fait de rassembler les informations et d'en déposséder, partiellement, le professionnel, contribuent à affaiblir ce pouvoir. La légitimité, aux yeux de la société, de l'opposition du secret par les professionnels s'en trouve nécessairement réduite. Ce mouvement est davantage sociologique que juridique mais se traduit en droit par une diminution progressive du contre-pouvoir dont bénéficiaient, en premier lieu, les professions de santé. Plus précisemment encore la mise en réseau, permise par l'interopérabilité des systèmes constitue la condition de l'accès aux données.

372. L'accès aux données de santé à caractère personnel rassemblées dans les systèmes d'information. Du point de vue des économistes, les systèmes d'information ont permis de réduire l'asymétrie informationnelle entre professionnels et instances de régulation[1797] dans une optique de rationalisation du système de financement des établissements de santé[1798]. Les données contenues dans les systèmes d'informations se sont progressivement diversifiées[1799],

---

[1795] M. COUTURIER, *Pour une approche fonctionnelle du secret professionnel*, *op. cit.*, n° 313.
[1796] G. SIMMEL, *Secret et sociétés secrètes*, rééd., Circé, 1991, p. 43.
[1797] G. de POUVOURVILLE, « « L'économie de la santé : périmètre et question de recherche », *in* P.-L. BRAS, G. de POUVOURVILLE et D. TABUTEAU, *Traité d'économie et de gestion de la santé*, *op. cit.*, p. 22.
[1798] C'est le but premier du PMSI : G. de POUVOURVILLE, « La crise d'identité des médecins face au nouveau management de l'hôpital », *Le journal de l'école de Paris du management* 2010/6, n° 86, p. 22.
[1799] Il n'est plus seulement question de systèmes d'information hospitalier (SIH) mais de systèmes d'information en santé (SIS). Ces derniers peuvent soutenir toutes formes de solutions (télémédecine, logiciel de gestion des patients, données cliniques) mais également les données traitées dans le cadre de réseaux de santé, dans des bases de données.

à tel point que ceux-ci sont devenus de véritables outils de gouvernance[1800]. Pour permettre cette « *gouvernance par les données* »[1801], il a été nécessaire de permettre l'*accès* aux données contenues dans les systèmes d'information. A titre d'illustration, depuis la loi de modernisation de notre système de santé[1802], les agences régionales de santé ont accès aux données contenues dans les systèmes d'information des établissements de santé et des établissements et services médico-sociaux[1803]. Outre cet exemple, le fait de rassembler les données relatives aux soins – et couvertes par le secret professionnel – en a facilité l'accès dans la mesure où la *demande d'accès*, faite par une institution sur le fondement de l'un des textes évoqués en amont[1804], ne s'effectue plus nécessairement auprès du professionnel qui a collecté les données, mais auprès du responsable de traitement, qui peut être l'établissement en tant que personne morale[1805] ou le directeur d'établissement. En effet, au regard de ces textes, les organisations concernées sont des *tiers autorisés*[1806].

[1800] Cette remarque rejoint celle, plus générale, de Madame Lasserre, qui explique que l'exploitation des flux d'informations dans l'Union européenne « *aux fins d'harmonisation, de coopération, d'intégration, de réglementation de secteurs extrêmement techniques et spécialisés est un mode de gouvernance indiscutable* » (V. LASSERRE, *Le nouvel ordre juridique. Le droit de la gouvernance*, LexisNexis, 2015, n° 119).

[1801] La formule est notamment celle employée par Madame Fery dans sa thèse de doctorat en science politique. L'auteur, spécialisée dans la sociologie des institutions, s'emploie à analyser la fonction du système d'information Cassiopée au sein de l'institution pénale. Elle explique notamment que l'outil participe au *new public management* par ses fonctions de traçabilité et d'évaluation (B. FERY, *Gouverner par les données ? : Pour une analyse des processus de traduction dans l'usage des systèmes d'information : Déploiement et utilisations de Cassiopée dans l'Institution pénale*, th. en science politique, ss. la dir. de J. DE MAILLARD, soutenue le 28 sept. 2015, Université de Versailles St Quentin-en-Yvelines, p. 304). Sans pouvoir transposer le raisonnement de l'auteur au système de santé, les systèmes d'information dans les établissements de santé participent du même mouvement, ainsi que nous l'avons évoqué à plusieurs reprises mais sous des angles à chaque fois différents. L'on peut néanmoins citer, dans le domaine de la santé, un ouvrage renvoyant à l'idée selon laquelle les données sont devenues des outils de management du système de santé, qu'il s'agit de *piloter*. C'est l'expression choisie par un collectif d'auteurs de différentes disciplines : *La révolution du pilotage des données de santé. Enjeux juridiques, éthiques et managériaux*, préf. J. LUCAS, coll. Décideur santé, LEH édition, 2019. Si le titre laisse penser qu'il s'agit de *piloter les données,* le propos porte davantage sur le *pilotage du système de santé par les données de santé.*

[1802] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

[1803] CSP, art. L. 1435-6, figurant dans une section relative à l'accès aux données de santé au sein d'un chapitre portant sur les modalités et moyens d'intervention des agences régionales de santé.

[1804] V. *supra* n° 366.

[1805] Au sein d'un groupement hospitalier de territoire (GHT), les établissements peuvent être co-responsables des traitements de donnnées de santé : « *Selon la nature des traitements, leurs finalités, l'organisation retenue au sein du GHT et dès lors qu'ils déterminent conjointement les finalités et les moyens du traitement, l'établissement support et établissements parties au GHT sont responsables conjoints de traitement (ex : dossier médical partagé, traitement utilisé pour le laboratoire commun de biologie médicale, traitement utilisé pour la pharmacie commune, etc.). Dans ce cas, il est nécessaire de formaliser la coresponsabilité par voie d'accord* » (DGOS, *Mémento RGPD, sensibilisation au règlement général sur la protection des données à l'usage des directeurs d'établissements,* édition 2019, p. 10).

[1806] Nous avons évoqué les tiers autorisés afin de les distinguer des autres acteurs intervenant dans le traitement des données (V. *supra* n° 209). Bien que la notion ne soit pas définie dans les textes, la CNIL a eu l'occasion d'affirmer qu'étaient des tiers autorisés les personnes « *qui ne peuvent avoir accès à tout ou partie des informations*

Il nous faut noter que les sources dont dispose le juriste sur ces questions sont faibles, nous n'avons trouvé aucune jurisprudence portant sur la question de l'opposabilité du secret, par des professionnels de santé, envers une organisation pour laquelle est prévu un droit d'accès. Si nous ne pouvons en déduire que cela est signifiant et vient appuyer notre raisonnement, il apparaît toutefois que la question ne semble pas s'être posée, ou du moins qu'il existe une certaine fluidité dans les accès des administrations, agences et organisations pour lesquels une mission de contrôle est prévue. Un décret du 26 décembre 2018 autorise et encadre l'accès aux dossiers médicaux des patients au bénéfice, d'une part, des prestataires extérieurs, pour leurs missions d'élaboration du programme de médicalisation des systèmes d'information (PMSI) et d'optimisation du codage des actes et, d'autre part, des commissaires aux comptes[1807]. Ce décret a modifié l'article R. 6113-5 du Code de la santé publique afin d'y inscrire les intervenants susceptibles d'accéder aux données de santé à caractère personnel prévus à l'article R. 6113-1 Code de la santé publique. L'accès par le commissaire aux comptes est ponctuel mais aléatoire[1808]. Soulignons par ailleurs que ce qui avait été considéré par la CNIL comme une atteinte au « secret médical » en 2013[1809] est entériné par ce décret. Les établissements ont désormais la possibilité de recourir à des prestataires extérieurs pour le codage des actes. Le décret crée l'article R. 6113-9-1 du Code de la santé publique disposant que lorsque, « *pour la mise en œuvre des activités mentionnées au présent chapitre, un établissement de santé recourt à un prestataire extérieur, celui-ci ne peut conserver les données mises à disposition par l'établissement au-delà de la durée strictement nécessaire aux activités*

---

qu'en vertu de dispositions légales particulières » (CNIL, *Dix ans d'Informatique et Libertés*, Economica 1988, p. 30). L'accès est nécessairement ponctuel et limité et concerne en premier lieu les autorités judiciaires et les auxiliaires de justice : « *Les officiers de police judiciaire de la police ou de la gendarmerie nationale doivent être considérés, lorsqu'ils agissent par réquisition judiciaire dans le cadre d'une enquête de flagrance, d'une enquête préliminaire ou d'une instruction préparatoire éventuellement sur commission rogatoire, comme des tiers autorisés à obtenir communication des données contenues dans les dossiers* » (CNIL, *Guide professionnel de santé*, 2011, p. 9). Peuvent également être qualifiés comme tels les experts désignés par les autorités civiles ou administratives et les agents de l'administration fiscale (*Ibid*.), et tous les tiers ayant une mission de contrôle définie par la loi ou le règlement, ce que sont toutes les autorités visées par les textes prévoyant un accès aux données ou aux informations (A. DEBET, J. MASSOT et N. METTALINOS (ss. la dir), *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, *op. cit.*, n° 564).

[1807] Décret n° 2018-1254 du 26 décembre 2018 relatif aux départements d'information médicale.

[1808] CSP, art. R. 6113-7.

[1809] V. *supra* n° 268.

qui lui ont été confiées par contrat ». Cela aboutit à un décloisonnement croissant entre les administrations et, selon les besoins, avec des entreprises privées.

373. L'interopérabilité, convergence des systèmes disséminés. L'interopérabilité est au centre des préoccupations des politiques nationales en matière de santé et de numérique. Sa mise en œuvre par les pouvoirs publics s'est affirmée avec la création de l'ASIP santé[1810]. Le terme *interopérabilité* ne connaît pas de définition en droit, il s'agit, dans son acception technique, de « *la capacité que possède un produit ou un système informatique à fonctionner avec d'autres produits ou systèmes existants ou futurs. C'est la possibilité qu'ont des systèmes à fonctionner en synergie, à « communiquer », ce qui implique d'utiliser un langage (interopérabilité sémantique) et des référentiels techniques (interopérabilité technique) communs* »[1811]. La Commission européenne a eu l'occasion de préciser qu'il s'agissait de « *la capacité de plusieurs systèmes de dossiers informatisés de santé d'échanger aussi bien des données exploitables par un ordinateur que des informations et des connaissances demandant une intervention humaine* »[1812]. Faire fonctionner les systèmes en *synergie* est la condition d'une mise en réseau des systèmes, d'une interconnexion qui consiste alors à rendre les données de santé recueillies par les professionnels à l'occasion de la prise en charge plus facilement et plus rapidement accessibles[1813]. La loi relative à l'organisation et à la transformation du système

---

[1810] L'ASIP santé a été créée en 2009 en remplacement du GIP-DMP. Sa création a été votée le 16 juillet 2009 portant transformation de la convention constitutive du GIP approuvée par arrêté ministériel du 20 octobre 2009 et modifiée en décembre 2009. L'ASIP santé est une agence de l'Etat, chargée de créer des référentiels d'interopérabilité. A ce titre, elle a mis en place le Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS), qui fixe les *règles* de l'opérabilité des systèmes d'information. Ces référentiels sont élaborés grâce à des normes techniques et des standards internationaux et sont donc évolutifs.

[1811] J. BOSSI, « Technologies de l'information et de la communication et données de santé : pour un cadre juridique en phase avec les évolutions technologiques et les besoins du système de santé », *Statistique et société*, mai 2014, vol. 2, n° 2, p. 37.

[1812] Recommandation n°2008/594/CE de la Commission européenne du 2 juillet 2008 sur l'interopérabilité transfrontalière des systèmes de dossiers informatisés de santé, *JOUE* L190 du 18 juil. 2008.

[1813] C'est pour cette raison que l'interopérabilité des systèmes d'information s'est imposée comme une nécessité pour la relance du DMP à partir de 2009 (Recommandation de la mission de relance du dossier médical personnel, *Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information en santé*, Recommandations de la mission de relance du projet DMP, 11 avril 2008 ; M. FIESCHI, *La gouvernance de l'interopérabilité sémantique est au cœur du développement des systèmes d'information en santé*, Rapport à la ministre de la santé et des sports, 9 juin 2009). La mise en œuvre de l'interopérabilité est toujours au cœur des programmes de politiques d'amélioration des soins, il en est fait mention dans tous les rapports des acteurs publics participant à sa mise en œuvre (DGOS, programme Hôpital numérique, 2012-2017, puis le programme *Hop'en* 2018-2022 qui prévoit, dans le cadre de la stratégie « ma santé 2022 », l'interopérabilité des systèmes d'information hospitaliers : instruction n° dgos/pf5/2019/32 du 12 février 2019 relative au lancement opérationnel du programme hop'en ; CNNum, *La santé, bien commun de la société numérique*, *Construire le réseau du soin et du prendre soin*, Rapport remis à la Ministre des Affaires sociales, de la Santé et des Droits des

de santé[1814] insiste, dans ses articles 44 et 45 relatifs à la mise en œuvre d'un espace numérique de santé pour chaque citoyen, sur la nécessité de favoriser l'interopérabilité des systèmes d'information. L'interopérabilité des systèmes d'information informatisés est communément évoquée comme un cadre technique garantissant notamment la confidentialité du partage des données de santé[1815]. Bien que l'évolution qui s'opère au travers de l'interopérabilité des systèmes d'information paraît, à première vue, relever du mouvement que nous décrivons dans ces lignes, nous ne l'envisagerons qu'ultérieurement. En effet, le *cadre* de l'interopérabilité répond à des normes qui ne sont plus juridiques et la notion révèle un dessein international[1816]. Il n'est par contre que rarement fait mention du mouvement sous-jacent qu'il révèle. Ce projet d'interopérabilité complète des systèmes d'informations en santé, condition de l'interconnexion, fait écho aux enjeux théoriques de l'accès exposés par Madame Rochfeld qui explique que la « *société de l'accès* »[1817] se conçoit dans « *un contexte renouvelé d'interdépendance et d'interconnexion* »[1818]. L'on voit alors s'ébaucher les liens entre les différentes notions que nous avons mis en balance pour parvenir à ce qui nous semble l'enjeu central : maîtrise de l'information, secret professionnel comme mode de réservation de

---

femmes, oct. 2015 ; M. CUGGIA, D. POLTON, G. WAINRIB et S. COMBES, *Rapport de la mission de préfiguration Health Data Hub*, oct. 2018; sur la nécessité d'intensifier, de manière générale, l'interopérabilité des bases de données et des systèmes d'information, le processus est évoqué à de nombreuses reprises dans le rapport du député Cédric Villani sur l'intelligence artificielle : C. VILLANI, Rapport au premier ministre, *Donner un sens à l'intelligence artificielle pour une stratégie nationale et européenne*, mars 2019).

[1814] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, *JORF* n° 0172 du 26 juillet 2019.

[1815] C'est pourquoi la première mention de *l'interopérabilité* dans le Code de la santé publique figure à la suite de l'article L. 1110-4, à l'article L. 1110-4-1 du Code de la santé publique. Il est précisé, au sein de cet article, que pour garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection « *les établissements et services de santé, et tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social dont les conditions d'exercice ou les activités sont régies par le présent code, utilisent, pour leur traitement, leur conservation sur support informatique et leur transmission par voie électronique, des systèmes d'information conformes aux référentiels d'interopérabilité et de sécurité élaborés* ». Le même Code comporte encore d'autres mentions identiques, concernant par exemple les systèmes d'information des centres antipoison et de la toxicovigilance (art. R. 1340-6), concernant le dossier médical personnel et sa mise en œuvre par la Caisse nationale de l'assurance maladie des travailleurs salariés (art. R. 1111-27) et concernant les logiciels d'accès au DMP (art. R. 1111-29 et R. 1111-41), pour la pratique des actes de télémédecine (R. 6316-10) concernant les comptes rendus des examens biologiques (art. R. 6211-4). C. ZORN, *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, *op. cit.*, n°307 et svt.

[1816] V. *infra* n° 453.

[1817] J. ROCHFELD, *V°* « Accès (enjeux théoriques) », *in* M. CORNU, F. ORSI et J. ROCHFELD (ss. la dir.) *Dictionnaires des biens communs*, coll. Quadridge, PUF, 2017.

[1818] *Ibid.*

l'information et des données, rassemblement et mise en réseau, accès vont finalement nous mener à poser la question des données issues de la relation de soin comme bien commun.

374. Remarques sur l'interconnexion des fichiers comportant des données couvertes par le secret. Dans le prolongement de nos propos relatifs aux fichiers pénitentiaires[1819], l'interconnexion entre les fichiers Hopsyweb et le fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT) interroge. Le fichier Hopsyweb, créé par un décret du 23 mai 2018[1820] après avis de la CNIL[1821], a pour finalité le suivi et la gestion administrative des mesures de soins psychiatriques sans consentement. La mise en œuvre de ce fichier a été fortement critiquée par les professionnels de santé et particulièrement les psychiatres, notamment au regard du nombre ne croissant de personnes pouvant y avoir accès[1822]. La fédération nationale des psychiatres a publiquement dénoncé ce traitement de données en ce qu'il aurait pour finalité cachée de lutter contre la radicalisation[1823]. Le second fichier, créé par un décret du 5 mars 2015[1824], a pour «*finalité principale de recenser et de centraliser les informations relatives aux personnes qui, engagées dans un processus de radicalisation, sont susceptibles de vouloir se rendre à l'étranger sur un théâtre d'opérations de groupements terroristes ou de vouloir prendre part à des activités à caractère terroriste, en vue de l'information des autorités compétentes et de leur exploitation par les services et du suivi des personnes concernées* »[1825].

[1819] V. *supra* n°335 et svt.
[1820] Décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement.
[1821] Délibération n° 2018-152 du 3 mai 2018 portant avis sur un projet de décret autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement (demande d'avis n° 18005564).
[1822] Communiqué du 18 juin 2018, Fédération française de psychiatrie, disponible sur : <https://sphweb.fr/wp-content/uploads/2018/06/FFP-CNPP_Communiqué-2018_06.pdf> (dernière consultation le 5 mai 2019). Un recours pour excès de pouvoir a notamment été introduit par l'association des secteurs de la psychiatrie pénitentiaire (<https://www.aspmp.fr/ >) et par le Conseil national de l'ordre des médecins. Le Conseil d'Etat n'a pas encore rendu sa décision sur ce point.
[1823] *Ibid.* ; D. VIRRIOT-BARRIAL, « Secret médical et terrorisme », *RDSS* 2019, p. 236 ; visant également le fichier Hopsyweb et son évolution (existant auparavant sous le nom d'« Hopsy » v. B. PY, « Fichier les fous. Au sujet du traitement des données à caractère personnel dénommé « REDEX » (répertoire des expertises) », *RDS* 2018, n° 84, p. 611 ; v. également P.-Y. CHAPEAU, V. MIJUSKOVIC, « Le recul des libertés en psychiatrie sous couvert de prévention de la radicalisation », *RDS* 2018, n° 85, p. 832.
[1824] Le décret n'a pas été publié en raison d'une dispense : Décret n° 2015-252 du 4 mars 2015 modifiant le décret n° 2007-914 du 15 mai 2007 modifié pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[1825] D. PARIS et P. MOREL-A-L'HUISSIER, *Rapport d'information présenté en conclusion des travaux d'une mission d'information sur les fichiers mis à la disposition des forces de sécurité*, 17 oct. 2018, p. 51.

Un décret du 6 mai 2019[1826] autorise l'interconnexion entre ces deux fichiers, abolissant ainsi la frontière dressée par le secret professionnel puisque les psychiatres n'ont plus la possibilité d'opposer leur secret, les donnnées qui sont rassemblées sur Hopsyweb étant directement accessibles par les agents ayant déjà accès au fichier FSPRT[1827]. Le décret a suscité de vives réactions de la part des soignants, qui ont dénoncé « une atteinte au « secret médical »[1828]. Il nous semble pourtant, au regard de notre démonstration, que les recours en ce sens auront peu de chance d'aboutir car la *logique d'accès* que nous décrivons emporte pour conséquence d'affaiblir les pouvoirs des professionnels de santé, mais ne porte pas atteinte au secret professionnel entendu comme une obligation de se taire dont le manquement est pénalement sanctionné, ni ne nécessite de créer un fait justificatif spécial afin de permettre une révélation. En d'autres termes, l'accès aux données issues d'informations couvertes par le secret entraîne, *de facto*, une coopération forcée entre les soignants et les agents chargés de la sécurité publique. Nous notons, sans une certaine ironie, que le rapport de la mission d'information sur les fichiers mis à la disposition des forces de sécurité, à la fin de l'année 2018, s'est félicité que « *le monde de la santé et celui de la sécurité publique* [aient] *commencé à engager un véritable dialogue* »[1829]. Dans le même temps, évoquant la possibilité d'une interconnexion de ces fichiers, le rapport souligne que « *le croisement avec ce fichier ne semble pas pertinent. Le milieu psychiatrique hospitalier se montre très réticent envers cette idée, eu égard au principe du secret médical* »[1830]. Seul le premier message semble avoir été entendu. Enfin, dans l'avis

---

[1826] Décret n° 2019-412 du 6 mai 2019 modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement.

[1827] Sont ainsi destinataires des données : le préfet en charge du suivi de la personne radicalisée, que les membres du groupe d'évaluation départementale et de la cellule pour la prévention de la radicalisation et l'accompagnement des familles, ou encore les personnes accédant au FSPRT seront destinataires de l'information selon laquelle une personne déterminée fait l'objet d'une mesure d'hospitalisation sans consentement (Délibération n° 2018-354 du 13 décembre 2018 portant avis sur un projet de décret modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement (demande d'avis n° 18020552)).

[1828] Dans un communiqué du 10 mai 2019, le Conseil national de l'Ordre des médecins à affirmé sa volonté d'introduire un recours contre ce décret, rappelant *« la nécessité de préserver le caractère absolu du secret médical, qu'il considère comme une condition* sine qua non *de la relation de confiance entre un patient et son médecin* » (CNOM, *Communiqué de presse à propos du décret autorisant la mise en relation des fichiers dits Hopsyweb et FSPRT : le CNOM examine les voies juridiques d'un recours au Conseil d'Etat*, 10 mai 2019, disponible sur <https://www.conseil-national.medecin.fr/sites/default/files/cnom_cp_hopsyweb.pdf>.)

[1829] D. PARIS et P. MOREL-A-L'HUISSIER, *Rapport d'information présenté en conclusion des travaux d'une mission d'information sur les fichiers mis à la disposition des forces de sécurité*, *op. cit.*, p. 54.

[1830] *Ibid.*, p. 53.

rendu à propos de ce décret, la CNIL souligne que « *dans la mesure où certaines informations contenues dans HOPSYWEB sont couvertes par le secret médical, des garanties suffisantes au regard du respect des principes fondamentaux du droit à la protection des données personnelles doivent être mises en œuvre. La Commission estime à cet égard que des mesures juridiques et techniques adaptées doivent être prévues afin d'assurer un haut niveau de protection des données* »[1831]. Ces remarques vont dans le sens de ce que nous évoquerons ultérieurement, à savoir une préservation des informations couvertes par le secret par des dispositifs normatifs autre que la règle juridique.

ii - L'accès

375. Le SNDS, seconde étape. Une autre manifestation de la perte de maîtrise, par les professionnels intervenant dans la prise en charge médicale et médico-sociale des personnes, sur les données et informations produites à l'occasion de leur activité tient à leur réutilisation croissante à d'autres fins que la prise en charge. Si nous l'avons précédemment envisagé sous des angles différents, il convient de préciser que le processus amorcé par la loi de 1994[1832] autorisant la transmission de données entre professionnels de santé et chercheurs s'est progressivement muée, sur le plan technique, en une mise à disposition des données au sein du SNDS. Les données des établissements contribuant au PMSI, les données du SNIIRAM également issues des soins[1833] et les données médico-sociales des maisons départementales des personnes handicapées y sont notamment accèssibles[1834]. Elles échappent en partie à la maîtrise

---

[1831] Délibération n° 2018-354 du 13 décembre 2018 portant avis sur un projet de décret modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement (demande d'avis n° 18020552).

[1832] Loi n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[1833] Il s'agit des données de l'assurance maladie issues, majoritairement, des feuilles de soins : CSS, art. L. 161-28-1 et L. 161-29.

[1834] Rassemblées mais de manière décentralisée, le SNDS est une entité, un système, qui permet de réaliser le chaînage de ces données : « *Le chaînage d'enregistrements est la tâche qui consiste à identifier parmi différentes sources de données les enregistrements qui concernent les mêmes entités. En l'absence de clé d'identification commune, cette tâche peut être réalisée à l'aide d'autres champs contenant des informations d'identifications* (…)*Le domaine médical est tout particulièrement intéressé par le chaînage d'enregistrements car la combinaison des informations d'un même patient provenant de différentes sources –afin par exemple de construire une image plus complète de son parcours de soins– est essentielle à la description fine de sa prise en charge ou, plus largement, aux études épidémiologiques* » (X. LI, *Evaluation et amélioration des méthodes de chaînage de données*, Th. dact. en Biostatistique et informatique medicale, ss. la dir. de J.-Y. BOIRE et L. OUCHCHANE, soutenue le 29 janv. 2015, Université d'Auvergne, p. 14). Outre données, le SNDS permet

des professionnels qui les ont recueillies voire produites, ainsi qu'au patient dans la mesure où leur accès ne dépend pas du consentement de la personne[1835]. Si, dans une certaine mesure, les données contenues dans le SNDS peuvent ne plus être considérées comme étant couvertes par le secret professionnel car elles sont anonymisées[1836], pour certaines d'entre elles le risque de réidentification existe puisqu'elles sont seulement pseudonymisées.

376. Risque de réidentification et pseudonymisation dans le SNDS. Le terme de *pseudonymisation* a fait l'objet d'une réflexion approfondie par le G29 portant sur l'anonymisation et sur les limites à tracer entre ces deux techniques[1837]. Le rapport met en exergue la différence entre données *pseudonymisées* et données *anonymisées*, ce qui permet de les différencier et, dans le même temps, de tracer les frontières des données à caractère personnel. Si le juriste se trouve rapidement démuni face aux réflexions d'ordre technique, il ressort de ces travaux que la *pseudonymisation* consiste à remplacer un attribut de la personne – permettant de l'identifier directement, c'est-à-dire de la distinguer de la masse des individus – par un autre. Ainsi, les données pseudonymisées continuent de permettre « *l'individualisation d'une personne concernée et la corrélation entre différents ensembles de données* »[1838]. Aussi,

---

également le chainage des données relatives aux causes médicales de décés (base CépiDC de l'INSERM) et des échantillones de données des organismes d'assurances maladie complémentaires. CSP, art. L. 1461-1.

[1835] Il s'agit en effet d'un droit d'opposition et celui-ci ne peut s'exercer que dans des hypothèses précises. L'article R. 1461-9 CSP prévoit en effet que le droit d'opposition ne s'exerce que pour les accès à des fins de recherche, d'étude ou d'évaluation (CSP, art. L. 1461-3) ayant pour finalité l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité ; la définition, la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale ; la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales ; l'information des professionnels, des structures et des établissements de santé ou médico-sociaux sur leur activité ; surveillance, à la veille et à la sécurité sanitaires ; la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale (CSP, art. L. 1461-1).

[1836] C'est dans ce cas que l'on parle d'*Open data* en santé. La mise à disposition au public de données de santé ne s'entend que des données anonymisées. Toutefois, comme le remarquait Madame Cluzel-Métayer à propos des données issues de la relation de soin « *la possibilité d'établir des liens entre les données anonymisées constitue la principale faiblesse de l'ensemble de ces dispositifs, puisqu'il suffit de croiser les informations pour qu'elles redeviennent identifiantes : à titre d'exemple, il a été prouvé que 89 % des patients d'un hôpital peuvent être identifiés à partir de leur code postal, du mois et de leur année de naissance, de leur sexe et du mois de sortie de l'hôpital en question* » (C. CLUZEL-METAYER, « Les limites de l'open data », *AJDA* 2016, p. 102 ; dans le même sens : P.-L. BRAS, A. LOTH, *Rapport sur la gouvernance et l'utilisation des données de santé*, 2013, p. 27).

[1837] Avis 05/2014 du Groupe de travail « article 29 » sur la protection des données sur les Techniques d'anonymisation, adopté le 10 avril 2014, 0829/14/FR WP216.

[1838] Avis 05/2014 du Groupe de travail « article 29 » sur la protection des données sur les Techniques d'anonymisation, *op. cit.*, p. 11. Citons également le Conseil d'Etat qui, dans une étude annuelle, explique que la pseudonymisation « *se distingue de l'anonymisation en ce qu'elle ne supprime pas toute possibilité d'identification,*

la *pseudonymisation* « *réduit le risque de mise en corrélation d'un ensemble de données avec l'identité originale d'une personne concernée* »[1839] sans que celui-ci disparaisse. Ce risque s'analyse ensuite au regard de la technique utilisée et s'apprécie en termes de probabilité[1840]. La possibilité de réindentification implique que « *l'anonymisation ne doit pas être vue comme une solution ultime mais plutôt comme un compromis entre protection des données et préservation de leur usage* »[1841].

La pseudonymisation est désormais définie à l'article 4 du RGPD comme « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* ». Les discussions à propos de cette technique, lors de la rédaction du projet du règlement général, ont principalement porté sur le fait de savoir si les données pseudonymisées devaient entrer dans le champ du règlement et devaient donc être qualifiées de données à caractère personnel[1842]. Partant du constat selon lequel les données pseudonymisées permettent seulement de rendre l'identification plus difficile, le choix a été fait de les conserver dans le champ du règlement. La pseudonymisation est encouragée par le RGPD car elle présente une garantie appropriée constituant l'un des critères permettant de « *déterminer le caractère compatible de la finalité*

---

mais la rend seulement plus difficile » (Conseil d'Etat, *Étude annuelle 2014. Le numérique et les droits fondamentaux*, coll. Les rapports du Conseil d'État, La Documentation française, 2014, p. 175, note 289).

[1839] Avis 05/2014 du Groupe de travail « article 29 » sur la protection des données sur les Techniques d'anonymisation, *op. cit.,* p. 22.

[1840] Les techniques d'anonymisation, en tant que « *processus de dégradation de l'information* », permettent simplement de rendre la réidentification de la personne la plus difficile possible (Ph. PUCHERAL, N. ANCIAUX, M. BEHAR-TOUCHAIS, V.-L. BENABOU, N. MARTIAL-BRAZ, *et al.*, « Directive Contenu numérique Données », *CCC* 2017, dossier 4, n° 5). Des recherches menées sur le sujet ont démontré comment les attributs, ou *quasi-identifiants*, lorsqu'ils sont uniques, permettent, par recoupement, de réidentifier une personne (L. SWEENEY, « k-anonymity : a model for protecting privacy », *Int. J. Uncertain. Fuzziness Knowl. - Based Syst*., vol. 10, n° 5, oct. 2002, p. 557) ; V. également pour une explication, technique cette fois, vulgarisée : L. ROCHER, « Des données anonymes…bien trop faciles à identifier », *The conversation*, 15 sept. 2019.

[1841] Ph. PUCHERAL, N. ANCIAUX, M. BEHAR-TOUCHAIS, V.-L. BENABOU, N. MARTIAL-BRAZ, *et alii*, « Directive Contenu numérique Données », *op. cit.*, n° 5.

[1842] Comme l'explique un auteur, certains *lobbies* souhaitaient qu'il n'en soit pas ainsi, ce qui aurait permis de les soustraire à la protection accordée aux données à caractère personnel : F. LESAULNIER, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p. 573.

secondaire d'un traitement avec sa finalité initiale »[1843]. Comme le souligne un auteur, « *ces techniques sont centrales dans le domaine de la recherche médicale et des statistiques dès lors que l'on veut faire de l'utilisation ultérieure ou secondaire des données au bénéfice de la santé publique* »[1844]. Les conditions d'accès au SNDS ont été pensées en fonction de la distinction entre données anonymisées et données pseudonymisées[1845]. Les données anonymisées, constituant des jeux de données agrégées ou des échantillons, sont ouvertes à tous. C'est ainsi qu'est mis en œuvre l'*open data* en santé[1846]. Quant aux données pseudonymisées, leur accès est restreint. La procédure mise en œuvre ne prend, dans ce cas, pas en compte l'avis des professionnels qui ont produit les données à l'occasion de la prise en charge des personnes. Dès lors, on constate que le professionnel à l'origine de la production des données n'en maîtrise pas la circulation. L'article 68 de la LIL prévoit que le professionnel de santé peut transmettre des données personnelles de santé pour les traitements présentant une finalité d'intérêt public[1847]. Toutefois, **cette *possibilité*, qui suppose, en miroir, celle d'opposer le secret professionnel, est réduite à néant dès lors que ces données sont centralisées et que la gestion de l'accès échappe totalement aux professionnels qui en sont la source**. Il nous semble que cette analyse en creux peut trouver une confirmation dans l'étude d'impact de la loi du 26 janvier 2016 créant le SNDS[1848]. Concernant l'accès aux données de santé, l'étude liste les options discutées puis écartées. L'une d'elle consistait à laisser perdurer les situations indésirables au titre desquelles « *l'accès difficile des chercheurs aux données couvertes par le secret* »[1849]. Si ces difficultés étaient d'ordre technique, elles tenaient également à la réticence des professionnels à fournir les données dont il avait la maîtrise[1850]. Le processus de perte de la maîtrise des données de santé s'est effectué progressivement, du PMSI vers le SNDS au *Health*

[1843] *Ibid.*
[1844] *Ibid.*
[1845] Elles ne contiennent ni les noms, ni les prénoms, ni l'adresse, ni le numéro de sécurité sociale des personnes consernées (CSP, art. L. 1461-4).
[1846] CSP, art. L. 1461-2.
[1847] LIL, art. 66, I.
[1848] Etude d'impact du projet de loi de modernisation de notre système de santé, 14 oct. 2014, NOR : AFSX1418355L/Bleue-1.
[1849] *Ibid.* p. 187.
[1850] « Données de santé, open data, big data et secret médical », Communication et Echanges lors de l'Assemblée générale de l'Ordre de février 2016.

Data Hub, dans la mesure où de nombreuses données qui échappaient à cette logique d'accès vont désormais faire partie du SNDS.

377. Procédures d'accès au SNDS, cas des accès ponctuels : cadre antérieur. La procédure d'accès aux données contenues dans le SNDS a été critiquée pour sa complexité et modifiée par loi relative à l'organisation et à la transformation du système de santé[1851] et tends à l'être encore par la loi de révision de la loi bioéthique[1852]. Deux hypothèses étaient, jusqu'alors, distinguées : d'une part, les accès permanents, d'autre part, les accès nécessitant soit une procédure d'autorisation, soit une procédure simplifiée. Cette dernière catégorie désignait les accès qui sont permis lorsque les données sont traitées à des fins de recherche, d'étude ou d'évalution, contribuant à l'une des finalités du SNDS[1853] et poursuivant un motif d'intérêt public. L'accès correspondant à une opération de traitement, les dispositions prévues aux articles 64 et suivants de la loi informatique et libertés s'appliquent dans ce cas. Deux régimes de traitement était à distinguer au regard de la finalité du traitement[1854]. Or, l'accès au SNDS n'est actuellement permis qu'à des fins d'étude, de recherche et d'évaluation dans le domaine de la santé et dans un intérêt public. La procédure était ensuite distincte selon que la recherche implique, ou non, la personne humaine. Dans la première hypothèse[1855], la procédure comportait la nécessité de recueillir l'avis du Comité de protection des personnes avant l'autorisation de la CNIL. Dans le second cas, l'INDS transmettait la demande au Comité d'expertise pour les recherches, l'études et les évaluations dans le domaine de la santé (CEREES) dont l'avis précèdait l'autorisation de la CNIL. Enfin, une procédure simplifiée existait dans la mesure où la recherche respectait l'une des méthodologies édictées par la CNIL,

[1851] Loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, *op. cit.*
[1852] Projet de loi relatif à la bioéthique, n° 2187 actuellement en cours de discussion.
[1853] CSP, art. L. 1461-1 ancien.
[1854] Selon qu'il correspond aux dispositions de la sous-section I ou II de la section 3 du chapitre III du titre II de la LIL. Pour les premiers, il s'agissait des traitements répondant à une finalité d'intérêt public, les seconds étaient mis en œuvre pour une finalité de recherche, d'études ou d'évaluation dans le domaine de la santé. Les premiers concernaient principalement les entrepôts de données de santé, et devaient faire l'objet d'une autorisation de la CNIL (pour un exemple récent d'entrepôt servant à de futures études observationnelles et autorisé par la CNIL : Délibération n° 2018-369 du 20 décembre 2018 autorisant la société Compugroup Medical Solutions à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité un entrepôt de données de santé (Demande d'autorisation n° 2135377)).
[1855] Entrant dans le champ de la loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine (dite loi Jardé).

et permettait soit un accès aux données pseudonymisées, soit un accès aux données agrégées (et donc anonymisées). Nous traiterons ultérieurement du cadre actuel.

378. Les accès permanents au SNDS. A coté des cas d'accès ponctuel au SNDS, la loi de modernisation de notre système de santé a prévu, pour certaines institutions publiques, un accès permanent, ces dispositions n'ont pas été modifiés par la loi du 24 juillet 2019. Cet accès permanent permet de contourner le secret professionnel. L'accès aux données de santé au sein du SNDS est facilité par l'habilitation délivrée à certains organismes d'accéder à une base de données qui, en raison du volume de données de santé qu'elle contient, ne peut exclure de manière définitive les possibilités de réidentification[1856]. Ainsi, la liste des organismes chargés d'une mission de service public autorisés à accéder au SNDS et les conditions d'accès sont prévus aux articles R. 1461-11 et suivants du Code de la santé publique. La liste concerne actuellement vingt-cinq organismes[1857], l'article R. 1461-14 du même code différenciant ensuite des niveaux d'accès aux données par ces organismes selon les risques d'identification en tenant compte du nombre d'identifiants potentiels et de leur croisement. L'accès est donc prévu au regard des besoins de ces organismes pour remplir leurs missions d'intérêt public.

B - L'affirmation du caractère commun des données

379. Le discours actuel porte sur le partage des utilités des données de santé issues de la prise en charge du patient ou de son suivi médico-social en ce qu'elles sont produites par le système de santé **(1)** ce discours qui vise à légitimer ce partage tient, pour beaucoup, aux attentes placées sur les innovations technologiques que doivent permettre les *Big data* et l'intelligence artificielle **(2)**.

[1856] En ce sens v. C. ZORN, « Libre circulation des données et RGPD : le cas des données composites », intervention au colloque *La libre circulation des données non personnelles* (dir. F. MACREZ), 24 mai 2019, Strasbourg, vidéos des interventions disponibles sur <http://www.canalc2.tv/video/15380>. V. également : SNDS, *référenciel de sécurité, Guide d'accompagnement*, p. 12-13 : (disponible sur <https://www.snds.gouv.fr/download/Guide_accompagnement.pdf>).
[1857] CSP, art. R. 1461-12.

1 - Les données de santé issues de la prise en charge du patient ou de son suivi médico-social

380. Propriété, autodétermination informationnelle et bien commun. Dans le prolongement du processus d'accès aux données de santé à caractère personnel issues de la prise en charge des personnes dans le système de santé, la question de la propriété sur les données ressurgit[1858]. Les données à caractère personnel, et notamment les données de santé à caractère personnel d'un individu, ont une valeur que l'on pourrait qualifier de résiduelle car la valeur économique des données ne se révèle que lorsqu'elles sont rassemblées et traitées en masse[1859]. C'est l'objet du *Big data* ou *données massives*. La réflexion engagée sur la qualification des données est toujours l'objet de controverses doctrinales qui sont le prolongement de celles, plus anciennes, portant sur les informations[1860]. Entre les deux voies – celle du droit de propriété et celle d'un droit de la personnalité rattaché au droit au respect de la vie privée – nous avons évoqué le droit à l'autodétermination informationnelle[1861]. S'il semble en effet que ce soit cette troisième voie qu'emprunte le législateur français, nous avons

---

[1858] Certains auteurs se sont depuis longtemps prononcés en faveur d'une vision patrimoniale des données et de la reconnaissance d'un droit de propriété sur celles-ci. Tant outre atlantique (L. LESSIG, « Privacy as property », *Social Research : An International Quarterly*, 69(1), 2002, p. 247) qu'en France, depuis longtemps concernant les données « nominatives » : P. CATALA, « La « propriété » de l'information », *Mélanges offerts à Pierre Raynaud*, Dalloz-Sirey, 1985, p. 97. Puis plus récemment, considérant que le cadre actuel de la protection des données est insuffisant : A. BENSOUSSAN, *Informatique et libertés*, Ed. Francis Lefebvre, 2008, n° 280, p. 39 ; « Pour un droit de propriété et de monétisation des données personnelles », blog www.figaro.fr, 28 févr. 2018 ; I. LANDREAU, *Rapport du think-tank Génération Libre, Mes Data sont à moi : pour une patrimonialité des données personnelles*, janv. 2018. Une thèse sur le sujet à récemment été soutenue, ce qui témoigne de l'intérêt de la question : M. CAVALIER, *La propriété des données de santé*, th. dact. ss. la dir. de M. GIRER, soutenue le 14 déc. 2016, Université Lyon III Jean Moulin. Passant en revue les différentes perspectives d'une vision patrimonialiste (propriété intellectuelle, droit de propriété *sui generis*, secret des affaires) pour les rejeter en raison du résultat d'une telle vision qui aboutirait à faire perdre, *in fine*, la maîtrise des données et laisserait les individus en proie au marché, v. Y. PADOVA, « Entre patrimonialité et injonction au partage : la donnée écartelée ? (Partie I) », *Revue Lamy Droit de l'Immatériel* 2019, nº 155. Dans la presse, par exemple : F.-P. LANI, « Vers un droit de propriété sur nos données personnelles », *Les Échos*, 5 juill. 2018.

[1859] L'institut Montaigne, dans un rapport sur les objets connectés insiste particulièrement sur la valeur économique des *Big data* : *« Les perspectives de création de valeur du Big data et des objets connectés sont stratégiques pour l'économie d'un territoire et concernent tous les pans de l'économie et de la société* » (Institut Montaigne, *Big data et objets connectés Faire de la France un champion de la révolution numérique*, Rapport, avr. 2015, p. 5). Les exemples, au sein du rapport, sont légion et les *big data* y sont comparés au pétrole : « *la métaphore du pétrole reste pertinente lorsqu'il s'agit de souligner les opportunités inexploitées du Big data. Le parallèle entre économie numérique et économie du pétrole peut se faire lorsqu'on rapproche la notion de réserve pétrolière avec la notion de « multitude » qui génère les réserves de données, or noir numérique* » (*Ibid.*, p. 13).

[1860] V. *supra* n° 46. La société de l'information, née avec les moyens de communication, avait fait émerger les premières. Elles se prolongent avec le perfectionnement des dispositifs d'information-communication et l'imbrication des sciences de l'information et de la communication, des mathématiques, de la génomique, de la médecine, de la physique.

[1861] V. *supra* n° 185.

expliqué que la maîtrise, par l'individu, de ses données de santé à caractère personnel issues de la prise en charge n'était pas complète et connaissait même de nombreux tempéraments. Il nous semble que la loi du 24 juillet 2019 relative à l'organisaiton et à la transformation du système de santé prend également un autre chemin en ce qui concerne la qualification des données de santé produite par les acteurs du système de santé : des biens communs. Cette qualification emporte des conséquences sur le secret professionnel.

381. Notions : choses communes ou biens communs. Nous avons, à plusieurs reprises, effleuré la notion de bien commun. A propos du statut des informations, Monsieur Libchaber proposait celui de *res communis*, affirmant que « *Le monde où nous vivons est commun, tout comme son reflet dans le miroir que nous lui tendons. L'appropriation des choses incorporelles doit ainsi se limiter à la reconnaissance d'une élaboration intellectuelle* »[1862]. Si, comme le souligne la doctrine majoritaire, le législateur européen a consacré le droit à l'autodétermination informationnelle, il semblerait que l'idée de consacrer les données de santé comme un *commun* ait le vent en poupe. *Biens communs* et *res communis* sont néanmoins deux notions différentes. Madame Bourcier, à l'occasion d'un article intitulé « *le bien commun, ou le nouvel intérêt général* » choisit de ne pas les distinguer, utilisant d'ailleurs le singulier à dessein[1863]. La nuance tient à l'objet de son étude, qui porte non pas sur la nature des biens mais sur les « *processus socio-politiques et juridiques qui les régulent* »[1864] afin d'expliquer comment la notion, dans une société où l'intérêt général provoque une certaine méfiance[1865], pourrait « *revivifier de façon émergente le lien social à partir d'institutions de gestion communautaire d'une ressource* »[1866]. Aussi, lorsque l'auteur envisage, à l'occasion d'un autre article portant sur les données de santé, la possibilité d'un droit collectif sur ces données, c'est comme mécanisme

[1862] R. LIBCHABER, « La recodification du droit des biens », *in Le code civil 1804-2004. Le livre du bicentenaire*, Dalloz-Litec, 2004, p. 348, n° 46. Cette élaboration intellectuelle, fut, un temps, au cœur du problème de la qualification des informations recueillies et produites à l'occasion des soins car, si elles concernent la personne, elles sont produites par les professionnels de santé. V. par exemple la question des notes personnelles du médecin *supra,* n°59.
[1863] D. BOURCIER, « Le bien commun, ou le nouvel intérêt général », *in Mélanges en l'honneur du professeur Jacques Chevallier, Penser la science administrative dans la post-modernité*, LGDJ, p. 93.
[1864] *Ibid.*, p. 97.
[1865] *Ibid.* p. 96.
[1866] *Ibid.* p. 102.

collectif de protection des individus et de dépassement de l'intérêt général qu'est évoqué le « *bien commun des données de santé* »[1867].

382. Partage de l'utilité et accès. L'étude de la nature des *res communis* et des *biens communs* en droit civil invite à les distinguer. Madame Danis-Fatôme, prenant l'exemple typique des ressources naturelles[1868], met en exergue les différences entre les notions, au regard de leur régime[1869]. Tandis que la notion de *choses communes* a été « *construite sur le postulat de l'existence de ressources naturelles inépuisables* »[1870], la notion de *biens communs* constitue une réponse à l'affaiblissement de ces ressources. Le *bien commun* renvoie à une conception tierce de la propriété, par rapport aux *biens publics* et aux *biens privés*. Il s'agit de permettre un « *usage modéré et raisonné* »[1871] du bien. Sur ce point, le *bien commun* se distingue des *res communis* qui ne sont la propriété de personne[1872]. Comme le souligne le même auteur, l'idée sous-jacente est identique[1873] : il s'agit de « *réunir des biens pour en organiser l'affectation collective, un partage* »[1874], en d'autres termes « *d'articuler une appropriation avec un accès collectif* »[1875]. D'autres auteurs évoquent une « *maîtrise concurrente* »[1876] ou « *co-maîtrise* »[1877]. Comme le remarque encore Madame Rochfeld la notion d'accès renvoi à l'accès aux utilités d'un bien, il s'agit d'une forme de « *socialisation de la propriété* » mais non d'une collectivisation ou d'une propriété commune[1878]. L'auteur précise encore que les communs

---

[1867] D. BOURCIER et P. DE PHILIPPI, « Vers un droit collectif sur les données de santé », *RDSS* 2018, p. 444.
[1868] A propos desquels : E. OSTRÖM, *La gouvernance des biens communs : pour une nouvelle approche des ressources naturelles*, 2010, Bruxelles (édition américaine 1990) ; B. PARANCE et J. de SAINT VICTOR (dir.), *Repenser les biens communs*, 2014, CNRS Éditions.
[1869] A. DANIS-FATOME, « Biens publics et choses communes ou biens communs ? Environnement et domanialité », *in Mélanges en l'honneur d'Etienne Fatôme*, Dalloz, 2011, p. 99.
[1870] *Ibid.* p. 102. Si elles ont un temps étaient confondu avec les biens publics, l'apparition de l'Etat a permis de les distinguer : « *Ce n'est qu'avec l'élaboration juridique de la notion d'État que l'on a pu clairement distinguer ce qui était par lui approprié, directement ou par l'intermédiaire de collectivités publiques, de ce qui, par nature, devait être considéré comme relevant de tous sans appartenir en propre à personne* » (R. LIBCHABER, *Rép. civ.*, *V°* Biens, mai 2016, act. avr. 2018, n° 273).
[1871] *Ibid.*
[1872] W. DROSS, *Droit civil. Les choses*, LGDJ, 2012, n° 318 s.
[1873] Raison pour laquelle Madame Bourcier ne les distingue pas (D. BOURCIER, « Le bien commun, ou le nouvel intérêt général », *op. cit.*).
[1874]A. DANIS-FATOME, « Biens publics et choses communes ou biens communs ? Environnement et domanialité », *op. cit.*, p. 105.
[1875] *Ibid.*
[1876] F.-G. TREBULLE, « La propriété à l'épreuve du patrimoine commun : le renouveau du domaine universel », *in Etudes offertes au professeur Philippe Malinvaud*, Litec, 2007, p. 659.
[1877] F. MODERNE, « Rapport de synthèse », *in La maîtrise du sol*, Travaux de l'association H. Capitant, t. XLI, Economica, 1990, p. 36.
[1878] J. ROCHFELD, *V°* « Accès (enjeux théorique) », *in* M. CORNU, F. ORSI et J. ROCHELD (ss. la dir.), *Dictionnaire des biens communs*, op. cit.

s'accompagnent en général d'une « *gouvernance* », c'est-à-dire que la ressource est soumise à une distribution des droits entre les membres d'une communauté[1879]. Ce qui n'est pas le cas des biens privés auquels il est prévu un accès, pas plus d'ailleurs qu'aux biens publics ou quasi-publics auxquels il est prévu un accès[1880]. Pourrait-on alors qualifier les données à caractère personnel issues de la prise en charge par le système de santé de *commun* ?

383. Les données de santé, *des communs* ? Dans un rapport rédigé en 2015[1881], Madame Rochfeld explique – outre l'intérêt de consacrer l'autodétermination informationnelle au profit d'un droit de propriété sur les données – que la perspective de qualifier les données de biens communs et d'en assurer la gourvernance collective comporte des avantages indéniables tels que celui de les soustraire « *à la seule mainmise des grands opérateurs privés* […] *en faveur des impératifs collectifs évoqués (information, innovation, création ; mais aussi en fonction des informations, pour servir la santé ou assurer la sécurité)* »[1882]. Il faut ajouter que les données ne concernent pas un seul individu particulier : « *dans un monde en réseau, on s'aperçoit que les données sont de moins en moins personnelles. En effet, beaucoup d'informations personnelles ne sont pas liées à un individu mais à une lignée généalogique* »[1883]. Il a ainsi été proposé de créer la catégorie des « *données pluripersonnelles* »[1884], qualification imposant une

---

[1879] *Ibid.* La notion de distribution des droits ou faisceau de droits (Bundle of Rights) renvoi à une conception rénovée de la propriété qui serait non plus un droit naturel et absolu mais distribuée et relative, caractérisée, selon la conceptualisation d'Edella Schalger et Elinor Ostrom par une distinction et une caractérisation des « différents régimes de propriété selon divers faisceaux de droits distribués entre différents individus ou groupes d'individus » (F. ORSI, *V°* « Faisceau de droits (Bundel of Rights) », *in* M. CORNU, F. ORSI et J. ROCHELD (ss. la dir.), *Dictionnaire des biens communs*, op. cit.

[1880] Dans sa définition des enjeux pratiques de *l'accès* Monsieur Perroud note que l'accès est une notion traditionnellement connue du droit public. Il rappelle que la « *notion moderne d'accès prend sa source dans le déclin du public. L'émergence de la notion contemporaine d'accès doit être replacée dans son contexte : la privatisation des biens publics entraîne un brouillage des frontières du public et du privé, et des espaces* (…) » c'est pourquoi il souligne que s'agissant de ces espaces quasi-publics l'accès « *sert davantage à accomoder les effets de la privatisation qu'à évoluer vers un système de gestion en commun de ces ressources* » (T. PERROUD, *V°* « Accès (enjeux pratiques) », *in* M. CORNU, F. ORSI et J. ROCHELD (ss. la dir.), *Dictionnaire des biens communs*, op. cit.

[1881] J. ROCHFELD, *Quelle politique européenne en matière de données personnelles ?* Rapport d'études *Digital New Deal Foundation*, sept. 2015.

[1882] *Ibid.,* p. 13.

[1883] D. BOURCIER et P. DE FILIPPI, « Vers un droit collectif sur les données de santé », *op. cit.* L'on comprend que cela vise au premier titre les données génétiques.

[1884] Prenant principalement pour exemple les données génétiques et proposant d'étendre la notion de *personne concernée* : I. COULYBALY, *La protection des données à caractère personnel dans le domaine de la recherche scientifique*, th. dact. ss. la dir. d'E. VERGES et I. DE LAMBERTERIE, soutenue le 25 nov. 2011, Univ. Grenoble

maîtrise collective de ces données. Madame Rochfeld relève néanmoins que l'un des inconvénients[1885] d'une telle proposition tient aux conséquences qu'elle implique : la possibilité de « *contraindre la volonté* »[1886] de la personne concernée à des fins d'utilité collective. Il nous semble pourtant que c'est dans ce sens que se dirige le régime des données produite à l'occasion de la prise en charge des personnes dans le système de santé. Les données publiques du secteur de la santé, quant à elles, sont au cœur de l'*open data*[1887]. Les qualifier de bien commun s'impose plus aisément[1888] dans la mesure où ces données n'ont plus rien de personnel[1889], leur diffusion est donc possible avec toutefois un risque mininme d'atteinte à l'intimité ou à l'identité des personnes. Il peut s'agir notamment de données brutes, de données relatives aux dépenses d'assurance maladie, à la consommation de soins et à l'activité des professionnels de santé, ainsi que des rapports, analyses et études statistiques ou médico-économiques[1890]. S'agissant des données de santé qui entrent, non plus dans cette catégorie, mais dans celle des

---

Alpes, p. 791 et svt. ; évoqué également par F. LESAULNIER, *L'information nominative*, th. dact. ss la dir. de P. CATALA, soutenue le 4 juill. 2005, Univ. Paris II.

[1885] Pour l'auteur, l'argument principal, qui explique son approche personnaliste tient au fait que ces données sont une émanation de la personne. Quand bien même il y aurait, particulièrement pour le traitement des données en masse, un travail valorisable et donc une possible patrimonialisation, Madame Rochfeld rappelle que c'est le fait de considérer les données comme *des choses* qui est discutable, au même titre qu'est discutable de qualifier de choses les éléments du corps humain (Dans une interview plus récente de J. ROCHFELD et B. WARUSFEL, *Les données personnelles. Le bien commun*, Amicus radio, animée par A. GARAPON, 15 janv. 2017, disponible sur <https://radio.amicus-curiae.net/podcast/les-donnees-personnelles/>).

[1886] J. ROCHFELD, *op. cit*.

[1887] « *Exigences de démocratie transparente, concertée et contributive, exigences d'efficacité administrative et de développement économique se conjuguent pour justifier que soient prises les mesures propres à restituer aux informations publiques, au-delà de leur statut juridique, les usages effectifs d'un bien commun* » (H. VERDIER et S. VERGNOLLE, « L'Etat et la politique d'ouverture en France », *AJDA* 2016, p. 92 ; CADA, *Rapport d'activité 2013*, p. 3) ; dans le même sens : D. FOREST, « 3 questions Open data et données publiques », *JCP E*, n° 30-34, 28 juill. 2016, 638. Ajoutons que l'ouverture des données publiques s'accompagne d'une liberté de réutilisation prévue par la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public modifiée par la Directive 2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public.

[1888] Cette qualification est plus évidente *a priori* seulement, car c'est encore sous l'angle du *droit d'accès* opposé au secret de l'administration, que l'ouverture des données publiques, (qui sont des documents administratifs, v. *supra* n° 49) est étudiée. Sur ce point v. A. GARIN, *Le droit d'accès aux documents* : *en quête d'un nouveau droit fondamental dans l'Union européenne*, préf. C. Blumann, Ed. A. Pedone, 2017.

[1889] « *L'accès en mode open data sera possible pour les données pour lesquelles aucune identification n'est possible – ni nom, prénom ou numéro de sécurité sociale – l'anonymisation sera complète et irréversible* » (CSP, art. L. 1461-1-4). Ces données deviennent des communs dans la mesure où l'accès permet un partage non exclusif de leur utilité, cette idée doit néanmoins être relativisé car, comme le constate un auteur « *la production de connaissances requiert plus que le traitement de jeux de données rendu possible par leur ouverture, traitement qui n'est pas accessible à tous et peut conduire à renforcer les inégalités* » (M. DULONG DE ROSNAY, *V°* « Données ouvertes (Open Data) », *in* M. CORNU, F. ORSI et J. ROCHFELD (ss. la dir.), *Dictionnaire des biens communs*, *op. cit.*).

[1890] Pour une liste des données de santé et médico-sociale en *open data* v. le site dédié au SNDS : <https://www.snds.gouv.fr/SNDS/Open-Data>.

données de santé à caractère personnel, ou qui sont produites à l'occasion d'une prise en charge sanitaire, la question est plus délicate.

384. Des communs informationnels ? Nous avons observé que l'accès aux données pseudonymisées ou potentiellement identifiantes, centralisées dans le SNDS, était réservé à certains organismes publics et que, pour certaines finalités, un accès ponctuel était également possible[1891]. En parallèle nous avons constaté que le droit d'opposition offert à la personne, qui plus est dans des hypothèses restreintes, tend, en l'état du droit positif, à affaiblir la force de la volonté des individus de même que la portée du secret professionnel tend également à s'affaiblir. Il nous semble que ces quelques évolutions permettent de caractériser certains élements qui seraient propres aux *communs informationnels* : Ils sont d'abord non-rivaux, « *leur consommation par un individu ne prive ni n'exclue aucun autre individu de cette consommation* »[1892], ensuite, pour maintenir cette non-rivalité il apparaît nécessaire de procéder à une redistribution des droits, si ce second élément est plus évident à concevoir en opposant communs informationnels et propriété intellectuelle[1893], l'on peut également considérer que l'affaiblissement du pouvoir des professionnels de santé sur les données et les limites posés aux droits des personnes sur ces même données est significatif d'une volonté de redistribution des droits. Les dispositions relatives au SNDS ont évolué dans ce sens, seulement trois ans après leur entrée en vigueur. Le *Data Health Hub*[1894],en français *plateforme d'exploitation de données de santé* en est l'expression. La définition du terme *Hub* en anglais, renvoie plus exactement au « *centre* », au « *noyau* » ou à l'outil qui permet de « *centraliser* »[1895]. C'est donc plus qu'un support, et les premiers mots du rapport de préfiguration informati déjà sur les orientations du législateur : « *les données de santé financées par la solidarité nationale constituent* ***un patrimoine commun*** *et doivent être mises pleinement au service du plus grand*

[1891] V. *supra* n° 374 et svt.
[1892] B. CORIAT, *V°* « Communs informationnels », *in* M. CORNU, F. ORSI et J. ROCHFELD (ss. la dir.), *Dictionnaire des biens communs*, *op. cit.*
[1893] Monsieur Coriat prend pour exemple les innovations juridiques qui ont permis de « *rétablir la qualité de l'information comme bien non-exclusif* » face à la montée en puissance de la propriété intellectuelle et du régime des brevets, tels que les licences *Creative Commons* et les autres licences organisant un régime de propriété inclusifs (*Ibid.*).
[1894]M. CUGGIA, D. POLTON, G. WAINRIB et S. COMBES, *Rapport de la mission de préfiguration Health Data Hub*, oct. 2018.
[1895] Le *Cambridge dictionnary* propose notamment pour définition « *a centre of activity or business* ».

nombre dans le respect de l'éthique et des droits fondamentaux des citoyens »[1896]. Ce rapport s'inscrit dans la droite ligne du rapport du député Cédric Villani sur l'intelligence artificielle, dans lequel le syntagme « *mise en commun des données* » est utilisé à plusieurs reprises, et où il est, par ailleurs, mentionné que cette mise en commun – avec pour objectif le développement de l'intelligence artificielle[1897] – doit contribuer à améliorer notre performance économique et, partant, servir le bien commun, nouvel intérêt général[1898]. La santé figure évidemment au titre des secteurs dans lesquels le développement de l'intelligence artificielle importe le plus. L'enjeu affiché est celui de la « *souveraineté nationale dans un contexte de course technologique internationale* »[1899]. Les données de santé devraient donc être *des* communs au service *du* bien commun. La loi relative à l'organisation et à la transformation du système de santé et le projet de loi relatif à la révision de la loi bioéthique permettent de confirmer le mouvement amorcé en ce sens. En ce sens, le rapport d'information relatif au projet de loi de révision de la loi bioéthique affirme, à propos de l'accès aux données du SNDS, que le consentement de la personne – et donc sa volonté– ne doit pas être au centre du futur dispositif : « *A trop vouloir protéger, nous nous empêcherions de découvrir des applications très utiles à la santé de nos concitoyens* »[1900]. La loi du 24 juillet 2019 contribue à renforcer ce mouvement. Particulièrement en ce qu'elle contribue à définir un dernier trait des données à caractère personnel issues de la relation de soin, qui est également un élément caractéristique des communs informationnels : ils font l'objet d'une « *gouvernance orientée non vers la conservation mais vers l'addition et l'enrichissement* »[1901].

[1896] M. CUGGIA, D. POLTON, G. WAINRIB et S. COMBES, *op. cit.*, p. 17 (Nous soulignons).
[1897] L'enjeu central se situe évidemment dans l'amélioration des capacités de *prédictibilité,* à l'échelle nationale, dans tous les domaines de la vie sociale (ce que rappelle d'ailleurs Madame Rochfeld lorsqu'elle évoque le traitement des données massives : J. ROCHFELD et B. WARUSFEL, *Les données personnelles. Le bien commun*, *op. cit.*).
[1898] C. VILLANI, Rapport au premier ministre, *Donner un sens à l'intelligence artificielle pour une stratégie nationale et européenne*, mars 2019, p. 49. Notons par ailleurs la formule éloquente du titre du rapport du CNNum : *La santé, bien commun de la société numérique* (CNNum, *Rapport remis à la Ministre des Affaires sociales, de la Santé et des Droits des femmes* « La santé, bien commun de la société numérique. Construire le réseau du soin et du prendre soin », oct. 2015).
[1899] *Ibid.*
[1900] X. BRETON et J.-L. TOURAINE, *Rapport d'information sur la révision de la loi bioéthique*, n° 1572, 15 janv. 2019, p. 251.
[1901] . CORIAT, *V°* « Communs informationnels », *in* M. CORNU, F. ORSI et J. ROCHFELD (ss. la dir.), *Dictionnaire des biens communs*, *op. cit.*.

2 - *Big data* et intelligence artificielle : aboutissement de la logique de partage des utilités des données

385. Le *Big data* en santé, carburant des algorithmes et de l'intelligence artificielle : une trinité et des questions. Si nous avons brièvement mentionné les notions de *Big data*, d'*algorithme* et *d'intelligence artificielle*, il convient à présent de les préciser. C'est au chercheur en informatique John M^{c} Carthy que l'on attribue la paternité du terme *intelligence artificielle*[1902], défini comme « *la construction de programmes informatiques qui s'adonnent à des tâches qui sont, pour l'instant, accomplies de façon plus satisfaisante par des êtres humains car elles demandent des processus mentaux de haut niveau tels que : l'apprentissage perceptuel, l'organisation de la mémoire et le raisonnement critique »*[1903]. Afin de rendre compte du mouvement à l'œuvre concernant les données – et plus particulièrement les données produites à l'occasion de la prise en charge des personnes dans le système de santé –, il est important de comprendre que ces programmes fonctionnent grâce à des algorithmes, dont la fonction varie selon leur perfectionnement[1904].

L'algorithme est la « *description d'une suite finie et non ambiguë d'étapes (ou d'instructions) permettant d'obtenir un résultat à partir d'éléments fournis en entrée* »[1905]/ Appréhendés sous l'angle de leurs fonctions, « *les algorithmes informatiques permettent de combiner des informations les plus diverses pour produire une grande variété de résultats :*

[1902] Le récit commun situe la naissance de la notion et de la discipline lors de la conférence *Dartmouth Summer Research Project on Artificial Intelligence* qu'il organisa avec Marvin Lee Minsky, en 1956.

[1903] Nous devons cette définition au cofondateur du Groupe d'intelligence artificielle du MIT (Massachusetts Institute of Technology) Marvin Lee Minsky. L'auteur est cité par la CNIL (CNIL, *Comment permettre à l'Homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Rapport de synthèse du débat public, déc. 2017) et dans le rapport d'information relatif à la révision de la loi bioéthique (X. BRETON et J.-L. TOURAINE, *Rapport d'information sur la révision de la loi bioéthique*, *op. cit.*, p. 241) mais la définition choisie, également attribuée à Marvin Lee Minsky lors de la conférence de Dartmouth, est : « *la science qui consiste à faire faire aux machines ce que l'homme ferait moyennant une certaine intelligence* ».

[1904] Dans son rapport relatif à l'intelligence artificielle et aux algorithmes la CNIL explique comment les avancées scientifiques sur les algorithmes ont relancé les projets relatifs à l'intelligence artificielle : « *Au-delà de ces différences techniques, une approche globale des algorithmes et de l'IA demeure cependant pertinente. Algorithmes déterministes et algorithmes apprenants soulèvent en effet des problèmes communs. Dans un cas comme dans l'autre, la finalité des applications de ces classes d'algorithmes consiste à automatiser des tâches autrement accomplies par des humains* » (CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, *op. cit.*, p. 18).

[1905] CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, *op. cit.*, p. 15.

simuler l'évolution de la propagation de la grippe en hiver, recommander des livres à des clients sur la base des choix déjà effectués par d'autres clients, comparer des images numériques de visages ou d'empreintes digitales, piloter de façon autonome des automobiles ou des sondes spatiales, etc. »[1906]. Le sociologue Dominique Cardon souligne encore que l'objectif des algorithmes est de rendre le monde « *mesurable en tout* »[1907]. Mesurer pour prédire, c'est l'objectif des algorithmes mis au service de l'intelligence artificielle. L'IA ne pose pas seulement des questions relatives à la décision et à la transparence des algorithmes qui la gouvernent[1908], la question de la protection des algorithmes et de l'IA se pose également aux juristes[1909]. Dans le domaine de la santé, ces techniques participent déjà – comme le mentionne les rapports et études sur le sujet[1910] – à la médecine dite des 4P (personnalisée, préventive,

---

[1906] *Ibid.*

[1907] D. CARDON, *A quoi rêvent les algorithmes. Nos vies à l'heure des big data*, coll. La république des idées, Seuil, 2015, p. 7. Niveau supérieur de la statistique qui servait déjà à « *conduire les conduites* » (M. FOUCAULT, « Le sujet et le pouvoir », *in Dits et écrits*, t. II, coll. Quarto, Gallimard, 1982, p. 1041-1062), les algorithmes « *chiffrent le monde, le classent et prédisent notre avenir* » (D. CARDON, *A quoi rêvent les algorithmes. Nos vies à l'heure des big data*, *op. cit.*, p. 12). Le droit n'échappe pas à cette transformation et la question de la justice prédictive pose de nombreuses questions relatives à la décision informatisée. V. J. ROCHFELD, « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT* 2018, p. 474 ; L. GODEFROY, « Le code algorithmique au service du droit », *D.* 2018, p.734 ; B. DONDERO, « Justice prédictive : la fin de l'aléa judiciaire ? », *D.* 2017, p. 532 ; F. ROUVIERE, « La justice prédictive, version moderne de la boule de cristal », *RTD civ.* 2017, p. 527, « Le raisonnement par algorithmes : le fantasme du juge-robot », *RTD civ.* 2018, p. 530 ; F. MELLERAY, « La justice administrative doit-elle craindre la « justice prédictive » ? », *AJDA* 2017, p. 193 ; J.- B. DUCLERCQ, « Big data - Les effets de la multiplication des algorithmes informatiques sur l'ordonnancement juridique », *CCC,* nov. 2015, étude 20 ; « Les algorithmes en procès », *RFDA* 2018, p.131 ; Ph. CONTE, « Algorithme idéologique », *Dr. pén.*, nov. 2017, repère 10. De façon plus générale, les algorithmes peuvent constituer une menace pour le droit lui-même puisqu'il serait aujourd'hui question de gouverner par les algorithmes (C. CASTETS-RENARD, « Traitement algorithmique des activités humaines : le sempiternel face-à-face homme/machine », *Cahiers Droit Sciences & Technologies* 2016, n°6, Regards croisés sur les objets et les pratiques scientifiques et techniques, p. 239-255).

[1908] Sur les enjeux de la transparence des algorithmes qui participent à la décision publique v. D. BOURCIER et P. DE PHILIPPI, « Transparence des algorithmes face à l'open data : quel statut pour les données d'apprentissage ? », *RFAP,* 2018/3, n° 167, p. 525 ; v. également D. FOREST, « 3 questions La gouvernementalité algorithmique », *JCP E*, 24 nov. 2016, n° 47, 932.

[1909] A. BENSAMOUN, « Intelligence artificielle et santé : l'intégration en droit de l'IA médicale », Dossier *intelligence artificielle et santé*, *journal de droit de la santé et de l'assurance maladie (JDSAM)*, n° 17, 2017, p. 30-33 (disponible en ligne : <http://www.institutdroitsante.fr/wp-content/uploads/2017/09/JDSAM_complet_12-09-2017.pdf>) ; A. BENSAMOUN et G. LOISEAU, « L'intégration de l'intelligence artificielle dans certains droits spéciaux », *Dalloz IP/IT* 2017, p. 295. Les créations des intelligences artificielles interrogent également : A. BENSAMOUN, « Création et données : différence de notions = différence de régime ? », *Dalloz IP/IT* 2018, p. 85. Deux thèses sur le sujet sont actuellement en cours : M. LAUMELAIS, *L'appréhension juridique des oeuvres participatives intelligentes*, th. en cours, ss. la dir. de A. BENSAMOUN, Univ. Rennes I ; E. GUIRAUD, *La création par intelligence artificielle et le droit d'auteur*, th. en cours, ss. la dir. de C. CASTETS-RENARD, Univ. Toulouse I.

[1910] X. BRETON et J.-L. TOURAINE, *Rapport d'information sur la révision de la loi bioéthique*, *op. cit.*, p. 241 et svt ; C. VILLANI, Rapport au premier ministre, *Donner un sens à l'intelligence artificielle pour une stratégie national et européenne*, *op. cit.*, p. 195 et svt. A propos des principaux éléments du premier rapport, Madame Bévière-Boyer a publié une série d'articles. A l'occasion du premier, l'auteur rappelle les applications déjà

prédictive et participative). Les algorithmes permettent, en effet, des applications en matière d'aide à la décision, ces possibilités pouvant être décuplées par le perfectionnement de l'intelligence artificielle[1911]. Ces applications de l'IA posent évidement des questions de responsabilités[1912]. Plus encore, la décision pourrait être complètement déléguée à la machine,

existantes de l'IA en santé : « *Les algorithmes permettant d'exploiter des grandes quantités de publications scientifiques afin de faciliter la connaissance des chercheurs et des professionnels de santé et de contribuer au développement de projets de recherches ; Les algorithmes d'aide à l'orientation des personnes dans le parcours de soins ;Les algorithmes d'aide au pré-diagnostic médical ; Les algorithmes informatisés d'aide au diagnostic (techniques d'apprentissage par la reconnaissance d'images dans le domaine de la radiologie utiles pour les domaines de l'oncologie, de l'ophtalmologie, de la dermatologie) ; Les applications d'aide à la décision médicale ; Les logiciels d'aide à la prescription médicamenteuse en tenant compte des données propres à l'individu pour la mise en place de traitements sans cesse plus ciblés ; Les algorithmes d'aide à la décision d'orientation des patients en hospitalisation à domicile (HAD) à destination des médecins prescripteurs ; Les algorithmes d'aide au champ visuel du chirurgien lors de l'utilisation de robots et d'outils de télé-opération* » (B. BEVIERE-BOYER, « Intelligence Artificielle & Loi de Bioéthique : quels sont les principaux éléments à retenir du rapport d'information du 15 janvier 2019 ? », n° 1, févr. 2019, disponible sur <managersanté.com> ainsi que d'autres articles du même auteur : « Bioéthique : la création du Health Data Hub national peut-elle contribuer à renforcer la protection des données sensibles de santé ? », n° 2, avr. 2019 ; « Quels sont les questionnements éthiques et juridiques du recours aux techniques de l'I.A. en Santé ? », n° 3, mai 2019 ; « L'I.A. en Santé : entre éthique et droit, quelles sont les 13 propositions du rapport Touraine ? », n° 4, juin 2019.

[1911] Contrairement au discours alarmiste, l'intelligence artificielle n'est pas en passe de dépasser l'intelligence humaine et les applications des IA que nous sommes aujourd'hui en capacité de faire sont très surrestimées du grand public. Selon Monsieur Gruson, « *il faut bien avoir à l'esprit que l'hyperexpostion actuelle du sujet de l'intelligence artificielle est aussi une projection ds fantasmes de notre époque face à la technologie* » (D. GRUSON, *La machine, mon médecin et moi*, Editions de l'Observatoire, 2018, p. 2) ; également cité par X. BRETON et J.-L. TOURAINE, *Rapport d'information sur la révision de la loi bioéthique*, *op. cit.*, p. 241). Dans le domaine de la santé l'évolution de la relation de soin constitue également une inquiétude pour l'instant injustifiée : en ce sens v. C. LEQUILLERIER, « L'impact de l'intelligence artificielle sur la relation de soin », Dossier *intelligence artificielle et santé*, *journal de droit de la santé et de l'assurance maladie (JDSAM)*, n° 17, 2017, p. 14-20 :
(Disponible en ligne : <http://www.institutdroitsante.fr/wp-content/uploads/2017/09/JDSAM_complet_12-09-2017.pdf>). Si ce discours tend à donner confiance dans l'IA, il nous semble que les préoccupations ne devraient pas se trouver dans la crainte de la domination de l'humain par la machine, dont il sera toujours maître, mais dans ce qu'implique l'usage de ces outils pour le droit.

[1912] L. MAZEAU, « Intelligence artificielle et responsabilité civile : le cas des logiciels d'aide à la décision en matière médicale », *Revue pratique de la prospective et de l'innovation*, avr. 2018, n° 1, dossier 6, pp. 38-43). A. BENSAMOUN, « Intelligence artificielle et santé : l'intégration en droit de l'IA médicale », *op. cit.* Interrogeant l'efficacité du droit souple (chartes éthiques) pour réguler l'intelligence artificielle v. A. BENSAMOUN et G. LOISEAU, « La gestion des risques de l'intelligence artificielle. De l'éthique à la responsabilité », *JCP G* 2017, doctr. 1203 ; G. LOISEAU, « Responsabilité », Dossier *Intelligence artificielle et santé*, *Journal de Droit de la Santé et de l'Assurance Maladie (JDSAM)*, n° 17, 2017, p. 21-24 :
(disponible en ligne : <http://www.institutdroitsante.fr/wp-content/uploads/2017/09/JDSAM_complet_12-09-2017.pdf>). La Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique évoque également les enjeux de la robotique et de l'IA en santé (robots de soins à la personne, robots médicaux, réparation et amélioration du corps humain) et rappelle que les appareils robotiques implantés dans le corps humain doivent répondre au cadre du règlement (UE) 2017/745 relatif aux dispositifs médicaux. Elle insiste également sur la nécessité de garantir un égal accès aux innovations en la matière et souligne la nécessité de protéger et d'assurer la maintenance des systèmes implantés (pour une analyse de la résolution v. A. BENSAMOUN et G. LOISEAU, « L'intelligence artificielle à la mode

notamment lorsque ce sont des algorithmes de *machine learning* ou de *deep learning* qui sont utilisés, ces derniers étant au centre de l'intelligence artificielle forte[1913]. L'inquiétude, d'ordre éthique, tenant à la médecine prédictive selon des facteurs relatifs au patrimoine génétique, est un sujet dont la loi bioéthique de 2004 s'était déjà emparé[1914], mais elle prend aujourd'hui une ampleur nouvelle et est remise sur l'ouvrage par la loi de révision de la loi bioéthique en cours de rédaction. L'information essentielle qu'il convient de tirer de ces quelques remarques tient, quant à notre objet d'étude, en ce que la performance des algorithmes et donc de l'intelligence artificielle dépend de la masse de données traitées. Ainsi, la question de la protection des données à caractère personnel tient une place essentielle dans le *triptyque Big data*/algorithmes/intelligence artificielle. Les *Big Data*[1915] sont le carburant des algorithmes : « *l'algorithme sans données est aveugle. Les données sans algorithmes sont muettes* »[1916].

éthique », *D.* 2017, p. 1371). Une communication de la Commission européenne intitulée *Artificial Intelligence for Europe* trace les linéaments de la politique européenne en la matière (COM (2018) 237 final, 25 avr. 2018). Le texte est largement commenté par A. BENSAMOUN, « Stratégie européenne sur l'intelligence artificielle : toujours à la mode éthique... », *D.* 2018, p. 1022 ; Pour une reflexion sur l'application de l'IA en santé et les questions qu'elle pose quant à la relation de soin et la responsabilité médicale v. P. MISTRETTA, « Intelligence artificielle et droit de la santé », Chapitre 12, *in* A. BENSAMOUN et G. LOISEAU (ss. la dir.), *Droit de l'intelligence artificielle*, coll. les intégrales, LGDJ, 2019.

[1913] L'intelligence artificielle forte relève pour l'instant de l'anticipation, c'est le scénario évoqué par les ouvrages du genre qui décrivent ce que serait une intelligence artificielle (robotique) qui aurait atteint le point de singularité technologique. Cette perspective imposerait sans doute une adaptation du droit à ces nouvelles formes d'intelligence qui seraient indepédantes de l'homme mais relève, pour l'instant, de la prospective : D. VALETTE, « De l'automatisation à l'intelligence artificielle dans le domaine de la santé. Le Droit humain doit-il se saisir de l'intelligence artificielle ? », Dossier *Intelligence artificielle et santé*, *Journal de Droit de la Santé et de l'Assurance Maladie (JDSAM)*, n° 17, 2017, p. 8-13 ; rappelant la nécessité de ne pas légiférer en versant dans une vision fantasmée de l'IA : G. LOISEAU et A. BENSAMOUN, « L'intelligence artificielle : faut-il légiférer ? », *D.* 2017, p. 581.

[1914] Loi n° 2004-800 du 6 août 2004 relative à la bioéthique, *JORF* n° 182 du 7 août 2004, p. 14040.

[1915] Le *Big Data* « *s'est développé avec l'accroissement de la puissance informatique des processeurs. Il repose sur la capacité des ordinateurs à stocker et collecter des quantités titanesques de données, alors que cette capacité n'aurait pas été envisageable quelques années auparavant* » (F. CONROY et L. CYTERMAN, « L'encadrement du « big data » et la protection des droits fondamentaux », *Revues des Juristes de Sciences Po* n° 10, mars 2015, p. 118). Le *Big data* se caractérise par ce que l'on nomme les *quatre V* pour « volume, variété, vélocité et véracité des données ». Pour une définition plus précise du point de vue technique : « *le Big data consiste à créer en exploratoire et par induction sur des masses de données à faible densité en information des modèles à capacité prédictive* » (P. DELORT, *Le Big Data*, coll. Que sais-je ?, PUF, 2015, p. 42). Les risques éthiques du *Big data* sont nombreux et constitue un enjeu considérable. V. sur ce point C. ZOLYNSKI, « Big data : pour une éthique des données », *I2D – Information, données & documents* 2015/2, vol. 52, pp. 25-26.

[1916] CNIL, *Comment permettre à l'Homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Rapport de synthèse du débat public, déc. 2017, p. 18.

386. *Big data is not about data!*[1917] La réticence à toute finalité prédéterminée, les enjeux du *Big data*. A l'occasion d'un article sur l'encadrement des nouveaux usages des données personnelles par les *Big data*, Mesdames Zolynski et Bensamoun ont expliqué pourquoi le cadre offert par le droit de l'Union et le droit national ne répondait plus, avant l'entrée en vigueur du RGPD, aux usages du *Big data*[1918]. Leur analyse, publiée en 2015, a conservé sa pertinence après l'entrée en vigueur du Règlement. Les auteurs posent un premier constat relatif au *Big data* : l'exploitation des données étant dynamique et cinétique[1919], une « *approche évolutive* », privilégiant les « *usages secondaires des données* », serait préférable à l'appréhension figée du droit positif[1920]. Elles expliquent ensuite que les fonctions des *Big data* s'accordent mal au cadre national et européen de protection des données car il s'agit d'une « *technique de concentration dynamique* » et de « *recyclage de l'information* »[1921]. Concernant le premier trait caractéristique des *Big data*, les auteurs soulignent que tout l'intérêt réside dans la « *concentration, la masse des données, mises en réseau, appréhendées de manière unitaire et non granulaire* »[1922], en d'autres termes, l'important dans le *big data* est la masse, et non les données prises isolément. Enfin, le caractère dynamique des masses de données implique un traitement « *en mouvement* »[1923]. Partant, la finalité du traitement ne peut, eu égard à la nature

---

[1917] Il s'agit du titre de la préface écrite par le statisticien et politologue américain Gary King pour un ouvrage publié par l'université de Cambridge, l'idée sous-jacente étant que l'enjeu des données massives n'est pas les données, c'est la masse qui importe : G. KING, « Big Data Is Not About The Data ! », *in* R. MICHAEL ALVAREZ, *Computational Social Science: Discovery and Prediction*, Cambridge University Press, 2016, p. VII.

[1918] A. BENSAMOUN et C. ZOLYNSKI, « *Cloud computing* et *Big data.* Quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux* 2015/1, n° 189, pp. 103-121.

[1919] Ce constat était déjà posé par Monsieur Forest : « *On constate d'évidence une contradiction entre une réglementation statique conçue pour des stocks de données prédéfinies en fonction d'une ou plusieurs finalités déterminées, d'une part, et des informations de toute nature en flux continu par essence dynamiques et inattendues, d'autre part. Ceci conduit à questionner la compatibilité de cette législation avec l'objet du « Big data ». Cette interrogation est loin d'être théorique car le responsable du traitement qui en définit les moyens et les finalités, engage lourdement sa responsabilité dès lors que la loi prévoit des sanctions pénales en cas de manquement. Il s'agit donc d'une butée conceptuelle de la loi Informatique et libertés aux prises avec des données que l'on pourrait qualifier de « cinétiques », en mouvement* » (D. FOREST, « 3 questions Le « Big data » », *JCP E* 2014, n° 8, 138).

[1920] A. BENSAMOUN et C. ZOLYNSKI, « *Cloud computing et Big data.* Quel encadrement pour ces nouveaux usages des données personnelles ? », *op. cit.*, p. 106. En effet, si l'article 4 du RGPD prévoit que le traitement peut constituer en des opérations de rapprochement et d'interconnexion la transformation des données par recoupement n'est pas évoquée (*Ibid.,* p. 110).

[1921] *Ibid.* p. 109.

[1922] *Ibid.*

[1923] *Ibid.*

de la technique envisagée, être déterminée en amont[1924]. Pour les auteurs, l'intérêt des *Big data* repose sur le « *réemploi potentiel des données à l'avenir à des fins que l'on a pu ne pas envisager lors de leur collecte* »[1925].

387. Première étape : extension du SNDS. Le législateur ayant pris acte, en réaction au rapport du député Cédric Villani, de l'enjeu de souveraineté lié au développement de l'intelligence artificielle et de la sous-exploitation des données de santé[1926], l'objectif est désormais de rassembler un maximum de données de santé au sein du SNDS. Avant la loi du 24 juillet 2019, celui-ci était composé des données de santé à caractère personnel recueillies à titre obligatoire, restriction supprimée de l'article L. 1460-1 du Code de la santé publique[1927] qui mentionne désormais les « *données de santé à caractère personnel destinées aux services ou aux établissements publics de l'Etat ou des collectivités territoriales, aux professionnels de santé ou aux organismes de sécurité sociale* »[1928]. Le contenu du SNDS a encore été étendu[1929] aux données issues de la protection maternelle et infantile[1930], des services de la médecine scolaire[1931], certaines des données collectées dans le cadre des demandes d'allocation personnalisée d'autonomie (groupe iso-ressources)[1932], les données des enquêtes dans le domaine de la santé et enfin les données de santé recueillies lors des visites d'information et de prévention de santé au travail[1933]. La loi a également prévu une « *gestion décentralisée* » des

---

[1924] *Ibid.*
[1925] *Ibid.* p. 110.
[1926] Rappelons que ce discours était déjà celui tenu, notamment par la Cour des comptes, s'agissant de l'exploitation du SNIIRAM (v. *supra* n° 322). Il nous semble qu'il fait écho à l'argument, toujours invoqué, du « retard » national en matière d'innovation, qui est celui même qui avait été mis en avant au moment de l'adoption de la loi informatique et libertés. L'argument de la concurrence des acteurs mondiaux est également invoquéé par Céline Castets-Renard, pronant une simplification des conditions d'accès et de traitement des données du SNDS : « […] l'ouverture générant un partage de la valeur ne doit pas se faire au détriment de la souveraineté numérique de l'Europe » (C. CASTETS-RENARD, « Santé connectée et politique française de l'*open data* », *in* E. BROSSET, S. GAMBARDELLA et G. NICOLAS (ss. la dir.), *La santé connectée et « son » droit : approches de droit européen et de droit français*, coll. Droit de la santé, PUAM, 2017, p. 191, spéc. p. 204.
[1927] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (*JORF* n° 0172 du 26 juill. 2019), art. 41, I, 1°.
[1928] CSP, art. L. 1460-1.
[1929] Loi n° 2019-774 du 24 juillet 2019, art. 41, II, modifiant l'article L. 1461-1 du CSP.
[1930] CSP, art. L. 1461, I, 10° (Données recueillies dans le cadre des mission définies à l'article L. 2111-1 du CSP).
[1931] CSP, art. L. 1461-1, I, 9° (Données recueillies lors des visites médicales et des dépistages obligatoires prévus à l'article L. 541-1 du Code de l'éducation).
[1932] CSP, art. L. 1461-1, I, 7° (Données prévues à l'article L. 232-2 du CASF mais uniquement lorsqu'elles sont appariées avec des données relatives aux soins. Ce dernier ajout a été sollicité par la Commission des affaires sociales du Sénat : Projet de loi relatif à l'organisation et à la transformation du système de santé, Sénat (1ère lecture), Compte rendu analytique de la séance du 6 juin 2019, intervention de Mme la Ministre Agnès Buzin, p. 35).
[1933] CSP, art. L. 1461-1, I, 11° (Données prévues à l'article L. 4624-1 du Code du travail).

données, une liste d'organismes sera définie par décret pour constituer des entrepôts de données alimentés par les données du SNDS[1934]. L'enrichissement du SNDS et sa gestion décentralisée, c'est-à-dire sa gouvernance, sont des éléments essentiels du glissement qui s'opère vers la reconnaissance des données à caractère personnels produites à l'occasion des soins comme *communs*. Il faut désormais envisager les nouvelles conditions d'accès et leur conséquence.

388. *Data health hub,* les nouvelles conditions d'accès au *bac à sable* de données de santé. Constitution d'entrepôts de données. Perspectives. La mission de préfiguration de la plateforme des données de santé[1935] avait donné le ton quant aux évolutions à venir. Si les données de santé doivent être conçues comme un patrimoine commun, le discours politique s'affirme dans le sens d'un partage généralisé des données de santé à caractère personnel : « *Les données financées par la solidarité nationale* ***doivent être partagées avec tous les acteurs****, publics comme privés, et bénéficier ainsi au système de santé, à la recherche, au tissu industriel et à l'assurance du maintien de la souveraineté nationale sur un secteur stratégique. Ce partage doit se faire dans le respect de l'éthique et des droits fondamentaux du citoyen, notamment en pseudonymisant les données* »[1936,] il s'agit de « *faire du partage la règle, de la fermeture l'exception* »[1937.] La loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé prévoit notamment, en ce sens, un accès facilité aux données. Le premier changement majeur consiste dans la suppression des finalités de traitement des données du SNDS. Lors de l'examen des propositions d'amendements devant la commission des affaires sociales du Sénat, le rapporteur de la commission a posé la question de savoir quelles pouvaient

---

[1934] CSP art. L. 1461-7.

[1935] La plateforme des données de santé remplace l'Institut national des données de santé et aura pour mission : de réunir, organiser et mettre à disposition les données du SNDS et de promouvoir l'innovation dans leur utilisation ; d'informer les patients, de promouvoir et de faciliter leurs droits ; d'assurer le secrétariat unique des demandes de traitement ; d'assurer le secrétariat du nouveau comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (qui remplace les deux comités). ; de contribuer à l'élaboration des référentiels et des méthodologies de référence auxquels les responsables de traitement doivent déclarer leur conformité; de procéder, pour le compte d'un tiers et à la demande de ce dernier, à des opérations nécessaires et à la réalisation d'un traitement de données issues du SNDS ; de contribuer à diffuser les normes de standardisation pour l'échange et l'exploitation des données de santé, en tenant compte des standards européens et internationaux ; d'accompagner, notamment financièrement, les porteurs de projets sélectionnés dans le cadre d'appels à projets lancés à son initiative et les producteurs de données associés aux projets retenus (CSP, art. L. 1462-1 créé par l'art. 41, VIII, 2° de la loi n° 2019-774 du 24 juillet 2019).

[1936] M. CUGGIA, D. POLTON, G. WAINRIB et S. COMBES, *Rapport de la mission de préfiguration Health Data Hub*, oct. 2018, p. 19.

[1937] *Ibid.*

être les *autres finalités* pour lesquelles les données du SNDS pourraient être traitées. En réponse Madame la Ministre de la santé explique que la finalité d'évalution, d'étude et de recherche est supprimée « *pour ne pas faire obstacle à la constitution de bases de données pérennes croisant données sanitaires, sociales ou environnementales* »[1938]. Le rapport diligenté par le sénateur Alain Milon précise qu'il s'agit d'un *assouplissement*, puisque désormais il s'agira de traiter des données concernant la santé pour un motif d'intérêt public[1939]. La finalité de recherche, d'étude et ou d'évaluation n'est plus mentionnée. L'assouplissement se poursuit avec la modification de la loi informatique et libertés, afin de permettre, pour les traitements utilisant le NIR non plus seulement à des fins de recherche mais également pour les traitements servant à constituer des bases de données à des fins ultérieurs de recherche, de bénéficier de l'exception posée par l'article 30 de la LIL et conditionnant le traitement à la seule conformité à la méthodologie de référence[1940]. La question sera alors de déterminer ce que recouvre *l'intérêt public*, la contrepartie à cet assouplissement, tel que proposé par le législateur, sera évoquée ultérieurement.

389. L'intérêt public, standard juridique. A propos de la finalité d'intérêt public, les travaux de la commission des affaires sociales soulignent « *qu'avec la disparition de la finalité d'étude, d'évaluation ou de recherche, l'examen du caractère d'intérêt public deviendra le seul critère de définition de la légalité d'un traitement de données de santé (en dehors, bien entendu, du maintien des finalités interdites). Cette évolution rend particulièrement urgente la clarification et la circonscription de la notion d'intérêt public* »[1941], précisant ensuite que la loi informatique et libertés ne fait qu'une seule mention de l'intérêt public pour les traitements de données à caractère personnel dans le domaine de la santé dans son article 66[1942].

[1938] Projet de loi relatif à l'organisation et à la transformation du système de santé, Sénat (1ère lecture), Compte rendu analytique de la séance du 6 juin 2019, intervention de Mme la Ministre Agnès Buzin, p. 34.

[1939] A. MILON, rapport fait au nom de la commission des affaires sociales sur le projet de loi, adopté par l'assemblée nationale après engagement de la procédure accélérée, relatif à l'organisation et à la transformation du système de santé, 22 mai 2019, p. 180-181.

[1940] Par le jeu combiné des article 30 et 73 de la LIL.

[1941] A. MILON, rapport fait au nom de la commission des affaires sociales sur le projet de loi, adopté par l'assemblée nationale après engagement de la procédure accélérée, relatif à l'organisation et à la transformation du système de santé, 22 mai 2019, p. 185.

[1942] Qui prévoit que « *La garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux constitue une finalité d'intérêt public* ». Les travaux préparatoires de la loi du 20 juin 2018 permettent de comprendre qu'il ne s'agit là que d'un exemple de ce qui peut être d'intérêt public (Assemblée nationale, XVe législature, Session ordinaire de 2017-2018, Compte rendu intégral, Première séance du mercredi 7 février 2018).

Il faut pourtant souligner que l'INDS – bientôt remplacée par la Plateforme de données de santé – avait eu recours, en 2017, à une expertise sur la notion d'intérêt public dans le domaine de la santé[1943]. Le rapport de cette expertise, au terme de l'analyse des textes, de la jurisprudence administrative, des décisions de la CNIL et de la doctrine formule des propositions aux fins de dégager les critères de *l'intérêt public* dans ce seul domaine. Il indique d'abord que l'intérêt public est, dans le cadre précis de l'accès au SNDS, un synonyme de l'intérêt général[1944] et nous apprend ensuite qu'il était déjà fait mention, dans les travaux préparatoires de la loi du 26 janvier 2016, de la vigilance à porter à la définition de *l'intérêt public*. Le rapport signale ensuite que, sous l'empire de la loi du 26 janvier 2016, les critères « *de recherche, d'étude ou d'évaluation* » et « *d'intérêt public* » sont cumulatifs[1945], et affirme que « *le champ matériel de cette finalité* […] *paraît renseigner utilement sur le cadre dans lequel l'existence du critère d'intérêt public doit être appréciée* »[1946]. Il précise en outre que les finalités du SNDS constituent une indication sur les traitements qui pourraient relever de l'intérêt public, ce que mentionnent par ailleurs les débats sur le projet de loi relatif à l'organisation et à la transformation du système de santé[1947]. Il nous semble que, dans le contexte de l'accès aux données du SNDS, l'intérêt public consiste en un standard juridique, dans la mesure où il comporte une « *instruction expresse* […] [*à*] *procéder à une évaluation au cas par cas* ». Le standard n'est en effet pas une norme dont le contenu doit être révélé mais un moyen de « *l'individualisation* […] *de la règle de droit* »[1948]. Aussi, il ne s'apprécie pas au

---

[1943] INDS, *Expertise juridique sur l'intérêt public dans le contexte des données de santé*, étude réalisée par le cabinet Simmons&Simmons, 29 juin 2017.

[1944] Le choix du vocable tiendrait à une volonté de cohérence entre les textes relatifs au SNDS et la loi informatique et liberté qui mentionnent. Le terme d'intérêt public à été substitué lors des débats, à celui d'intérêt général afin de maintenir la cohérence avec les textes européens relatifs à la protection des données à caractère personnel et la loi informatique et libertés (Assemblée nationale, XIVe législature, Session ordinaire de 2014-2015, compte rendu intégral, Troisième séance, 10 avril 2015- *Adde* INDS, *Expertise juridique sur l'intérêt public dans le contexte des données de santé*, étude réalisée par le cabinet Simmons&Simmons, 29 juin 2017, p. 12).

[1945] *Ibid.*, p. 14.

[1946] *Ibid.* Ce qu'affirme d'ailleurs les travaux préparatoires de la loi relative à l'organisation et à la transformation du système de santé (S. RIST et T. MESNIER, *Rapport fait au nom de la commission des affaires sociales sur le projet de loi relatif à l'organisation et à la transformation du système de santé, volume II, commentaires d'articles et annexes*, 14 mars 2019, p. 95).

[1947] Projet de loi relatif à l'organisation et à la transformation du système de santé, Sénat (1ère lecture), Compte rendu analytique de la séance du 6 juin 2019, intervention de Mme la Ministre Agnès Buzin, p. 34.

[1948] Il « *constitue ainsi le lieu privilégié de la rencontre de la règle de droit avec d'autres (règles techniques, morales ou sociales) auxquelles il faut faire appel pour vérifier l'absence ou la présence de la qualité qu'exige la*

regard des critères *de recherche, d'étude ou d'évaluation* mais permet au contraire d'autoriser le traitement pour ces usages. La suppression, d'abord dans la loi informatique et libertés puis dans le Code de la santé publique, de ces mentions nous semble simplement indiquer que le traitement des données issus du SNDS pourra désormais avoir d'autres *buts* au regard desquels la balance entre intérêts privés (commerciaux par exemple) et collectifs (au sens de public) devra permettre de déterminer la finalité d'intérêt public[1949]. Outre la recherche, l'étude ou l'évaluation, qui nécessitent des méthodes particulières appréciées afin de déterminer la durée du traitement et permettent également de déterminer l'existence d'un intérêt public[1950], il pourrait par exemple être invoqué un *but* d'innovation. Ce dernier correspondrait davantage à la nature des *Big data* qui ne répond pas à une méthode scientifique décrite à l'avance en fonction d'un objectif prédéterminé[1951].

390. Quelles conséquences sur le secret professionnel ? De notre point de vue, et au regard des développements antérieurs, il apparaît que l'exigence tenant aux finalités de recherche, d'étude ou d'évaluation pour le traitement des données issues du SNDS participait des garanties en contrepartie de l'exception posée au secret professionnel des professionnels de santé et qui justifiait la transmission de données pseudonymisées aux organismes chargés de la recherche[1952]. Les données pseudonymisées pourraient désormais être transmises à des entreprises privées, des start-up, dès lors que le traitement répond à une finalité d'intérêt

---

règle (internomativité) » (A.-J. ARNAUD (ss. la dir.), *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2e éd., LGDJ, 1993, *V°* « Standard juridique », par P. ORIANNE).

[1949] Sur la nécessité de ne pas considérer l'existence d'une finalité commerciale comme exclusive de l'intérêt public v. Groupe 29, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/45/CE. *Adde* INDS, *Expertise juridique sur l'intérêt public dans le contexte des données de santé*, *op. cit.*, pp. 24-26.

[1950] La CNIL souligne à propos de l'ouverture du SNDS à tout type de traitement : « *cette ouverture conduit par elle-même, à étendre les cas de présentation de demandes de constitution des systèmes fils contenant des données issues du SNDS, y compris pour des traitements effectués en dehors d'une recherche précise et limitée dans le temps* » (Délibération n° 2019-008 du 31 janvier 2019 portant avis sur un projet de loi relatif à l'organisation et à la transformation du système de santé (demande d'avis n° 19001144)).

[1951] C'est en ce sens que la CNIL semble d'ailleurs entendre l'extension du SNDS : « *Si l'extension prévue dans le projet de loi peut se justifier par des objectifs d'aide à la recherche et à l'innovation dans le domaine de la santé, et si l'évaluation de la conformité de l'ensemble du dispositif suppose l'intervention des actes réglementaires d'application, en l'absence de toute précision dans le projet de loi sur l'architecture précise du dispositif, la Commission appelle dès maintenant l'attention sur la problématique majeure du respect, en pratique, des principes de limitation des finalités et de minimisation des données par ces nouveaux traitements, évoluant dans un contexte d'accumulation de données pour alimenter les algorithmes d'intelligence artificielle* » (Délibération n° 2019-008 du 31 janvier 2019 préc.).

[1952] V. n° 177¤. Il faut noter que cette exigence avait déjà été supprimée, dans l'article 66 de la loi informatique et libertés, par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

public[1953]. Pourtant, sur la question du secret professionnel, les travaux préparatoires de la loi relative à l'organisation et à la transformation du système de santé sont muets. De la même manière, le rapport de la mission de pré-figuration sur la future plateforme des données de santé et l'avis de la CNIL sur le projet n'évoquent, à aucun moment, le secret professionnel. Seul le CCNE, dans son avis relatif à la santé et aux données massives, mentionne à plusieurs reprises le « secret médical »[1954]. Le rapport met en exergue l'existence de dangers pour le « secret médical » s'inquiètant principalement du recours, pour le traitement des données massives en santé, à un nombre croissant d'acteurs qui n'appartiennent pas au domaine de la santé mais répondent à une logique « *d'exploitation d'un marché* »[1955]. Le danger mis en avant par le Comité nous semble toutefois mal identifié. La question n'est pas tant de savoir si la multiplication des acteurs engendre un risque, puisque toutes les personnes ayant accès à des données de santé à caractère personnel issues d'une prise en charge par des personnes intervenant dans le système de santé sont soumises au secret professionnel[1956], que de constater que la protection ces données, une fois admise la dilution du secret professionnel médical, relève de mécanismes non-juridiques[1957].

391. Quel lien avec le secret professionnel dans le domaine de la santé ? Il nous semble toutefois que les motifs d'inquiétude tenant à la réidentification potentielle des personnes ne doivent pas être surestimés, ce risque ne relevant pas, par ailleurs, d'une violation du secret professionnel. Les enjeux soulevés par les *Big data* tiennent à la valorisation des données résultant d'une « *logique inductive et non plus déductive* »[1958]. Aussi, les interrogations portent actuellement sur la nature de données secondaires issues de la valorisation des *Big data*. L'enjeu dépasse donc très largement la protection de l'intimité des personnes[1959]. Plus encore, la

---

[1953] Cela s'inscrit donc dans le prolongement de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
[1954] Nous notons neuf occurrences du terme (CCNE, *Données massives et santé : Une nouvelle approche des enjeux éthiques*, Avis n° 130, 29 mai 2019).
[1955] *Ibid.* p. 19 et p. 50.
[1956] CSP, art. L.1461-1, IV, 2°.
[1957] V. *infra* Titre II Partie II.
[1958] C. ZOLYNSKI et A. LATREILLE, « Nouvelle pratiques : faut-il de nouvelles protections ? », *in* N. MARTIAL-BRAZ (ss la dir.), *La proposition de règlement européen relatif aux données à caractère personnel : propositions du réseau Trans Europe Experts*, coll. Trans Europe Experts, Société de législation comparée, 2014, p. 265.
[1959] « […] *dans le contexte de la révolution du Big Data et de l'Intelligence artificielle, nombreux plébiscitent désormais de compléter cette vision individualiste de la protection des données personnelles en admettant*

concurrence internationale quant au développement de l'intelligence artificielle guide l'ouverture des données de santé et un certain libéralisme. Quant bien même ce mouvement engendrerait un risque pour les personnes, l'enjeu de la souveraineté numérique dans le contexte de montée en puissance des GAFAM est cruciale. Ce qui précède doit être lu au prisme de la politique européenne du numérique à propos de laquelle Madame Castets-Renard remarque que l'un « *des enjeux géopolitiques sous-jacents est aussi de faire face à la domination des géants américains d'internet (les fameux « GAFAM » - Google, Amazon, Facebook, Apple, Microsoft - mais aussi les sociétés de l'économie du partage, tels Uber, Airbnb...) en encourageant les entreprises européennes à proposer des services innovants ou alternatifs* »[1960]. La vice-présidente du Conseil national du numérique, Madame Peugeot, résume ainsi la question de l'accès aux données de santé : « *Si cette course à la massification et à la "désanonymisation" ne peut qu'inquiéter* […]*, la stratégie industrielle qui sous-tend le projet est intéressante : il s'agit ni plus ni moins que de contrer le déploiement intensif de géants états-uniens dans le champ de l'intelligence artificielle et de rouvrir un espace compétitif pour des acteurs de petite ou moyenne taille qui pourront avoir accès à ces données. Encore faut-il accepter la logique de mutualisation* »[1961]. Cet encouragement consiste notamment dans la mise en oeuvre d'une gestion publique des données de santé à caractère personnel.

S'il est évident que le professionnel qui prend en charge le patient n'est pas « dépossédé » de son savoir et qu'il est toujours tenu de taire les informations dont il a connaissance et de veiller à la confidentialité de leur support, il n'en est plus l'unique gardien. Aussi ce n'est pas la dimension juridique du secret professionnel qui est atteinte mais sa dimension sociologique et politique : « *Cette dimension politique met en lumière ce qui sous-tend le rapport entre l'information et le secret, entre la rétention et la diffusion du savoir : l'information comme pouvoir. En effet, l'information constitue un pouvoir dès l'instant qu'elle n'est pas partagée, dès l'instant qu'elle est appropriée par une personne, un groupe, une classe* »[1962]. C'est cette dimension du secret professionnel qui est touchée, sans que la vie privée

---

également la protection d'intérêts collectifs […] *la plupart des algorithmes fonctionnent non à l'échelle de la personne mais à celle du groupe et les données ne sont pas tant granulaires que réticulaires, c'est-à-dire organisées en réseau. Elles peuvent dès lors être exploitées afin de produire des corrélations concernant des segments ou groupes d'individus* […] » (C. ZOLYNSKI, « Les nouveaux contours de l'action de groupe et de l'action collective au lendemain de la loi pour la protection des données : un *empowerment* renforcé », *Dalloz IP/IT* 2018, p. 470).

[1960] C. CASTETS-RENARD, « Marché unique numérique » : la Commission européenne présente les premières mesures en droit d'auteur », *D.* 2016, p. 388.

[1961] V. PEUGEOT, « Données de santé : contours d'une controverse », *L'Économie politique*, 2018/4, n° 80, p. 40.

[1962] M.-A. FRISON-ROCHE (ss. la dir.), *Secrets professionnels*, coll. Essais, Édition Autrement, 1999, p. 29.

des personnes ne soit elle-même atteinte. Sans doute peut-on exprimer l'idée que cette dimension du secret professionnel porte en elle une partie de la légitimité de la règle juridique. Si l'on admet que les données issues de la prise en charge des personnes dans le domaine de la santé sont désormais *des communs* l'affaiblissement du pouvoir des professionnels tenus au secret en est un corollaire.

392. Conclusion de second chapitre : Le secret professionnel a fait l'objet d'aménagements successifs, sous-tendus par une logique de compromis. Cette approche met en balance les intérêts au service desquels est mis le traitement et ceux protégés par le secret professionnel. Ce dernier ressort souvent perdant de cette conciliation.

Outre ce premier mouvement, l'on constate une ouverture progressive de la réutilisation des données à caractère personnel couvertes par le secret professionnel. Elle se manifeste en premier lieu par le constat que la personne n'a pas pleinement maîtrise de ses données. Affirmée dans le disours d'une majorité de la doctrine, elle n'est que très partielle[1963]. Parallèlement, les professionnels voient également leur maîtrise de ces données se réduire. La logique d'accès et la mise en réseau participent de ce phénomène. Les acteurs principaux de la prise en charge, à savoir les professionnels soumis au secret et les personnes concernées n'ont pas la pleine maîtrise des données, ni même une co-maîtrise. L'on constate par ailleurs que les données produites à l'occasion d'une prise en charge sont désormais qualifiées de biens communs. Or, le « secret » moyen, la réservation des données qu'il implique, est antinomique à celle de *communs*. L'idée des données de santé comme *communs* participe du diagnostic d'affaiblissement de la portée du secret professionnel.

393. Conclusion du premier titre : Le secret professionnel, soit le secret comme « moyen » juridique, semble de moins en moins privilégié pour assurer la réservation des données. Les critères, considérés par la doctrine comme traditionnellement attachés à la désignation des

[1963] Nous mentionnerons ici, car les travaux préparatoires sont encore en cours, l'article 11 du projet de loi n° 2187 relatif à la bioéthique. Cet article prévoit la possibilité pour le médecin de recourir au « traitement algorithmique de données massives », la question du consentement du patient au recours à une telle méthode a fait l'objet de débats. Nous remarquons que la question de la réutilisation des données, leur intégration à ces traitement massifs destiné à nourrir l'intelligence artificielle ne s'est pas posée. Des réflexions auraient toutefois pu être menées car il n'est plus certain que cet usage entre dans les seules finalités de médecine préventive, de diagnostic et de soins (Assemblée nationale, XV^e^ législature, Session ordinaire de 2019-2010, Compte rendu intégral, Deuxième séance du vendredi 4 oct. 2019, art. 11).

personnes qui y sont astreintes, ne permettent plus d'expliquer certaines évolutions législatives. Il n'est pas certain, par ailleurs, que la nature des informations soit réellement importante dès lors qu'il est impossible d'évaluer avec certitude la portée de la désignation prévue à l'article L. 1110-4 du Code de la santé publique. L'on constate toutefois que les acteurs techniques et les personnes réutilisant les données sont explicitement soumis au secret professionnel. Ils ne semblent néanmoins pas bénéficier de l'option de conscience offerte aux professionnels de santé ou à ceux de l'action sociale et médico-sociale. Nous avons considéré qu'il s'agissait de secrets de « second rang » puisque leur portée est moindre. La norme est ainsi réduite à un instrument, il n'est plus tenu compte de ses fondements axiologiques. La doctrine de la CNIL n'est pas étrangère à cette évolution. La confiance, critère de la confidentialité, doit être créée à l'égard de tous les acteurs. Tandis que le secret professionnel était institué en raison de la confiance nécesssaire que le professionnel devait inspirer en raison de rôle social, le secret professionnel est désormais un outil de confiance dans le traitement des données et dans les technologies numériques.

394. L'assujettissement au secret professionnel de nouveaux acteurs emporte autant de permissions et d'obligations de révéler à l'égard des professionnels qui rencontrent la personne prise en charge. C'est un compromis qui s'opère alors entre les finalités assignées aux traitements de données mis en œuvre par l'Etat et les personnes publiques et le secret professionnel. Les aménagements opérés tiennent principalement à la réutilisation des données à des fins de recherche dans le domaine de la santé, de statistiques, d'évaluation et de maîtrise des dépenses ainsi que, dans une moindre mesure, de maintien de l'ordre public. Contrairement à ce que laisse pressentir le discours de la doctrine et des acteurs politiques, le consentement de la personne n'est qu'une cause de justification parmi d'autres. Il semble même que ce soit plutôt un droit d'opposition qui soit offert aux personnes lorsqu'il s'agit de permettre l'accès aux données issues de la prise en charge. L'accès est en effet le nouveau « maître mot » du traitement des données à caractère personnel dans le domaine de la santé. La mise en réseau progressive des données favorise cette évolution, elle se concrétise par une mise en commun des utilités des données produites par les acteurs du système de santé. Si le secret professionnel ne semble plus être le mécanisme adéquat de la réservation des données, d'autres moyens, extérieurs au droit, assurent cette fonction. Le secret conçu comme « moyen » fait l'objet d'une normalisation croissante.

TITRE II. Le secret comme moyen hors du droit

395. Les données de santé seraient désormais des communs, le partage des utilités des données traitées participe à la disparition du pouvoir des professions, corollaire de leur place dans la société[1964]. Il s'agit, à présent de prolonger cette dernière démonstration et de confirmer le mouvement que nous avons dessiné, pas à pas : l'affaiblissement du secret professionnel, dans toutes ses dimensions (juridique et politique), ne signifie nullement la disparition du « secret médical » si l'on admet que l'expression peut désigner l'état de secret ainsi que nous l'avons expliqué en amont.

Il semble toutefois que le « secret médical » entendu comme le moyen de réserver l'information ne soit pas privilégier protéger le secret des données issues de la relation de soin. Plus encore, cette protection ne peut plus être assurée par les seules normes juridiques. Si les dispositifs techniques de l'information et de la communication comportent un risque pour le « secret médical », ce n'est pas tant celui d'une disparition de la situation de secret que d'une mise à la marge du secret professionnel et, plus généralement, de la norme juridique. Dans la « reproduction numérique du monde », « l'écosystème des données de santé », la normalisation joue un rôle de premier ordre. Il s'agira donc de voir comment le secret « moyen » est assuré *ex ante* par des normes dont la particularité est de répondre aux enjeux du monde numérique **(Chapitre I)** et comment le trait caractéristique de ces normes, la souplesse, permet leur adaptation dans un contexte de globalisation **(Chapitre II)**.

[1964] V. *supra* chapitre I, titre I, partie II.

Chapitre 1 - La diversification des dispositifs normatifs

396. Contexte et plan de chapitre. Lors de nos précédents développements, nous avons expliqué que l'obligation de sécurité et de confidentialité des traitements de données à caractère personnel qui pèse sur le responsable de traitement et le sous-traitant consistait notamment à s'assurer que les données ne soient accessibles qu'aux seuls tiers autorisés. L'examen des décisions de la CNIL et de la jurisprudence nous a permis de dégager les critères de détermination des tiers autorisés (*a contrario* des tiers non-autorisés) : le secret professionnel peut constituer une garantie suffisante de confiance en vertu de laquelle une personne, les membres d'un organisme ou d'une institution, peuvent avoir accès à des données à caractère personnel ; le critère de nécessité consiste ensuite à prendre en compte les fonctions des personnes afin de déterminer, au regard de la finalité du traitement, si celles-ci ont besoin des données. Nous avons ensuite formulé l'idée, au regard de la doctrine de la CNIL, selon laquelle cette définition des tiers autorisés s'est trouvée en contradiction avec les hypothèses dans lesquelles la loi ou le règlement autorisait ou permettait la révélation d'une information à caractère secret. Cette contradiction a été progressivement gommée par les aménagements successifs du secret professionnel. Nous avons alors expliqué que ces transformations avaient pour finalité de permettre une réutilisation accrue des données. Dans l'espace de plus en plus large laissé à la circulation des données, il incombe au responsable de traitement de mettre en œuvre les moyens propres à garantir le respect des secrets garantis par la loi[1965], c'est-à-dire la confidentialité des traitements. Il lui revient alors de préserver la sécurité des données, des échanges et des systèmes. Ces moyens font l'objet d'une normalisation qu'il s'agira de mettre en lumière **(section 2)**. Il faut, avant de l'envisager, déplacer notre regard afin de replacer le mouvement que nous souhaitons décrire dans un autre, plus vaste, qui impose une réflexion *sur* le droit **(section 1)**.

[1965] V. Les considérants 74 et 75 du RGPD qui précisent que le responsable du traitement doit mettre en œuvre des mesures appropriées et effectives permettant d'éviter « *une perte de confidentialité de données protégées par le secret professionnel* ». La loi informatique et libertés contenait déjà une telle disposition avant l'entrée en vigueur du RGPD, elle a d'ailleurs toujours précisé que lorsque le traitement est soumis à des formalités préalables les demandes d'avis doivent préciser « *Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi* » (LIL, art. 33 9°).

Section 1 - L'existence de normes étrangères au droit

397. Il s'agira dans un premier temps décrire la place du droit dans l'espace des normativités **(paragraphe 1)** afin de mieux cerner le phénomène de normalisation technico-managériale **(paragraphe 2)**.

§ 1 - Le droit dans l'espace des normativités

398. Un mouvement. L'obligation de sécurité et de confidentialité consiste dans le fait de mettre en œuvre les mesures organisationnelles et techniques adaptées. Les caractéristiques de ces mesures, qui consistent également en une forme de secret « moyen », doivent à présent être déterminés. Ces derniers sont appuyés sur des dispositifs normatifs variés : des guides de bonnes pratiques, des référentiels, mais aussi des normes techniques et managériales. Porter un regard sur ce mouvement impose la prudence. De quel mouvement parle-t-on ? C'est à cette question que nous tenterons de répondre, dans un premier temps.

Jusqu'à présent, les normes sur lesquelles nos développements ont porté n'ont pas posé question quant à leur rapport au droit. Nous avons investi la notion de « secret médical » et la façon dont le droit s'est saisi des dispositifs techniques en adoptant, de la même manière que les auteurs auxquels nous succédons, un point de vue positiviste, c'est-à-dire en prenant pour acquise une certaine conception du droit. Ainsi, il a été tenu pour acquis que le « secret médical » désignait l'obligation faite à certaines personnes de ne pas révéler les informations et les données venues à leur connaissance, obligation dont le manquement est pénalement sanctionné, ce que l'on désigne comme le secret professionnel. L'expression recouvre une prérogative défensive offerte aux individus et leur permettant de demander réparation dès lors qu'un tiers à la relation de soin a porté atteinte à ce secret en prenant connaissance des informations ou en les révélant. Le Code de la santé publique contient par ailleurs une infraction spécifique sanctionnant le fait de prendre ou de chercher à prendre connaissance de ces informations couvertes par le secret professionnel. Enfin, l'évolution des dispositifs techniques a amené à interroger l'articulation entre l'obligation de sécurité et de confidentialité – telle qu'en dispose le RGPD et la LIL – et le secret professionnel pour ensuite analyser l'évolution du champ d'application et du régime de l'infraction. A aucun moment donc la nature de ces normes n'a été mise en question, car il est communément admis qu'elles sont *juridiques*. Cette posture est toutefois mise en difficulté, en raison de l'explosion des normes qualifiées de *droit souple* et du rôle croissant des normes techniques et managériales dans la

protection des données couvertes par le secret et pour la garantie du respect du secret professionnel. La présence de ces normes, « *objets normatifs non ou mal identifiés* […] *dont le caractère juridique est douteux ou controversé, mais qui produisent en pratique ou tentent de produire des effets de régulation* »[1966], nous invite à un détour par la réflexion *sur* le droit et non plus seulement *en* droit.

399. Normes et normes juridiques. Nous pourrions exposer et développer à l'envi les différentes conceptions de ces termes, nous avons toutefois fait le choix de la synthèse avec tout ce qu'elle a d'imparfait. Le chemin emprunté pourrait en effet nous entrainer sur des terrains de réflexions dont jamais nous ne sortirions et nos développements sur ses points seraient alors trop denses et nous éloigneraient de notre étude, ils demeureraient néanmoins toujours incomplets et trop pauvres pour apporter un éclairage sur ce qui se place à la base de toute réflexion sur le droit. Notre ambition est plus modeste, il nous faut replacer nos propos dans un mouvement plus vaste et trouver quelques jalons méthodologiques pour le décrire au regard de notre objet.

400. Les différentes conceptions de ces termes pourraient être développées à l'envi, nous avons toutefois fait le choix de la synthèse avec tout ce qu'elle a d'imparfait. Le chemin emprunté pourrait en effet nous entraîner sur des terrains de réflexion qui dépassent largement l'objet de notre étude. Notre ambition est plus modeste, l'objectif étant de se replacer dans un mouvement plus vaste et de déterminer quelques jalons méthodologiques pour décrire ce mouvement au regard de notre objet.

Si le droit peut être défini comme une technique de direction des conduites humaines, la norme est considérée comme son instrument[1967]. Le détour par l'étymologie, dont le rappel est systématique pour quiconque entreprend de définir le droit, nous apprend que la norme est ainsi métaphoriquement désignée par référence à un outil de mesure, *norma*, et plus précisément une équerre[1968]. La norme peut alors être directement rapprochée du terme *règle*, qui « *fait*

[1966] B. FRYDMAN, « Comment penser le droit global ? » *in* J.-Y. CHEROT et B. FRYDMAN, *La science du droit dans la globalisation*, coll. Penser le droit, Bruylant, 2012, p. 20.
[1967] P. AMSELEK, « Le droit, technique de direction publique des conduites humaines, *Droits*, 1989, n° 10, p.7.
[1968] L'on ne citera qu'un ouvrage d'un seul auteur pour la précision de ces développements sur la nature d'outil des règles et des normes, que l'auteur considère comme synonymes : P. AMSELEK, *Cheminements*

apparaître le même passage du concret à l'abstrait »[1969] et dont l'étymologie désigne un outil servant à tracer des lignes droites[1970]. La norme – qui désigne *toujours* un outil pour Monsieur Amselek[1971] – connaît une multitude de définitions selon l'usage qui en est fait[1972] et selon l'angle sous lequel elle est observée[1973]. En droit, le terme sera alors, en fonction, distingué ou non du terme de *règle*[1974]. Indépendamment de cette possible distinction, la question de la définition de la norme revêt une importance centrale pour la théorie du droit[1975] : trouver les critères distinctifs de la norme juridique afin de pouvoir définir *le droit*. Cette distinction n'a d'intérêt que parce que, dans la masse des dispositifs qui peuvent *orienter les conduites* et qui seraient donc *normatifs*, la norme n'est que l'un des outils disponibles[1976]. Plus encore, le droit n'est qu'un mode de régulation, dans ce que Monsieur Ost désigne comme le

---

philosophiques dans le monde du droit et des règles en général, coll. Le temps des idées, Armand Colin, 2012, spéc. pp. 56-60.

[1969] *Ibid.,* p. 58.

[1970] *Ibid*.

[1971] *Ibid.,* p. 59.

[1972] La norme peut être un énoncé impératif ou prescriptif ; la signification de cet énoncé (H. KELSEN, *Théorie pure du droit,* 2e éd., Dalloz, 1962) ; un instrument de mesure, un modèle (P. AMSELEK, « Normes et loi » *Arch. ph. dr.*, Sirey, 1980).

[1973] L'on trouve, dans le dictionnaire encyclopédique de théorie et de sociologie du droit plusieurs définitions à l'entrée « norme ». Outre les sens que l'on pourrait qualifier de généraux, la diversité des conceptions de la norme s'exprime en anthropologie du droit, en logique, en sémiotique, en sociologie du droit et en théorie du droit (A.-J. ARNAUD (ss. la dir.), *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2e éd., LGDJ, 1993, *V°* « Norme » par M. JORI et N. ARNAUD-DUC).

[1974] Souvent selon le degré de généralité, sur ce point v. A.-J. ARNAUD (ss la dir.), *Dictionnaire encyclopérdique de théorie et de sociologie du droit*, *op. cit.*, *V°* « Norme (en anthropologie du droit) » par E. LE ROY, n° 2 et *V°* « Norme (en théorie du droit) » par M. TROPER, n° 3. Pour un autre éclairage, v. C. THIBIERGE, « Au coeur de la norme : le tracé et la mesure. Pour une distinction entre normes et règles de droit », *Arch. phil. dr.*, Dalloz, 2008, p. 341. Normes et règles sont généralement distinguées en droit mais il est également possible, dans une perspective plus vaste, de considérer que les règles juridiques sont un sous-ensemble des normes juridiques. Utiliser le terme de *norme juridique* signale simplement un degré de généralité supplémentaire, or nous ne nous situons pas *en* droit mais tentons d'observer la norme juridique dans l'espace plus vaste du normatif.

[1975] Monsieur Troper explique que la distinction entre *théorie du droit* et *philosophie du droit* « *est raisonnable, mais ne correspond pas à l'emploi effectif des expressions* « philosophie du droit » *et* « théorie générale du droit ». *En pratique, il est impossible d'établir une corrélation entre le titre d'un ouvrage et la liste des questions qu'il aborde, le niveau d'abstraction auquel il se situe, la méthode qu'il emploie ou le courant doctrinal auquel il appartient*. *Le bon sens commande donc de prendre ces expressions pour des synonymes*. » (M. TROPER, *La philosophie du droit*, coll. Que sais-je ? PUF, 2015, p. 12). Nous utilisons néanmoins l'expression à dessein puisque la recherche des critères de la norme juridique dans l'espace du normatif a pu correspondre à une démarche qui « *viserait exclusivement à décrire et analyser le droit tel qu'il est, grâce à l'emploi d'une méthode scientifique, et se voudrait pure de tout jugement de valeur* » (*Ibid.*).

[1976] Pour ne prendre qu'un seul exemple, *les nudges* peuvent être considérés comme normatifs : « *On en arrive même à constater la montée en puissance d'une gouvernance sans véritables normes, en se penchant sur l'empire des statistiques et la nébuleuse des nudges, ces objets normatifs non identifiés qui prolifèrent aujourd'hui, et qui, à l'instar d'un coup de coude, incitent « en douceur » à adopter le comportement souhaité* » (F. OST, *A quoi sert le droit ? Usages, fonctions, finalités*, coll. Penser le droit, Bruylant, 2016, pp. 3-4).

« *grand tout culturel* »[1977] désignant l'espace de la normativité sociale, au sein duquel le droit prend place, sans que cette place ne lui soit assurée. C'est dans la quête de la distinction du droit que sont nées les différentes approches de la norme juridique par rapport ou dans leur rapport avec, d'abord, les normes morales[1978] ou religieuses[1979]. L'on ne pourra développer ces théories[1980], il importe toutefois de rappeler que la norme juridique est habituellement présentée comme remplissant certains critères caractéristiques : le premier est l'obligatoriété et la sanction qui s'y rattache ; le deuxième tient à l'entité dont elle émane : l'Etat – ayant le monopole de la violence légitime –, présenté comme l'unique producteur de la norme juridique[1981] ; le troisième critère est celui de la validité[1982]. Cette présentation du droit constitue la base du positivisme[1983] au sens large, c'est-à-dire une théorie systémique du droit représentée par la pyramide. Si nous évoquons principalement ces critères, d'autres ont pu être posés, par

---

[1977] F. OST, *A quoi sert le droit ? Usages, fonctions, finalités*, *op.cit.*, p. 6, p.114-115, p. 371 et p. 557.

[1978] La distinction entre normes juridiques et normes morales a revêtu une importance fondamentale en ce qu'elle pose la question des finalités de la norme juridique. La pensée de Hans Kelsen, dont le succès fut considérable et perdure, a notamment consisté à élever le droit au rang de science. C'est pourquoi il s'est avéré nécessaire de départir son étude de toute appréciation subjective et donc de tout jugement d'ordre moral. Partant, et en simplifiant quelque peu, le « normativisme » dont il est le père, a donc consisté à présenter le droit comme un système ou un ordre dans lequel la norme est juridique car conforme à la norme qui lui est supérieure au sein de cet ordre.

[1979] P. LEGENDRE, *Sur la question dogmatique en Occident*, Fayard, 1999, p. 13 ; *Adde* A. SUPIOT, *Homo juridicus. Essai sur la fonction anthropologique du Droit*, coll. Essais, Points, 2005, p. 30, expliquant la singularité du droit au regard de ses « *ressources d'interprétation* » par rapport à la religion : « *La particularité du Droit depuis son apparition dans l'Antiquité greco-romaine, est de s'être progressivement détaché de cette origine religieuse et d'avoir opéré ce que Louis Gernet a pu appeler une « laïcisation de la parole ». Le Droit est ainsi devenu une technique de l'Interdit. C'est une technique parce que son sens n'est pas enfermé dans la Lettre d'un Texte sacré et immuable, mais procède, comme celui de n'importe quel autre objet technique, de fins qui lui sont données de l'extérieur par l'Homme, des fins humaines et non pas divines* ».

[1980] L'on pourra évidemment se reporter à quelques manuels qui sont le support adéquat à ce type de panorama et notamment, présentant les théories ayant connu un rayonnement certain : R. SEVE, *Philosophie et théorie du droit*, 2e éd., coll. Cours, Dalloz, 2017 ; v. également l'excellente introduction générale au droit de P. DEUMIER, *Introduction générale au droit*, 5e éd., coll. Manuel, LGDJ, 2019.

[1981] « *L'Etat seul détenteur du pouvoir de contraindre et source unique du droit. - Le droit peut, à mon avis, se définir exactement : l'ensemble des normes en vertu desquelles, dans un Etat, s'exerce la contrainte. Cette définition renferme deux éléments : la* norme*, et la réalisation de celle-ci par la* contrainte. *Les statuts sociaux sanctionnées par la contrainte publique, constituent seuls le droit. Or, nous l'avons vu, l'Etat est le souverain détenteur de cette contrainte. Les prescriptions revêtues par lui de cette sanction, sont donc seules des normes juridiques. En d'autres termes,* l'Etat est l'unique source du droit » (R. VON JHERING, *L'évolution du droit*, Librairie A. Marescq, 1901, p. 215).

[1982] Validité à une norme supérieure dans l'ordre juridique, selon la théorie Hans Kelsen.

[1983] Le positivisme peut désigner une approche du droit, il est alors épistémologique. L'un de ses plus éminents représentants est Norberto Bobbio, lequel adoptait un mode « *caractérisé par une distinction nette entre le droit réel et le droit idéal… entre le droit tel qu'il est et le droit tel qu'il devrait être et pas la conviction que le droit dont les juristes doivent s'occuper est le premier et non pas le second* » (cité par M. TROPER, *V°* « Positivisme » *in* A.-J. ARNAUD (ss la dir.), *Dictionnaire encyclopédique de théorie et de sociologie du droit*, *op. cit.*).

exemple celui de l'effectivité sociale[1984]. Il n'importe toutefois pas tant d'énumérer ces critères que de souligner que chacune des théories ayant proposé une définition de la norme juridique en apporte un éclairage différent à partir de ces mêmes critères[1985]. Par ailleurs, les critères d'obligatoriété et ceux tenant à la source de la norme juridique se sont trouvés tout à fait relativisés sous l'effet conjugué de la mondialisation – qui participe selon Monsieur Frydman de l'émergence d'un droit global[1986] – et de l'évolution des fonctions de l'Etat[1987]. La *soft law*, depuis longtemps identifiée mais d'abord cantonnée à l'ordre international[1988], est l'une des

---

[1984] Critère posé par la *sociological jurisprudence*, courant de pensée juridique amércain exposé par F. MICHAUT, *V°* « Etats-Unis (Grands courants de la pensée juridique américaine contemporaine) » *in* D. ALLAND, S. RIALS, *Dictionnaire de la culture juridique*, Lamy-PUF, 2003.

[1985] V. en ce sens P. DEUMIER, *Introduction générale au droit*, *op. cit.*, p. 40; Usant d'une métaphore que nous trouvons éclairante, Monsieur Sève explique : « […] *les différentes approches de la règles sociale, juridique ou morale se situent dans une sorte de salon élégamment décoré mais que chaque occupante (les théories) met diversement en valeur par un jeu d'éclairage, en positionnant ses lampes et en jouant les intensités de chaque éclairage* » (R. SEVE, *Philosophie et théorie du droit*, *op. cit.*, n° 217).

[1986] La formule tient à la méthode de l'auteur, qui, pour traiter des questions que la mondialisation pose au droit, prend le parti méthodologique de se départir du concept d'ordre juridique « *pour envisager immédiatement les normes et les interactions juridiques entre les acteurs en tant que telles, indépendamment du ou des ordres dans lesquels elles s'inscrivent ou non* » (B. FRYDMAN, « Comment penser le droit global », *in* J.-Y. CHÉROT et B. FRYDMAN (ss. la dir.), *La science du droit dans la globalisation*, coll. Penser le droit, Bruylant, 2012, p. 17, spéc. p. 23).

[1987] On se reportera notamment à la littérature relative à *l'Etat postmoderne*, qui se manifeste par le passage du gouvernement à la gouvernance, de la règlementation à la régulation, mouvement mis en exergue par Monsieur Chevallier, qui explique notamment, au travers des transformations des fonctions de l'Etat, comment le droit « *a perdu les attributs de systématicité, généralité et stabilité, qui* (le) *caractérisaient* » (J. CHEVALLIER, « Vers un droit post-moderne ? Les transformations de la régulation juridique », *RDP* 1998, pp. 659-714). L'approche du droit serait désormais nécessairement complexe : « *La complexité se mesure d'abord à la multiplicité des foyers de droit, très diversement articulés les uns aux autres, ce qui tend à transformer l'ordre juridique en une construction baroque ; elle se mesure aussi à l'éclatement des processus d'élaboration des normes, qui font désormais appel à de nombreux intervenants* » (*Ibid.*). L'éclatement des foyers du droit a affermi les thèses du pluralisme juridique défendues par des auteurs tels que Santi Romano (S. ROMANO, *L'ordre juridique*, trad. fr. de la 2e éd. (1946) par L. François et P. Gothot, Dalloz, 1975), Georges Gurvitch (G. GURVITCH, *L'expérience juridique et la philosophie pluraliste du droit*, Pedone, 1935) et plus récemment Monsieur Vanderlinden (J. VANDERLINDEN, *Les pluralismes juridiques*, coll. Penser le droit, Bruylant, 2013). La gouvernance conduit à une négociation, un mode participatif de l'élaboration des règles où des acteurs, traditionnellement destinataires de la norme juridique, prennent place (par exemples les lobbies : M. MEKKI, « L'influence normative des groupes d'intérêt : force vive ou force subversive », *JCP G* 2009, partie 1 n° 43, p. 370, et partie 2, n° 44, p. 392 ; les experts : V. LASSERRE, *Le nouvel ordre juridique. Le droit de la gouvernance*, LexisNexis, 2015). Enfin, « *Le droit post-moderne est conçu essentiellement comme un droit pragmatique, sous-tendu par une volonté d'action sur le réel ; cette préoccupation d'efficacité modifie en profondeur la conception traditionnelle de la normativité : à la rigidité fait place la souplesse et à la stabilité l'adaptabilité* » (J. CHEVALLIER, « Vers un droit post-moderne ? Les transformations de la régulation juridique », *RDP* 1998, *op. cit.*).

[1988] Si tant est que l'on admette l'existence de plusieurs ordres juridiques : « *Ces formes de normativité relative pouvaient être réservées à cet ordre imparfait qu'est l'ordre international, une sorte de pis-aller à son incapacité à agir par la contrainte* » (P. DEUMIER, *Introduction générale au droit*, *op. cit.*, n° 31).

manifestations de ces évolutions. Des normes, qui proposent plus qu'elles n'imposent[1989], dont les sources de production sont multiples et diverses autant que leurs modes d'élaboration et qui produisent des effets juridiques[1990] ou des effets de régulation[1991], ont remis en cause les théories traditionnelles du droit. Repenser l'approche du droit confronté à toutes sortes « *d'anomalies* » c'est l'immense entreprise de Messieurs Ost et Van de Kerchove. Dans l'un de leurs ouvrages les plus remarqués, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, les auteurs proposent, comme substitut du paradigme dominant de la pyramide des normes, comme cadre théorique de la pensée juridique, celui du *réseau*[1992]. C'est alors au travers d'une forme de graduation qu'est pensée la juridicité des normes, selon une vision *tridimensionnelle de la validité* axée autour de trois pôles : légalité, effectivité et légitimité[1993]. Il s'opère, en somme, un effacement progressif des critères traditionnels de la norme juridique. Malgré notre volonté de décrire, ce court développement révèle déjà une certaine inclinaison

---

[1989] Le propre du *soft law* et qu'il est mou, doux et qu'il relève d'une « *direction juridique non autoritaire des conduites* » (P. AMSELEK, « L'évolution générale de la technique juridique dans les sociétés occidentales », *RDP* 1982, p. 287).

[1990] Par exemple sur le droit souple produit par les autorités administratives indépendantes et que nous avons déjà citées auparavant : S. GERRY-VERNIERES, *Les « petites » sources du droit : à propos des sources étatiques non contraignantes*, coll. Recherches juridiques, Economica, 2012.

[1991] « […] *plus généralement, la norme juridique tend à être englobée dans une problématique plus large de la régulation, qui infléchit sa logique : Visant à assurer la reproduction des équilibres sociaux, la régulation suppose en effet le recours à une panoplie de moyens d'action, les uns juridiques, les autres non-juridiques ; le droit n'apparaît plus que comme un instrument de « guidance » ou de « pilotage », au service de politiques qui le dépassent. Ce glissement est très explicite dans le cas des autorités administratives indépendantes : ces autorités sont dotées d'une série de pouvoirs juridiques, dont le cumul contraste avec les typologies classiques ; mais ces pouvoirs sont mis au service d'une fonction plus globale de régulation sectorielle, qui passe aussi par des moyens plus informels d'influence et de persuasion. La problématique de la régulation débouche ainsi sur une vision instrumentale du droit, faisant passer au second plan l'idée de commandement qui était au coeur de la conception moderne* » (J. CHEVALLIER, « Vers un droit post-moderne ? Les transformations de la régulation juridique », *RDP* 1998, *op. cit.*).

[1992] F. OST et M. VAN DE KERCHOVE, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, FUSL, 2002.

[1993] *Ibid.* Pour penser ces normes à la juridicité réduite ou relative, Madame Thibierge propose de développer une méthode basée sur un concept précisément forgé à cette fin : *la force normative*. Les travaux collectifs dirigés par l'auteur conduisent à proposer un outil de diagnostic permettant d'intégrer dans la sphère du droit des normes qui ne répondent pas aux critères traditionnels de la norme juridique. Sans les évacuer ces critères ne sont plus que *l'un* des marqueurs composant les trois pôles de la force normative : valeur normative, garantie normative et portée normative (C. THIBIERGE (ss. la dir.), *La force normative. Naissance d'un concept*, LGDJ-Bruylant, 2009, spéc. la conclusion rédigée par Madame Thibierge, p. 813 et svt). Un ouvrage regroupant juristes québécois, belges et français évoque la nécessité de « reformater » la norme juridique. Monsieur Ost et Madame Thibierge y contribuent d'ailleurs, le premier dans le prolongement de ses travaux sur les sources du droit revisitées et la seconde au regard du concept de force normative (L. LALONDE et S. BERNATCHEZ (ss. la dir.), *La norme juridique « reformatée ». Perspectives québécoises des notions de force normative et de sources revisitées*, éd. RDUS, 2016).

puisque nous considérons que le droit – si tant est qu'il puisse être défini – n'est qu'une forme de normativité parmi d'autres, et que le positivisme juridique – issu de la pensée de Hans Kelsen et encore étudié dans nos facultés – rend le juriste aveugle à certaines évolutions. Il en est une qui nous intéresse au premier chef et qu'il convient à présent d'exposer.

§ 2 - Le phénomène de normalisation technico-managériale

401. La normalisation : éléments de définition socio-historique. Le phénomène de normalisation pourrait être abordé par son étude historique mais, comme le rappelle Monsieur Frydman, l'entreprise est impossible car cette histoire « *n'est rien d'autre que celle de la culture elle-même* »[1994]. En normalisant le langage, l'écriture, le temps et l'espace, l'humanité a procédé à « *une forme de quadrillage du monde et des êtres, animés ou non, une forme de langage commun et de soubassement nécessaire aux normes techniques et managériales* »[1995]. La normalisation consiste donc, en premier lieu, à permettre une forme de communication, les ordres de mesure en sont un exemple primaire. L'essor de la normalisation technique correspond à celui des techniques elles-mêmes et se précise avec l'intensification des échanges internationaux[1996]. L'industrialisation a joué un rôle central dans son institutionnalisation. En effet, la norme technique a longtemps consisté en une « *technique par laquelle l'ingénieur s'adresse à d'autres ingénieurs ou aux chefs d'ateliers qui dirigent la fabrication des produits et le fonctionnement des machines* »[1997]. Puis, l'émergence de la société

[1994] B. FRYDMAN, « Prendre les standards et les indicateurs au sérieux », *in* B. FRYDMAN et A. VAN WAEYENBERGE (ss. la dir.), *Gouverner par les standards et les indicateurs : De Hume au rankings*, coll. Penser le droit, Bruylant, 2013 p. 14 ; dans le même sens v. « *Dès la préhistoire l'homme a moulé son activité dans des normes, que ce soit pour le vêtir, construire des habitations au sol ou sur pilotis, ou bien encore pour cultiver la terre. Les vestiges des armes et des outils découverts au cours des fouilles suffisent aujourd'hui à préciser une époque. Les dimensions, poids, matériaux employés répondent très tôt à des règles d'aptitude à l'emploi* » (F. CAUPERT, *La normalisation*, th. dact., Montpellier I, 1977, p. 4) ; « *La normalisation est aussi vieille que l'hominisation, voire l'a précédé. Les êtres humains ont toujours eu besoin de sélectionner les meilleurs outils et leurs meilleurs processus de production* » (J.-M. BORDE, A. VAUCELLE et H. HUDRISIER, « La normalisation : dynamique opaque ou bonne gouvernance », *Pensée plurielle* 2014, n° 36, p. 9, spéc. p.10) ; *Adde* A. TURINETTI, *La normalisation. Etude en droit économique*, Préf. A. PENNEAU, coll. Droit civil et procédures, Connaissances et Savoirs, 2018, p. 17.

[1995] *Ibid.* p. 15.

[1996] « (…) *au milieu du XIX^e siècle, en fait avec la première phase d'une mondialisation véritablement globale, il est apparu indispensable d'élargir, de systématiser et d'institutionnaliser à des niveaux nationaux, puis mondiaux la normalisation* stricto sensu » (J.-M. BORDE, A. VAUCELLE et H. HUDRISIER, « La normalisation : dynamique opaque ou bonne gouvernance », *op. cit.*, p. 9, spéc. p.10).

[1997] B. FRYDMAN, « Prendre les standards et les indicateurs au sérieux », *op. cit.*, p. 18.

industrielle faisant naître une société du risque[1998], ces normes n'ont plus seulement été destinées aux fabricants mais ont également permis au public d'être informé sur la qualité d'un produit et de sa conformité à un « label ». Ce dernier a précisément été perçu comme le tournant de l'institutionnalisation de la normalisation : « *Le label est bien plus que le signe extérieur de la norme. Il est la pointe émergée, mais aussi le point d'ancrage d'un dispositif complexe qui tend à intégrer dans une filière unique ou cohérente plusieurs techniques opérant à différents stades de la normalisation* »[1999]. C'est ainsi « *l'ensemble d'une chaîne de confiance* […] *qui se met en place* »[2000], formule importante sur laquelle nous reviendrons. Si l'on évoque l'histoire de la normalisation au travers de celles des normes techniques, son sens général rappelle qu'il ne s'agit pas uniquement d'un phénomène technique. La normalisation consistant en l'action « *de rendre normal, conforme à une norme, à un modèle* »[2001], elle s'applique également aux individus et à leurs comportements. La normalisation est alors rapprochée de *normal*[2002] et, sous la plume de Michel Foucault, elle est conçue par opposition au droit, et se rapproche ainsi de la discipline en ce qu'il est question de « *nouveaux procédés de pouvoir qui fonctionnent non pas au droit mais à la technique, non pas à la loi mais à la normalisation, non pas au châtiment mais au contrôle, et qui s'exercent à des niveaux et dans des formes qui débordent l'Etat et ses appareils* »[2003]. Comme le rappelle encore Monsieur Frydman, l'histoire de la normalisation – ou standardisation technique – est intimement liée à celle des normes de gestion ou managériales[2004]. L'auteur explique ainsi comment les normes managériales à l'époque moderne se sont *déplacées* à différents niveaux de la société : des lieux d'enfermement étudiés par Michel Foucault aux lieux de production[2005], de l'entreprise à l'administration[2006] jusqu'à l'ensemble de la vie sociale, « *à l'air libre* »[2007]. La normalisation revêt ainsi deux sens

---

[1998] U. BECK, *La société du risque. Sur la voie d'une autre modernité*, Aubier, 2001.
[1999] B. FRYDMAN, « Prendre les standards et les indicateurs au sérieux », *op. cit.*, p. 18
[2000] *Ibid.*
[2001] G. PARNET et A. SUPIOT, *V°* « Normalisation », *Dictionnaire encyclopédique de théorie et de sociologie du droit*, *op. cit*.
[2002] G. CANGUILHEM, *Le normal et le pathologique*, PUF, 1975.
[2003] M. FOUCAULT, *Histoire de la sexualité*, t. 1, La *volonté de savoir*, Gallimard, 1976, p. 118.
[2004] Pour une synthèse historique, v. B. FRYDMAN, « Prendre les standards et les indicateurs au sérieux », *op. cit*, pp. 25-32.
[2005] *Ibid.,* pp. 26-30.
[2006] *Ibid.*
[2007] G. DELEUZE, « Qu'est-ce qu'un dispositif ? », *in* Association pour le Centre Michel Foucault, *Michel Foucault philosophe, rencontre internationale*, Seuil, 1989, pp. 185-195.

historiquement et sociologiquement liés, tenant tantôt à une filiation avec le terme de *norme*, tantôt avec celui de *normal*. Il faut, à présent, s'intéresser plus spécifiquement à la normalisation technico-managériale.

402. Eléments de définition de la normalisation technique et managériale. Evolution des techniques et mondialisation des échanges ont donc contribué à l'extension du phénomène de normalisation technico-managériale. Selon la définition généralement admise, la normalisation est un « *dispositif cognitif collectif qui rend disponibles et met en circulation, sous forme codifiée et transférable, des savoirs et des moyens d'action, et contribue à la coordination de l'organisation industrielle* »[2008]. Les normes qui en sont issues sont « *la manifestation écrite du résultat d'un choix collectif raisonné en vue de servir de base d'entente pour la solution de problèmes répétitifs* »[2009] ou, selon la définition de *l'International Organization for Standardization* (ISO), un « *document établi par consensus, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné* »[2010]. A partir du milieu du XX[e] siècle, les organismes de normalisation et leurs activités vont être progressivement saisis par le droit tant au niveau national qu'au niveau européen[2011]. En France, la normalisation est définie par décret comme une « *activité d'intérêt général qui a pour objet de fournir des documents de référence élaborés de manière consensuelle par toutes les parties intéressées, portant sur des règles, des caractéristiques, des recommandations ou des exemples de bonnes pratiques, relatives à des produits, à des services, à des méthodes, à des processus ou à des organisations* »[2012]. Cette définition ne confine pas la normalisation à la seule production de normes techniques[2013]. De plus, si le décret fixe les missions d'intérêt public de l'Association française de normalisation (AFNOR), le rôle de celle-ci ne consiste pas seulement

---

[2008] Cette définition est formulée par Monsieur Van Waeyenberge (A. VAN WAEYENBERGE, « Les normes ISO, CEN et celles issues des consortiums privés : bric à brac ou système pour l'Union européenne », *in* B. FRYDMAN et A. VAN WAEYENBERGE, *Gouverner par les standards et les indicateurs : De Hume aux rankings*, *op.cit.*, p. 93) à partir des critères dégagés par Madame Benezech à l'occasion d'un article de référence sur la question : D. BENEZECH, « La norme : une convention structurant les interrelations technologiques et industrielles », *Revue d'économie industrielle* 1996, n° 75, p. 27 et svt.
[2009] *Ibid.* p. 27.
[2010] <https://www.iso.org/sites/ConsumersStandards/fr/1_standards.html>
[2011] Loi n° 41-1987 du 24 mai 1941 relative à la normalisation et Décret n° 84-1988 du 24 mai 1941 définissant le statut de la normalisation, *JORF*, 28 mai 1941, p. 2219.
[2012] Il s'agit de fixer le statut de la normalisation : Art. 1[er] du Décret n° 2009-697 du 16 juin 2009 relatif à la normalisation, *JORF* n° 0138.
[2013] A. PENNEAU et D. VOINOT, *JCl Concurrence – Consommation,* fasc. 970 : Normalisation, oct. 2010, n° 19.

à agir dans le cadre de cette délégation, elle a également des activités de normalisation *privée*. Au travers des définitions évoquées, plusieurs critères propres à la normalisation se retrouvent : il s'agit d'une activité non strictement technique ce que nous avons expliqué par ailleurs en utilisant le terme, employé par Monsieur Frydman, de normes technico-managériale[2014] ; l'activité de normalisation consiste, ensuite, en la production de « *documents de référence* » qui peuvent prendre des formes diverses[2015], l'essentiel étant que « l'instrumentum *véhicule un modèle de conduite technique, sociale, sociétale* »[2016] ; enfin l'activité de normalisation est négociée et collective.

403. Les acteurs de la normalisation technico-managériale. Il nous est impossible de faire une liste exhaustive des organismes de normalisation. Il convient de remarquer que certains sont institutionnalisés au niveau national tel que l'AFNOR, tandis qu'il existe des normalisateurs européens. Au premier niveau se trouvent les organismes nationaux de normalisation (ONM) tandis qu'à un second niveau se trouve le Comité européen de normalisation (CEN), le Comité européen de normalisation électronique (CENELEC) ou encore l'Institut européen des normes de télécommunication (ETSI)[2017]. Outre ces organismes institutionnalisés au plan national et européen, il existe de nombreux organismes privés de normalisation dont le principal et le plus influent est l'Organsation internationale de normalisation (ISO)[2018]. Celle-ci travaille en collaboration avec deux autres organismes : la

---

[2014] Ainsi que l'explique l'auteur, l'hybridation des normes de gestion et des normes techniques, la montée en puissance des premières (le souci croissant de l'efficacité de la production et de la qualité des produits) et la libération des secondes hors des institutions *normalisantes*, en font des « *concurrents directs et sérieux des règles juridiques et des institutions politiques issues de la Modernité* » (B. FRYDMAN, « Prendre les standards et les indicateurs au sérieux », *in* B. FRYDMAN et A. VAN WAEYENBERGE, *Gouverner par les standards et les indicateurs : De Hume aux rankings*, *op. cit.*, p. 32).

[2015] « *Le propre des documents référents est de proposer, à ceux qui sont appelés à s'en servir, des outils, des méthodes, des repères mais abec des finalités différentes selon que le document peut être qualifié d'anticipatif, de prescriptif ou de descriptif* » (P. SABLIERE, « Une nouvelle source de droit ? Les « documents référents » », *AJDA* 2007, p. 66).

[2016] A. TURINETTI, *La normalisation. Etude en droit économique*, coll. Droit civil et procédures, Editions Connaissances et Savoirs, 2018, n° 13.

[2017] A. VAN WAEYENBERGE, « Les normes ISO, CEN et celles issues des consortiums privés : bric à brac ou système pour l'Union européenne ? », *Gouverner par les standards et les indicateurs : De Hume aux rankings*, *op.cit.*, p. 93, *spéc.* p. 100.

[2018] Sur la normalisation internationale et les enjeux politique sous-jacents (qui implique également d'admettre que la normalisation technique n'est pas uniquement technique) v. J.-C. GRAZ, « Quand les normes font loi : Topologie intégrée et processus différenciés de la normalisation internationale », *Etudes internationales* 2004, n° 2, vol. 35, Pp. 233-260 ; « […] *l'élaboration des normes est assurée par les parties prenantes intéressées, notamment les industriels, au sein de commissions de normalisation* ». Pour un panorama sur la production des

Commission électronique internationale (CEI) et l'Union internationale des télécommunications[2019]. La première intéresse particulièrement notre domaine de recherche. Nous aurons l'occasion de revenir sur le rôle de ces acteurs. L'important, à ce stade, est de concevoir qu'au-delà de leur disparité, les liens entre organismes de normalisation institutionnalisés (au niveau national, européen et international) et privés sont étroits. Il suffit, pour s'en convaincre, de mentionner le fait que les membres des organismes nationaux et européens sont *également* membres de l'ISO[2020], les producteurs privés des normes techniques pouvant aussi être appelés à devenir, pour des besoins précis, des « *producteurs officiels* » des normes européennes[2021]. Les liens entre ces organismes forment un maillage, un réseau entre les normalisateurs nationaux, européens et internationaux, d'une part, et les organismes issus de consortiums privés, d'autre part[2022].

404. Normalisation, théorie du droit et méthodologie juridique. Une fois rappelé l'existence d'autres dispositifs normatifs que les règles de droit et leur enchevêtrement, avoir précisé ce qu'était la normalisation technico-managériale, il manque encore des repères méthodologiques pour traiter spécifiquement de ce qui nous occupe et espérer en tirer un quelconque enseignement. En raison de la nature des normes techniques et managériales, les juristes ont, nous l'avons dit, relativement peu investi ce champ d'étude. Nos méthodes traditionnelles conduisent, en, effet, à leur reconnaître un intérêt limité pour l'étude du droit en raison de leur absence de juridicité[2023]. Lorsqu'elles sont étudiées, c'est principalement pour questionner leur potentielle juridicité ou leur intégration à l'ordre juridique[2024], ou encore pour observer la place qui leur est donnée dans l'ordre juridique[2025]. Ces normes demeurent ainsi « *le parent pauvre du champ de la théorie du droit. Comme s'il n'y avait rien ou si peu à en*

---

normes techniques et la diversité des organismes nationaux et internationaux v. par exemple : V. GIARD, « La normalisation technique », *Revue française de gestion* 2003/6, n° 147, p. 49.

[2019] *Ibid*. p. 65.

[2020] A. VAN WAEYENBERGE, « Les normes ISO, CEN et celles issues des consortiums privés : bric à brac ou système pour l'Union européenne ? », *Gouverner par les standards et les indicateurs : De Hume aux rankings*, *op. cit.*, p. 100.

[2021] *Ibid.,* p. 105.

[2022] Pour une réflexion complète sur ce « système » dans l'ordre européen v. *Ibid.*

[2023] Dès lors qu'il s'agit de ne penser les normes qu'au travers des ordres normatifs

[2024] L. BOY, « Normes techniques et normes juridiques », *in* La normativité, *Cahiers du Conseil Constitutionnel*, Janvier 2007.

[2025] V. par ex. L. BOY, « Liens entre la norme technique et la norme juridique en droit communautaire et international, *in* E. BROSSET et E. TRUILHE-MARENGO (ss. la dir.), *Les enjeux de la normalisation technique internationale. Entre environnement, santé et commerce international*, La documentation française, 2006.

dire, compte tenu de leur caractère purement technique (entendez dénué d'enjeu politique) et de leur position infiniment modeste dans l'échelle des normativités »[2026]. Constatant la multiplication des dispositifs normatifs difficilement identifiables, certains juristes se sont engagés dans la voie de leur étude en acceptant de sortir du seul champ de la juridicité pour réflechir les normes dans le vaste champ de la normativité. De nouveaux outils méthodologiques ont donc été proposés, et de nouvelles pistes de réflexion *sur* le droit ont été dégagées : en France, l'on citera les travaux de Madame Thibierge, tandis qu'en Belgique, les travaux les plus notables sont ceux du Centre Perelman de philosophie du droit, qui ont développé le concept de *droit global*[2027].

405. L'approche pragmatique et la théorie du droit global. Parmi les chantiers de réflexion initiés par le programme *droit global* du Centre Perelman de philosophie du droit figure l'étude consacrée à « *l'émergence de nouvelles formes de régulation dans différents secteurs* »[2028], comprenant les normes techniques et managériales. Des recherches sectorielles ont été menées sur ces transformations et ont fait émerger la théorie du *droit global*. Comme l'explique Monsieur Frydman, c'est au travers de l'approche pragmatique issue de la pensée de l'Ecole de Bruxelles[2029] qu'ont été étudiés ces « *dispositifs multiples et hétéroclites, qui prolifèrent, de manière souvent anarchique, dans les domaines les plus mondialisés »* et qui « *mettent au défi l'entendement des juristes, de par l'extraordinaire diversité de leurs origines, de leurs formes ou de leurs effets et l'apparent arbitraire de leur agencement et de leurs combinaisons* »[2030]. S'il explique que le pluralisme juridique a été mobilisé comme une méthode pour réfléchir ces dispositifs dans leurs rapports avec les règles juridiques[2031], il

---

[2026] L. BOY, « Normes techniques et normes juridiques », *op. cit.*
[2027] V. not. B. FRYDMAN, *Petit manuel du droit global*, série « L'économie de marché est-elle *juste ?* » vol. 4, coll. L'Académie en poche, Académie Royale de Belgique, 2014 ; C. BRICTEUX et B. FRYDMAN (dir.), *Les défis du droit global*, coll. penser le droit, Bruylant, 2017.
[2028] B. FRYDMAN, « Comment penser le droit global », *in* J.-Y. CHEROT et B. FRYDMAN, *La science du droit dans la globalisation*, coll. pense
[2029] Ecole de pensée issue de l'Université libre de Bruxelles, ayant regroupé des théoriciens tels que Chaïm Perelman, Paul Foriers, Henri Buch et René Dekkers. Le pragmatisme propre à l'Ecole de Bruxelles à ceci de particulier qu'il exclut « *toute conception a priori du droit sous la forme d'un système logique de normes ou d'un ordre déterminé* » (G. LEWKOWICZ et A. VAN WAEYENBERGE, « L'École de Bruxelles : origines, méthodes et chantiers », *in La méthodologie et l'épistémologie juridiques*, Éditions Yvon Blais, 2016, pp. 363-372).
[2030] B. FRYDMAN, « Comment penser le droit global », *in* J.-Y. CHERIOT et B. FRYDMAN, *La science du droit dans la globalisation*, coll. penser le droit, Bruylant, p. 18.
[2031] Notamment par Jean Carbonnier et Madame Delmas-Marty (*Ibid.*, p. 23).

considère que l'option méthodologique la plus adéquate consiste à se « *passer purement et simplement du concept d'ordre juridique pour envisager immédiatement les normes et les interactions juridiques entre les acteurs en tant que telles, indépendamment du ou des ordres dans lesquels elles s'inscrivent ou non* »[2032]. Analysant les approches qui mobilisent le pluralisme juridique et tentant d'étudier les rapports entre normes techniques et règles juridiques de la même façon que l'on essaie de « *coordonner les relations des différents ordres juridiques entre eux* »[2033], il évoque les différentes thèses des auteurs ayant pensé les rapports entre les ordres juridiques et normatifs, notamment celles qui conçoivent le droit comme un médiateur, un coordinateur de ces différents systèmes[2034]. Il relève à ce titre que cette façon d'envisager les rapports entre les formes alternatives de normativité et le droit est « *caractéristique de la pensée juridique moderne, spécialement continentale, qui présente le droit sous le paradigme de l'ordre juridique, apparaît cependant à la fois massive et très exigeante quant aux conditions à réunir pour aménager les relations entre le droit et les normes techniques* »[2035]. L'approche pragmatique du *droit global* consiste au contraire à « *envisager immédiatement les normes et les interactions juridiques entre les acteurs en tant que telles, indépendamment du ou des ordres dans lesquels elles s'inscrivent ou non* »[2036]. Ce choix provoque nécessairement une nouvelle réflexion *sur* le droit : pourrait s'ébaucher une théorie du droit global qui « *ne reposera ni sur un inventaire exhaustif de ses sources, ni sur la construction d'un ordre cohérent et complet, mais bien sur la description d'un nombre fini d'éléments simples, dont les combinaisons permettraient de rendre compte de la multiplicité des agencements apparemment anarchique, incohérents et arbitraires que la réalité place*

[2032] *Ibid,*. p. 23.
[2033] B. FRYDMAN, « Prendre les standards et les indicateurs au sérieux », *in* B. FRYDMAN et A. VAN WAEYENBERGE (ss. la dir.), *Gouverner par les standards et les indicateurs : du Hume aux rankings*, *op. cit.*, p. 62 ; Cette coordination des ordres juridiques renvoie notamment au cours de Madame Delmas-Marty donné au Collège de France et qui a fait l'objet d'un ouvrage de référence : M. DELMAS-MARTY, *Les forces imaginantes du droit. Le pluralisme ordonné*, t. II, Seuil, 2006.
[2034] B. FRYDMAN, « Prendre les standards et les indicateurs au sérieux », *in* B. FRYDMAN et A. VAN WAEYENBERGE (ss. la dir.), *Gouverner par les standards et les indicateurs : du Hume aux rankings*, *op.cit.*, pp. 59-61.
[2035] B. FRYDMAN, « « Prendre les standards et les indicateurs au sérieux », *in* B. FRYDMAN et A. VAN WAEYENBERGE (ss. la dir.), *Gouverner par les standards et les indicateurs : du Hume aux rankings*, *op.cit.*, p. 62.
[2036] B. FRYDMAN, « Comment penser le droit global », *in* J. -Y. CHEROT et B. FRYDMAN, *La science du droit dans la globalisation*, *op. cit.*, p. 23.

devant nos yeux »[2037]. Aussi le juriste doit-il « *s'émanciper d'une conception par trop étroite, formelle et rigide de la juridicité, afin de porter son regard, son intérêt et ses études dans le champ plus vaste de la normativité, dans toute la diversité de ses formes et de ses techniques* »[2038]. Sans adopter pleinement la vision des chercheurs de l'Ecole de Bruxelles ni prétendre adopter la méthode pragmatique nécessaire à une reflexion sur le *droit global* – par essence pluridisciplinaire alors que nous ne sommes que juriste –, nous les rejoignons dans leur ambition de ne pas laisser hors du champ d'étude la question des normes techniques et managériales. L'analyse de ces normes est tout à fait pertinente, particulièrement dans l'étude de la protection des données de santé, comme nous allons le montrer. Notre choix de prendre en compte des normes techniques et managériales ne doit, toutefois, pas être compris comme une prise de position quant à la juridicité de ces objets normatifs.

Section 2 - L'utilisation de normes étrangères au droit dans la mise en œuvre de la confidentialité

406. Garanties des secrets protégés par la loi. Si la CNIL a toujours veillé à la mise œuvre des mesures de sécurité les plus abouties pour préserver la confidentialité, c'est d'abord en vertu

---

[2037] B. FRYDMAN, « Prendre les standards et les indicateurs au sérieux », *in* B. FRYDMAN et A. VAN WAEYENBERGE (ss. la dir.), *Gouverner par les standards et les indicateurs : du Hume aux rankings*, *op.cit.*, p. 65.

[2038] En France, le constat d'une densification normative (C. THIBIERGE *et alii*, *La densification normative. Découverte d'un processus*, Mare&Martin, 2015) et de la diversité des formes de normativités a donné lieu à des recherches menées sous la direction de Madame Thibierge. Constatant la diversité des normes dont la juridicité est incertaine, la démarche de l'auteur est avant tout de proposer un outil, une méthode qui s'inscrit dans une *théorie ouverte du droit*. Il s'agit donc de ne plus penser les normes en termes de juridicité, c'est-à-dire au regard des critères juridiques, mais de les analyser au regard de leur force normative. Le concept de force normative, né des recherches produites par un collectif d'auteurs est donc conçu comme un outil qui permet de graduer la normativité. La question posée à chacun des auteurs appelés à participer aux travaux était « *qu'est-ce qui, en droit, fait la force d'une norme ?* » (C. THIBIERGE, « Le concept de « force normative » », *in* C. THIBIERGE *et alii*, La *force normative. Naissance d'un concept*, Mare&Martin, 2013, p. p. 813 s., spéc. p. 816). C'est à partir des réponses apportées, dans des branches du droit différentes et parfois sur des sujets spécifiques, que Madame Thibierge a forgé le concept de force normative. Elle identifie trois pôles, qui constituent les marqueurs de la force normative : la valeur normative, qui permet de déterminer la « *force conférée à la norme par son émetteur* » (*Ibid.*, p. 822) ; la portée normative, c'est-à-dire la manière dont la norme est reçue par les destinataires, son effectivité (*Ibid.*) ; enfin, la garantie normative attachée à la norme par le système juridique et qui garantit son respect (*Ibid.*). Chaque pôle se rattache à la *source* de la norme, à ses *effets* et à son *respect* (*Ibid.,* p. 823). Il est alors possible de concevoir qu'il existe des distorsions entre les différents pôles, et par exemple qu'une norme émanant d'une autorité légitime n'a qu'une effectivité limitée. A l'inverse, certains dispositifs normatifs peuvent avoir une effectivité importante tout en émanant d'autorités consultatives ou d'organismes privés.

de l'article 33 de la LIL, disposant que, pour les traitements automatisés de données à caractère personnel, les demandes d'avis, lorsqu'elles sont nécessaires, doivent mentionner les mesures prises pour « *assurer la sécurité des traitements et des informations et la garantie des secrets protégés par la loi* »[2039]. Au titre des secrets protégés par la loi figure évidemment le « secret médical ». Or il ne s'agissait pas, pour la commission, de donner un avis sur l'affaiblissement de la norme sanctionnant l'atteinte au secret professionnel mais d'évaluer la protection du *secret des données* issues de la prise en charge des personnes par un professionnel intervenant dans le système de santé.

Aussi, le contrôle de la CNIL avant la mise en œuvre du traitement permettait de vérifier les mécanismes de *sécurité technique* assurant la confidentialité. Selon ses propres propos, « *elle veille à ce que les mesures de sécurité prises garantissent la confidentialité des données traitées* […] *et qui sont couvertes par le secret professionnel* »[2040]. La confidentialité doit désormais être assurée *ex-ante*, dans une logique de co-régulation qui se réalise, du coté de l'autorégulation, par la *compliance* et *l'accountability*. La CNIL veille donc de moins en moins à la mise en œuvre de ces mesures en amont du traitement, c'est au responsable de traitement et au sous-traitant de prendre les mesures appropriées et de le démontrer[2041]. La *compliance* est ainsi particulièrement propice à la montée en puissance des normes techniques[2042], et ce mouvement et encore plus visible en raison de la pratique de la *privacy by design* qui guide désormais la protection des données à caractère personnel et le cadre européen sur la

---

[2039] Ancien art. 17 LIL, devenu art. 19 par le décret n° 95-682 du 9 mai 1995 pris pour l'application du chapitre V bis de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et modifiant le décret n° 78774 du 17 juillet 1978.

[2040] CNIL, *Rapport d'activité* 1982-1983, p. 180.

[2041] C'est la logique du *comply or explain* qui signifie littéralement : « se conformer ou expliquer » v. P. DEUMIER, Le principe « appliquer ou expliquer », appliquer la norme autrement ? », *RTD civ.* 2013, p. 79.

[2042] Comme l'explique un auteur proposant une analyse de la *compliance* des entreprises : « *La compliance ne table plus seulement sur le face-à-face vertical de l'entreprise et de la loi, mais également sur l'aménagement d'un milieu horizontal au sein même de l'entreprise qui puisse faire diminuer tendanciellement le risque d'infraction aux règles* » (A. GAUDEMET, « Qu'est-ce que la compliance », *Commentaires* 2019/1, n° 165, P. 109, *spéc.* p 110). Diminuer le risque d'infractions aux règles est le propre de la compliance si l'on admet qu'il s'agit de « *l'ensemble des processus qui permettent d'assurer la conformité des comportements de l'entreprise, de ses dirigeants et de ses salaries aux normes juridiques et éthiques qui leur sont applicables* » (*Ibid.*). L'auteur explique ainsi que la caractéristique de la compliance est d'inciter les acteurs à mettre en œuvre des techniques préventives. Il souligne que « *l'ensemble de ces techniques a pour objectif d'amener les entreprises les plus importantes à assurer elles-mêmes, en leur sein et à leurs frais, le contrôle des règles qui leur sont applicables, à internaliser le contrôle de ces règles* » (*Ibid.* p. 111). Il s'agit en outre *d'organiser* la compliance au sein de la structure concernée. Les normes techniques et managériales constituent, nous le verrons, des outils essentiels pour assurer le contrôle des dispositions relatives à la protection des données à caractère personnel.

cybercriminalité **(paragraphe 1)**. Ensuite, la mise en œuvre de la sécurité et de la confidentialité consiste dans le fait de s'assurer de l'identité des personnes **accédant** aux données. La sécurité des **échanges** autant que la sécurité des **systèmes** doivent donc être garanties[2043] *en amont*. A l'échelle nationale, la sécurité et la confidentialité des échanges et des systèmes conditionnent également le *virage numérique* de la santé, et à l'échelle européenne, elles conditionnent le marché unique des données de santé. La *soft law* et les normes techniques et managériales se présentent, non seulement comme les instruments adaptés de la *compliance* mais également comme des outils des politiques publiques à chacun de ces niveaux **(paragraphe 2)**.

§ 1 - La *privacy by design* et la cybersécurité : des domaines de prédilection de la normalisation

407. Afin de mieux saisir le processus de normalisation à l'œuvre au travers du principe de *Privacy by design* et du domaine de la cybersécurité il nous faut préciser le lien entre ce processus et les moyens techniques **(A)** et organisationnels **(B)**.

A - Des moyens techniques normalisés

408. La cybersécurité **(1)** et la *Privacy by design* **(2)** sont des domaines dans lesquels la normalisation connaît une inflation importante.

1 - Les moyens techniques de la cybersécurité

409. Le règlement européen relatif à la cybersécurité est une manifestation visible de la place grandissante qu'occupe la normalisation **(a)**. La cybersécurité étant une forme de secret « moyen », il nous faut approcher la notion, dans la limite de ce que nous permettent nos connaissances **(b)**.

[2043] Dans le même sens mais évoquant plus généralement le téléservice public, v. L. CLUZEL-METAYER, « Les téléservices publics face au droit à la confidentialité des données », *RFAP* 2013/2, n° 146, pp. 405-418.

a - Le rôle de la cybersécurité

410. Les mesures techniques et la cybercriminalité. Le RGPD a renouvelé l'approche de la sécurité et de la confidentialité en matière de traitement des données à caractère personnel. En développant les obligations de sécurité et de confidentialité, nous avons montré que la sécurité était un préalable à la confidentialité et que le couple sécurité/confidentialité constituait une obligation générale pesant sur le responsable de traitement et le sous-traitant[2044]. Nous avons par ailleurs expliqué que la confidentialité des traitements pouvait, en partie, être assurée par le secret professionnel et d'autres mécanismes juridiques de réservation de l'information. Il convient d'ajouter qu'assurer la confidentialité *ex-ante* consiste à prendre des mesures de sécurité *techniques et organisationnelles* appropriées[2045]. Supposant, en partie, de protéger *le secret des données couvertes par le secret professionnel*, la confidentialité est ainsi mise en œuvre par ces mesures de sécurité[2046]. L'article 32 du RGPD fournit quelques exemples de mesures, telles que la pseudonymisation et le chiffrement. Surtout, le règlement impose désormais au responsable de traitement de déterminer, avant la mise en œuvre du traitement, « *la probabilité et la gravité du risque pour les droits et libertés de la personne concernée* »[2047]. Il précise également comment est calculé le degré de probabilité et de gravité des risques : il varie en fonction des dommages physiques, matériels, ou du préjudice moral que pourrait entraîner le traitement, et notamment en cas de « *perte de confidentialité de données protégées par le secret professionnel* »[2048] ou lorsque le traitement « *concerne des données à caractère*

[2044] La sécurité ne recouvre pas uniquement la confidentialité des données mais également l'intégrité et la disponibilité des données (RGPD, art. 5 f)), lesquelles peuvent être de nature à engendrer un préjudice non seulement moral mais également physique pour les personnes concernées par le traitement (des données de santé indisponibles ou dont l'intégrité est atteinte peuvent par exemple engendrer un retard de prise en charge où des erreurs dans la détermination des traitements à mettre en œuvre et provoquer, par exemple, l'administration de médicaments contre-indiqués).

[2045] Obligation générale du responsable de traitement et du sous-traitant (art. 24) précisée à l'article 34 du RGPD : « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ». Selon Monsieur Douville, *la mise en place de mesures techniques et organisationnelles* est un des principes du droit commun – émergent – de la cybersécurité (T. DOUVILLE, « L'émergence d'un droit commun de la cybersécurité », *D.* 2017, p. 2255) sur lequel nous reviendrons.

[2046] La sécurité permet également d'assurer « *l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* » (RGPD, art. 34 1 b)).

[2047] RGPD, consid. 76.

[2048] RGPD, consid. 75.

personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle […] » [2049]. Le règlement européen énonce encore que l'évaluation des risques incombe, dans une logique de responsabilisation, aux responsables de traitement ainsi qu'aux sous-traitants. Lorsque le ou les traitements mis en œuvre présentent des risques élevés, le responsable de traitement doit effectuer une analyse d'impact. Celle-ci permet de déterminer « *les mesures appropriées* » mais permet surtout au responsable du traitement de pouvoir démontrer[2050] que les mesures qu'il a prises pour assurer la sécurité sont adaptées au risque. La mise en place de ces mesures participe donc de la cybersécurité, qui désigne : « *les usages défensifs et offensifs de ces systèmes d'information qui irriguent désormais nos organisations modernes. Elle prend en compte les contenants, c'est-à-dire les moyens techniques (réseaux informatiques, téléphoniques, satellitaires…) utilisés pour l'échange de données, qui peuvent faire l'objet d'opérations d'infiltration, d'altération, de suspension voire d'interruption, comme les contenus, c'est-à-dire l'ensemble des informations qui circulent ou sont stockées sur des supports numériques (informatique industrielle, site Internet, bases de données, messageries et communications électroniques, transactions dématérialisées…)* »[2051]. Outre la protection des systèmes, la cybersécurité vise également à garantir la confidentialité, l'intégrité et la disponibilité des données qui peuvent être compromises par des atteintes extérieures. « *La sécurité des données et des services, dans le cyberespace, est devenue grâce au RGPD, le dénominateur commun de tous les projets numériques européens* »[2052], un règlement européen est récemment venu confirmer l'emergence d'un cadre commun de la cybersécurité au sein de l'Union européenne.

[2049] *Ibid.*
[2050] La logique d'*accountability* impose que le responsable du traitement et le sous-traitant soient en mesure de démontrer, en cas de contrôle de la CNIL, qu'ils mettent en œuvre les mesures de sécurité adéquates.
[2051] N. ARPAGIAN, *La cybersécurité*, coll. Que sais-je ? PUF, 2018, p. 9-10 ; pour quelques exemples issus du RGPD (que nous avons ou allons évoquer) : A. JOMNI, « Le RGPD : un atout ou un frein pour la cybersécurité ? », *Dalloz IP/IT* 2019, p. 352.
[2052] A. JOMNI, « Le RGPD : un atout ou un frein pour la cybersécurité ? », *Dalloz IP/IT* 2019, p. 352.

b - Le règlement européen, marqueur de la normalisation

411. La cybersécurité et la protection des données couvertes par le secret. Le discours de la doctrine porte majoritairement sur les risques que l'utilisation des outils fait courir au « secret médical »[2053]. L'expression est utilisée, nous l'avons dit, pour viser tantôt la violation du secret professionnel par le biais des outils, tantôt le secret des données issues de la prise en charge des personnes par un professionnel intervenant dans le système de santé. La confidentialité, au sens technique, consiste ainsi dans le fait de s'assurer que les informations ne sont accessibles qu'aux personnes autorisées[2054] tandis que les dispositions du Code de la santé publique désignent les personnes autorisées. Aussi, toujours au sens technique, la confidentialité désigne un processus par lequel l'information, les données, sont gardées secrètes, qu'il s'agisse d'empêcher les révélations ou les accès illicites. Les dispositifs techniques permettent, entre autres, de s'assurer de l'identité des personnes accédant aux données, ce qui relève autant de la sécurité des échanges que de la sécurité des systèmes. Ainsi, la cybersécurité, dont la vocation est de prévenir les attaques sur des systèmes et dispositifs techniques, ne vise pas, en premier lieu, à protéger la vie privée des individus dont les données sont traitées mais à empêcher la paralysie des activités qui utilisent les dispositifs techniques de l'information et de la communication. Certaines cyberattaques n'ont pas pour but de prendre connaissance des informations mais d'empêcher le fonctionnement normal d'une activité. Dans le secteur de la santé, les cyberattaques sont régulières et consistent parfois à demander une

---

[2053] Evoquant par exemple les risques pour le *secret médical* et traitant des « *indiscrétions* », des risques « *d'intrusion délictuelle* » : F. STEFANI, « Le secret médical à l'épreuve des nouvelles technologies », *D.* 2009, p. 2636 ; utilisant l'expression *secret médical* pour traiter des risques d' « accès illégal à l'information médical » : D. TABUTEAU, « Le secret médical et l'évolution du système de santé », *D.* 2009, p. 2629 ; soulignant l'*inviolabilité du secret médical* dans un développement consacré à la cybersécurité : P. DE ROUGE MAISON, « Décryptage sur la protection juridique des informations sensibles », *Dalloz IP/IT* 2017, p. 273.

[2054] « *La confidentialité est un objectif de sécurité permettant de protéger l'information au repos et lors de son échange contre toute divulgation et accès non autorisés. La confidentialité doit être assurée techniquement (mécanisme de chiffrement et de contrôle d'accès) et non techniquement (classification des informations et mise en place de politiques de contrôle d'accès) afin de ne donner l'accès qu'à ceux qui sont autorisés. Cet objectif peut porter sur la protection d'un message élémentaire ou d'un champ spécifique à l'intérieur d'un message en recourant aux objectifs support d'authentification et de contrôle d'accès. Les informations peuvent avoir différents niveaux de confidentialité. Si certaines informations n'ont aucune exigence de confidentialité (information publique qui peut être accessible par tout le monde) d'autres informations doivent être plus étroitement contrôlées et partagées uniquement par les partenaires métier, voire pour les plus sensibles n'être accessible que par certaines personnes* » (P. BOU NASSAR, *Gestion de la sécurité dans une infrastructure de services dynamique : Une approche par gestion des risques,* Thèse dact. en informatique et mathématique, Institut National des sciences appliquées de Lyon, 2012, p. 49).

rançon pour rétablir le fonctionnement normal des systèmes ayant subi l'attaque. Ainsi, la cybersécurité a vocation à protéger l'intégralité des systèmes et dispositifs qui traitent, véhiculent, stockent les données[2055], participant incidemment à protéger les données couvertes par le secret. Cette branche de la sécurité est principalement guidée par des normes technico-managériales dont les juristes se sont longtemps désinteressés[2056]. Les champs de la cybersécurité et de la *Privacy by design* se recoupent : l'obligation de sécurité et de confidentialité doit être, au regard de l'article 25 du RGPD portant sur l'obligation générale protection des données, mise en œuvre dès la conception et par défaut.

412. Le règlement européen sur la cybersécurité, mise en œuvre d'un cadre européen de certification[2057]. Le règlement (EU) 2019/881 du 17 avril 2019 relatif à l'Agence de l'Union européenne pour la cybersécurité et à la certification de cybersécurité des technologies de l'information et de la communication prévoit notamment un cadre européen de la certification en matière de cybersécurité[2058]. Ainsi que le remarque Monsieur Douville, la France a, depuis longtemps, mis en œuvre des procédures de certification sectorielles en matière de sécurité des dispositifs techniques et des systèmes d'information[2059]. L'Agence nationale de sécurité des systèmes d'information (ANSSI) est l'autorité nationale de certification de cybersécurité, dans le secteur de la santé elle travaille conjointement avec l'Asip-santé et la CNIL à la certification des produits, service et procédure TIC. Le règlement européen sur la cybersécurité se présente comme la pièce centrale des instruments d'harmonisation de la cybersécurité en Europe. Le second volet du règlement, portant sur le cadre européen de certification, vise la « *mise en place de schémas européens de certification de cybersécurité dans le but de garantir un niveau adéquat de cybersécurité des produits TIC, services TIC et processus TIC* »[2060]. Le règlement

---

[2055] Ce qui correspond à la définition des systèmes d'information.

[2056] C'est un domaine technique à « *expertise forte* » (J. SERRIS et L. TOUTAIN, « Introduction », *in Normaliser le numérique ?*, série Enjeux Numériques, Annales des Mines, mars 2019, n° 5).

[2057] Nous envisagerons ultérieurement les normes techniques issues du cadre de la directive NIS puisque l'effort de normalisation qui en découle est issu d'une coopération étatiques visible au niveau national. V. *infra* n° 455.

[2058] PE et Cons., Règlement (UE) 2019/881, relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013 (règlement sur la cybersécurité), 17 avril 2019, *JOUE* 7 juin 2019, L 151/15. Pour un commentaire de la loi v. notamment T. DOUVILLE, « Le règlement européen sur la cybersécurité », *JCP E* 2019, n° 25, act. 408.

[2059] *Ibid.*

[2060] Règlement (UE) 2019/881, art. 1.

définit dans son deuxième article le *produit TIC* comme un « *élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information* »[2061]. Un *service TIC* est, toujours selon le règlement, un service consistant « *intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information* »[2062]. Enfin, un *processus TIC* est défini comme un « *ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance* ». Le règlement entend donc étendre la certification et définir un schéma commun à tous les pays de l'Union européenne englobant le vaste ensemble des technologies de l'information et de la communication. La certification, comme la labellisation, s'intègre au processus de normalisation, elle est le signe extérieur de la norme technique et la preuve de son respect[2063]. La santé est le premier domaine cité par le règlement et pour lequel ces dispositifs et processus remplissent une fonction essentielle[2064]. Nous verrons que la normalisation croissante des technologies de l'information et de la communication révèle un dessein européen. Pour l'instant, il s'agit simplement de remarquer que le secteur de la santé est l'un des premiers concernés par le processus de normalisation et de certification européenne de la cybersécurité. Comme le constate Monsieur Douville, cette « *exigence de sécurité par défaut et dès la conception des produits, services et processus doit être respectée, les données – à caractère personnel ou non – doivent être protégées contre tout traitement non autorisé et leur confidentialité, leur intégrité et leur disponibilité garantie* »[2065]. Il s'agit donc de consacrer, à côté du principe de *Privacy by design*, un autre, qualifié de ***Security by design***. Ce dernier a vocation à empêcher les attaques qui peuvent potentiellement porter atteinte au secret des données issues de la prise en charge des personnes par un professionnel intervenant dans le système de santé.

2 - Les moyens techniques de la *privacy by design*

[2061] Règlement (UE) 2019/881, art. 2.
[2062] *Ibid.*
[2063] B. FRYDMAN, « Prendre les standards et les indicateurs au sérieux », *in* B. FRYDMAN et A. VAN WAEYENBERGE, *Gouverner par les standards et les indicateurs : de Hume aux rankings*, coll. Penser le droit, Bruylant, 2013, p. 20.
[2064] Cons. 1 du Règlement (UE) 2019/881.
[2065] T. DOUVILLE, « Le règlement européen sur la cybersécurité », *op. cit.*

413. La mise en œuvre de la *Privacy by design* **(b)** doit en partie être assuré par des moyens techniques **(a)**.

a - Le concept de *privacy by design*

414. Du concept à la mise en œuvre. La *privacy by design* est au centre des attentions depuis quelques années[2066] et particulièrement depuis l'entrée en vigueur du RGPD au sein duquel *la protection des données dès la conception* est érigée en *principe*[2067] de la protection des données à caractère personnel. La *privacy by design* consiste en « *une modalité, parmi d'autres, de la régulation de la vie privée dans l'univers numérique* »[2068]. Elle est guidée par sept *principes*[2069].

[2066] L'expression et le concept sont nés en 2009 sous la plume d'un Commissaire canadien à l'information et à la vie privée (A. CAVOUKIAN, *Privacy by Design : The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, 2009, disponible sur : <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> (dernière consultation le 09/07/2019)). La *privacy by design* est alors plutôt pensée comme une philosophie du respect de la vie privée (CNIL, *La forme des choix. Données personnelles, design et frictions désirables*, Cahiers ip innovation & prospective n° 6, janv. 2019, p. 10), et devient un objet de réflexion pour le juriste et également pour les concepteurs des dispositifs techniques (*Ibid.*). Avant d'être ainsi conceptualisée, l'idée d'incorporer la protection des données dans les dispositifs existait déjà, l'on parlait alors de *Privacy Enhancing Technologies* (A. RALLET, F. ROCHELANDET et C. ZOLYNSKI, « De la *privacy by design* à la *Privacy by Using* », *Réseaux* 2015/1, n° 189, p. 15).

[2067] Le considérant 78 du RGPD précise que : « *Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données* ». La définition de la protection des données dès la conception figure parmi les obligations générales incombant au responsable du traitement et au sous-traitant, l'article 25 dispose : « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée* ».

[2068] Ph. PUCHERAL, A. RALLET, F. ROCHELANDET et C. ZOLYNSKI, « La privacy by design : une fausse bonne solution aux problèmes de protection des données personnelles soulevés par l'open data et les objets connectés ? », *Légicom* 2016/1, n° 56, p. 89.

[2069] Ces sept principes sont présentés comme suit : 1° *Proactivité* (prévenir les risques, logique *ex ante*), 2° *Protection par défaut* (*by default*, c'est-à-dire indépendamment des actions de la personne concernée par les données), 3° *Protection par construction* (dès la conception du système, dans l'architecture des dispositifs), 4° *Somme positive* (protection de la vie privée tout en permettant de tirer un avantage du traitement des données pour le responsable du traitement), 5° *Protection de bout en bout* (protection des données pendant toute la durée de vie de l'information), 6° *Visibilité et transparence* (possibilité d'auditer le système), 7° *Souveraineté de l'individu* qui est « *reconnu comme le chef d'orchestre autour duquel s'organisent tous les échanges d'information*

L'importance de la production doctrinale sur le sujet est aussi importante que dans le domaine de la *Blockchain*. Il faut dire que les applications de *la protection des données dès la conception* sont transversales et tendent à s'appliquer à tous les dispositifs – robots et intelligence artificielle[2070], objets connectés[2071] – et à tous les traitements de données à caractère personnel. Intégrer la protection des données dans la conception des dispositifs techniques, c'est-à-dire « *faire* ab initio *de la garantie de la vie privée une cellule de veille placée au sein de la technologie en phase de conception* »[2072], désigne non pas une technique particulière mais une manière de penser les techniques, les objets et leurs usages. L'une des caractéristiques principales de l'approche *by design* tient dans le fait qu'il s'agit d'une forme de régulation *ex-ante*. Ses principes directeurs visent « *l'adoption d'une approche proactive plutôt que réactive sur les questions du respect de la vie privée. Il s'agit d'anticiper les évènements invasifs, volontaires ou accidentels, avant qu'ils ne surviennent afin de les éviter* »[2073]. Répond ainsi au concept de *Privacy by design* la technique de pseudonymisation des données issues la prise en charge des patients[2074]. Dans la mesure où le concept consiste à « *intégrer la norme juridique dans la norme technique* »[2075], et que les normes techniques ont pour objectif d'intégrer la confidentialité dans l'architecture technique[2076] des dispositifs dans le domaine de la santé, il est nécessaire d'identifier les normes à intégrer avant de voir les techniques et les normes qui sous-tendent cette migration.

---

dans ce qu'il convient d'appeler son éco-système de données personnelles » (Ph. PUCHERAL, A. RALLET, F. ROCHELANDET et C. ZOLYNSKI, « La privacy by design : une fausse bonne solution aux problèmes de protection des données personnelles soulevés par l'open data et les objets connectés ? », *op. cit.*, n° 91).

[2070] Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique ; A. BENSAMOUN et G. LOISEAU, « L'intelligence artificielle : faut-il légiférer ? », *D.* 2017 p.581 ; A. BENSAMOUN, « Des robots et du droit... », *Dalloz IP/IT* 2016, p. 281.

[2071] C. ZOLYNSKI, « La *Privacy by Design* appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel », *Dalloz IP/IT* 2016, p. 404. Notons que, s'agissant des objets connectés en santé, ils répondent à un régime complexe puisqu'ils entrent dans la catégorie des dispositifs médicaux. Ces dispositifs doivent donc répondre à plusieurs corps de règles légales et règlementaires et aux normes prises par la Haute autorité de santé et la CNIL.

[2072] G. LOISEAU, « De la protection intégrée de la vie privée (*privacy by design*) à l'intégration d'une culture de la vie privée », *Légipresse* 2012, n° 300, p. 712.

[2073] G. CHASSANG, « E-santé, droit de l'union européenne et protection de la vie privée des personnes : vers l'émergence d'un « technodroit » spécifique au travers de la proposition de règlement général sur la protection des données personnelles ? », *RLDI*, 1er oct. 2014, n° 108

[2074] *Ibid.*, p. 93.

[2075] A. BENSAMOUN et C. ZOLYNSKI, « Quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux* 2015/1, n° 189, p. 103, spéc. p. 115.

[2076] Dans le cadre de la *Privacy by design*, Mesdames Bensamoun et Zolynski proposaient, bien avant l'entrée en vigueur du RGPD, de diversifier les modes de régulation, et notamment de « *développer le recours à la norme techniques* » (A. BENSAMOUN et C. ZOLYNSKI, « *Cloud computing et big data*. Quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux* 2015/1, n° 189, pp. 103, *spéc.* p. 115).

b - La mise en œuvre de la *privacy by design*

415. Les normes à intégrer. A l'occasion de nos développements portant sur l'articulation entre obligation de sécurité et de confidentialité et le secret professionnel dans le domaine de la santé, nous avons relevé que la première consistait dans l'obligation de protéger le secret à l'égard des tiers non autorisés. La détermination des personnes qui ne peuvent être considérées comme des tiers et qui, par conséquent, peuvent accéder aux données issues de la prise en charge des personnes, s'effectue au regard des faits justificatifs du secret professionnel, et spécialement du secret partagé tel que défini dans le Code de la santé publique, mais également au regard des aménagements prévus dans la loi informatique et libertés.

Dans le contexte de notre recherche, il importe de penser l'approche *by design* au regard de cette articulation. Dès lors, il ne s'agit pas seulement de s'assurer que les données ne sont accessibles qu'aux seules personnes autorisées, mais aussi d'empêcher les atteintes et la violation du secret professionnel par le biais des dispositifs techniques, afin de rechercher les techniques les plus appropriées. Nous reviendrons sur ces enchevêtrements. Pour l'instant, nous pouvons constater que, si la pseudonymisation constitue la première des techniques à mettre en œuvre pour respecter le principe de *privacy by design*, d'autres procédés techniques et organisationnels participent de cette approche. Il faut en évoquer certains.

416. Normes techniques et pseudonymisation. Il importe de mentionner, à ce stade, que la pseudonymisation ne vise pas une technique en particulier. Plusieurs méthodes peuvent être utilisées pour parvenir à une dégradation des données afin de rendre plus difficile l'identification des personnes concernées. Sollicitée dans le cadre de la *privacy by design*[2077], la pseudonymisation est notamment utilisée afin de réutiliser des données à caractère personnel dans le domaine de la santé[2078]. Elle a vocation à être utilisée dans toutes les hypothèses de

---

[2077] RGPD, art. 25 consacré à la *Privacy by design* et *by default* : « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation* […] ».
[2078] V. *supra* n° 375.

réutilisation de données issues d'une prise en charge par un professionnel intervenant dans le système de santé. Les techniques de pseudonymisation font désormais l'objet d'une normalisation technique. De manière générale, la norme ISO/IEC 20889 propose un jeu de techniques de pseudonymisation éprouvées[2079] tandis que dans le domaine de la santé, il faut citer la norme ISO 25237 relative à la pseudonymisation dans le domaine de l'informatique de santé[2080]. Nous verrons comment cette norme est mobilisée au niveau national et quelles sont les conséquences de la normalisation de la pseudonymisation.

417. Des techniques de cryptage aux *Blockchain*. Il serait inutile, dans le cadre de nos travaux, de développer longuement l'histoire des techniques de cryptage ni de disserter sur leur mise en œuvre[2081]. Il importe toutefois de signaler que la cryptographie est une « *écriture secrète qui consiste généralement à transposer les lettres de l'alphabet ou à les représenter par des signes convenus, de manière à ce que le sens de l'écrit ne soit accessible qu'au destinataire en possession du code* »[2082]. Etymologiquement, le mot se compose du préfixe *κρυπτός* qui signifie *caché* et du suffixe *γράφω*, *écrire*. Si le secret est ce qui demeure caché, la cryptographie est ce qui permet d'échanger des communications dont seuls les initiés peuvent comprendre le sens. La technique du cryptage s'est complexifiée et perfectionnée avec l'évolution des recherches en mathématique et en informatique[2083]. Elle s'est également diversifiée et regroupe aujourd'hui des sous-techniques telles que le hachage, le chiffrement et la signature numérique[2084]. Ces techniques n'ont, toutefois, pas toutes les mêmes fonctions. La

---

[2079] La normes ISO/IEC AWI 20889 (« Terminologie et classification des techniques de dé-identification de données pour la protection de la vie privée », nov. 2018), disponible sur : <https://www.iso.org/fr/standard/69373.html> (dernière consultation le 10 août 2019). Citant cette norme technique en exemple pour la mise en œuvre de la *Privacy by design,* un auteur précise que « *Face à la rapidité d'évolution des objets techniques (en particulier dans les univers numériques et algorithmiques), l'utilisation de la technologie comme moyen de garantir la protection des individus a été avancée comme une alternative à la lenteur (relative) d'adaptation des normes juridiques. En application du principe selon lequel « code is law », l'intégration de garde-fous, contre les atteintes aux droits, directement dans l'architecture informatique fait partie de ces solutions* » (J.-M. DELTORN, « La protection des données personnelles face aux algorithmes prédictifs », *RDLF* 2017, chron. n° 12, p. 7).

[2080] ISO 25237, janv. 2017 <https://www.iso.org/fr/standard/63553.html> (dernière consultation le 10 août 2019).

[2081] V. l'ouvrage de référence en la matière : D. KAHN, *The Codebreakers : the Story of Secret Writing*, McMillan Pub., 1967.

[2082] TLFi, op. cit., *V°* « Cryptographie ».

[2083] Sur ce point v. J. SEGAL, *Le zéro et le un*, coll. Sciences&philosophie, éd/ Matériologiques, 2011, spéc. « Chapitre 2. Claude Shannon et le contexte de l'axiomatisation de la notion d'information », p. 101 et svt.

[2084] Sur le plan de la technique informatique v. E. LEOPOLD et S. LHOSTE, *La sécurité informatique*, coll. Que sais-je ? PUF, 2007 spéc. « Chapitre 4. La sécurité informatique », p. 60 et svt. Les trois fonctions de la cryptographie sont : la confidentialité, l'authenticité et l'intégrité (O. EYMARD, « Questions de cryptologie », *Délibérée* 2018/1, n° 3, p. 60).

signature numérique a pour fonction d'assurer l'intégrité, de permettre la vérification de l'origine de l'information et de son authenticité. Elle a fait l'objet de nombreuses réflexions en droit de la preuve et des contrats[2085]. La technique du hachage permet d'assurer l'intégrité des données. Le chiffrement correspond à ce que l'on entend habituellement par cryptographie et consiste dans une méthode de codage des informations qui permet que seules les personnes autorisées puissent y accéder[2086]. L'accès indu ne suffit donc plus à comprendre les informations, seuls ceux qui bénéficient de la *clef* sont en mesure de leur redonner leur intelligibilité, c'est-à-dire d'en prendre connaissance dans une forme conventionnelle. Le chiffrement est donc une technique de protection du *secret* des données faisant l'objet d'un échange. Il est devenu un moyen privilégié pour garantir la confidentialité des données à caractère personnel dans le domaine de la santé. Les techniques de cryptage participent toutes à garantir la confidentialité dans sa dimension technique, en s'assurant que seules les personnes habilitées puissent prendre connaissance des données. Ces techniques sont l'objet d'une

---

[2085] La bibliographie sur le sujet est trop vaste pour être entièrement reproduite, quelques références notables doivent tout de même être mentionnées tant en droit de la preuve qu'en matière de contrat, la question est d'ailleurs transversale : v. notamment M. VIVANT, « L'informatique dans la théorie générale du contrat », *D.* 1994, chron. p. 117 ; P. LECLERCQ, « Evolutions législatives sur les signatures électroniques », *RD informatique et télécoms* 1998-3, p. 19 ; L. GRYNBAUM, « La preuve littérale et la signature à l'heure de la communication électronique », *Comm. et Com. életr.* 1999-2, p. 9 s ; P. CATALA, I. DE LAMBERTERIE, P.-Y. GAUTIER, « L'introduction de la preuve électronique dans le code civil », *JCP G* 1999, n° 47, doctr. 182 ; P. CATALA, « Le formalisme et les nouvelles technologies », *Defrénois* 2000, p. 897 ; I. DE LAMBERTERIE (dir.), *Les actes authentiques électroniques. Réflexion juridique prospective*, Mission de recherche « droit et justice », La Documentation française, 2002 ; *Le contrat électronique*, Association H. Capitant, LGDJ – Panthéon-Assas, 2002 ; E. JOLY-PASSANT, *L'écrit confronté aux nouvelles technologies*, préf. M. VIVANT, coll. Bibliothèque de droit privé, T. 465, LGDJ, 2006 ; A. PENNEAU, « Contrat électronique et protection du cybercontractant, Du Code de la consommation au Code civil », *LPA* 13 mai 2004, n° 96, p. 3 ; « Rapport de droit français », *in La preuve des actes juridiques électronique privés : mosaïque de droits européens ou trait d'union ? Rev. Lamy dr. de l'immatériel* août-sept. 2009, supp. n°52 ; P.-Y. GAUTIER, « Le bouleversement du droit de la preuve : vers un mode alternatif de conclusion des conventions », *LPA* 5 mai 2000, n° 90 ; L. GRYNBAUM, « Loi économie numérique : le sacre des égalités formelles », *Rev. des contrats* 2005/2, p. 580 ; P.- Y. GAUTIER, « L'équivalence entre supports électronique et papier, au regard du contrat », *in Droit et technique. Etudes à la mémoire du Professeur Xavier Linant de Bellefonds*, LexisNexis, 2007, p. 195 ; M. MEKKI, « Le formalisme électronique : la "neutralité technique" n'emporte pas "neutralité axiologique" », *Rev. des contrats* 2007/3, p. 681 ; B. BERTIER-LESTRADE, « Acte électronique et métamorphoses en droit des contrats », *in* M. NICOD (ss. la dir.), *Métamorphoses de l'acte juridique*, coll. Travaux de l'IFR, Presses de l'Université Toulouse 1 Capitole, LGDJ, 2011, p. 50.

[2086] L'art. 29 de la loi n° 2004-575 pour la confiance dans l'économie numérique définit ce que l'on entend par chiffrement : « *on entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité* ».

normalisation que nous ne pouvons explorer, faute de connaissances en la matière. L'on peut tout de même mentionner que les techniques de cryptage les plus utilisées sont celles de l'organisme privé NIST (*National Institute for Standards and Technology*).

Si les techniques de cryptage sont les premières à avoir fait l'objet de travaux de recherche dans le domaine de l'informatique et des mathématiques, la convergence des techniques occupe désormais les chercheurs de tous les domaines[2087]. La technologie *blockchain*, dont le droit s'est saisi depuis peu[2088], fait l'objet d'une littérature déjà dense[2089].

[2087] La recherche nationale et européenne est lancée, depuis quelques années dans une autre compétition globale, celle des technologies quantiques qui auraient des implications en matière de cryptage et de calcul (Office parlementaire d'évaluation des choix scientifiques et technologiques, « Les technologies quantiques : introduction et enjeux », note n° 13, mars 2019).

[2088] C. mon. fin., art. L. 223-12.

[2089] La technique de *Blockchain* a d'abord trouvé à s'appliquer en matière de transfert de monnaies et d'actifs*, elle est née avec la monnaie virtuelle bitcoin* (P. DE PHILIPPI, *Blockchain et cryptomonnaie*, coll. Que sais-je ?, PUF, 2018). Partant, si le droit est devenu « *l'objet de la blockchain, il convient de penser demain la blockchain comme objet du droit* » (M. MEKKI « Les mystères de la blockchain », *D.* 2017, p. 2160). S'est posée alors la question de la place de la *blockchain* dans ses rapports avec le droit : est-ce un objet de régulation ou un objet *à réguler* ? (*La blockchain : de la technologie à la technique juridique*, Dossier, *Dalloz IP*/*IT* 2019, p. 414 ; P.-J. BENGHOZI, « Blockchain : objet à réguler ou outil pour réguler ? », *JCP E* 2017, n° 36, 1470 ; posant également la question : I. RENARD, « Régulation de la *blockchain*, il est urgent d'attendre », *Expertise* juin 2016, p. 215 ; C. ZOLYNSKI, « Quelle approche légale de la *blockchain* », *Banque et stratégie* 2016, p. 16 ; O. HIELLE, « La technologie *blockchain* : une révolution aux nombreux problèmes juridiques », *Dalloz act.*, 31 mai 2016 ; Y. MOREAU et C. DORNBIERER, « Enjeux de la technologie des *blockchains* », *D.* 2016, p. 1856 ; G. CANIVET, « Blockchain et régulation », *JCP E* 2017, n° 36, 1469). La littérature s'est densifiée à un point tel qu'il est impossible d'en donner une liste exhaustive par secteur : la *blockchain* s'est saisie du droit dans de nombreuses branches (pour approche sectorielle et synthétique des applications, v. Cabinet d'avocats Simmons & Simmons LLP, « Le droit et la technologie blockchain : une approche sectorielle », *CCC* oct. 2017, n° 10, étude 10). De par son domaine originel, les questions juridiques sont apparues en premier lieu, en droit des contrats, en droit bancaire, en matière financière et des affaires et, corollairement, en droit de la concurrence. En droit des contrats avec la naissance des *smart contracts* (C. ZOLYNSKI, « Blockchain et smart contracts : premiers regards sur une technologie disruptive », *RD banc. fin.* 2017, dossier 4 ; C. ROQUILLY (ss. la dir.), *Blockchain* et *smart contracts : enjeux technologiques, juridiques et business*, *Cah. Dr. entr.* 2017 ; É. CAPRIOLI, B. CHARPENTIER, V. CHAVANNE, J. DE LABRIFFE, D. O'KANE, C. ROQUILLY, A. TOUATI et É. VIGUIER, « Blockchain et smart contracts : enjeux technologiques, juridiques et business », *Cah. Dr. entr.* 2017, n° 2, entretien 2 ; J. MOIROUX, « Commande publique et technologie blockchain : un avenir, mais quel avenir ? », *JCP A* 2017, 2180 ; M. MEKKI, « Les mystères de la blockchain », *D.* 2017, p. 2160 ; « Le contrat, objet des smart contracts (Partie 1) », *Dalloz IP/IT* 2018, p. 409 ; « Le smart contract, objet du droit (Partie 2) », *Dalloz IP/IT* 2019, p. 27), en matière financière en raison de l'utilisation de la *Blockchain* pour la transmission de titres et pour la réalisation des sûretés (D. LEGEAIS, « L'apport de la Blockchain au droit bancaire », *RD banc. fin.* 2017, dossier 5 ; « Quel avenir pour la blockchain ? », *RD banc. fin.* 2018, repère 2 ; « L'utilisation de la blockchain pour les titres de sociétés non cotées », *Dr. sociétés* 2019, n° 2, étude 2 ; « Blockchain et actifs numériques : le droit français va-t-il devenir réellement attractif ? », *RD banc. fin.* 2019, repère 2). La technique a vocation à s'appliquer à des domaines de plus en nombreux tels que la propriété intellectuelle : M. MALAURIE-VIGNAL, « Blockchain et propriété intellectuelle », *PI* 2018, n° 10, étude 20). Outre les questions juridiques posées par la *Blockchain*, la disparition du tiers de confiance implique une réflexion de fond sur la place des juristes dans les secteurs saisis par cette technique (M. MEKKI, « Blockchain, smart contracts et notariat : servir ou asservir ? », *JCP N* 2018, n° 27, act. 599 ; E. NETTER, « Blockchain et professions réglementées », *Cah. Dr. entr.* 2018, n° 3, dossier 21 ; T. DOUVILLE, T. VERBIEST, « *Blockchain* et tiers de confiance : incompatibilité ou complémentarité ? », *D.* 2018, p. 1144).

La *Blockchain* est une technique de registre distribué[2090], il s'agit d'une « *technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle* »[2091], ce qui permet de se passer de l'intervention humaine[2092]. Monsieur Mekki, dans un article particulièrement éclairant, définit la technologie *Blockchain* au regard de ses fonctions avant de poser certains problèmes juridiques propres aux contrats. Il explique que la *Blockchain* recouvre des fonctions de transmission, de conservation et d'automatisation[2093]. A ce titre, cette technique est, selon lui, susceptible de participer à la protection des données et de contribuer à assurer le secret des données issues de la prise en charge des personnes par le système de santé[2094].

418. Application de la *Blockchain* dans le domaine de la santé. Les applications de la *Blockchain* dans le domaine de la santé sont en plein développement[2095]. Sur le plan des usages, la technologie est sollicitée dans le domaine pharmaceutique afin de tracer les lots et s'intégrer dans la chaîne de distribution, ce qui permettrait également de lutter contre la contrefaçon[2096]. Elle contribuerait ainsi à une meilleure traçabilité et à garantir la sécurité sanitaire[2097]. Il est

---

[2090] « […] *la blockchain se caractérise quant à elle par un registre de transactions distribué, une base de données décentralisée qui repose sur un réseau pair à pair destiné au stockage et au transfert de données. Grâce à la cryptographie, la blockchain permet le transfert de ressources en format numérique (monnaies virtuelles ou autres ressources dont la valeur dépend de leur rareté) sans passer par un intermédiaire de confiance. Contrairement aux bases de données traditionnelles, administrées par des opérateurs centralisés, la blockchain est administrée de manière collective par tous les nœuds du réseau. Ces nœuds obéissent tous à un même protocole informatique, qui définit les procédures à suivre, ainsi que les conditions à respecter pour mettre à jour cette base de données* » (P. DE PHILIPPI, *Blockchain et cryptomonnaie*, *op. cit.*, p. 4).

[2091] <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>, *Blockchain Partner* (dernière consultation le 5 oct. 2019).

[2092] Y. COHEN-HADRIA, « *Blockchain* : révolution ou évolution ? », *Dalloz IP/IT* 2016, p. 537.

[2093] M. MEKKI, « Les mystères de la blockchain », *op. cit.* L'auteur parle d'ailleurs de la préservation du « secret médical ».

[2094] Citant des iniatives outre-Atlantique telles que le Projet MedRec, le projet Watson d'IBM et la *blockchain health*, Monsieur Mekki explique : « *En droit médical, la* blockchain *permet un échange d'informations sur les dossiers des patients en garantissant l'intégrité des documents, en évitant les erreurs et en préservant le secret médical* » (M. MEKKI, « Les mystères de la blockchain », *op. cit.*, spéc. n° 13).

[2095] De nombreux concours et start-up dans ce domaine voient le jour : « Use of *blockchain* in health IT and health-related research », 30 août 2016, <https://bravenewcoin.com/news/15-blockchain-whitepapers-awarded-winners-of-us-department-of-health-and-human-services-challenge/> ; par exemple la start-up 23consulting spécialisée dans la *Blockchain* en santé ou encore *Blockchain Partner*.

[2096] Cabinet d'avocats Simmons & Simmons LLP, « Le droit et la technologie blockchain : une approche sectorielle », *CCC* Oct. 2017, n° 10, étude 10, n° 21 ; *Blockchain Partner*, Etude *Blockchain et Santé*, p. 9 disponible sur <https://blockchainpartner.fr/wp-content/uploads/2017/06/Sant%C3%A9-Industrie-Pharmaceutique-Blockchain.pdf>.

[2097] *Ibid.*

aussi question de faire de la *Blockchain* le support du dossier médical partagé. Toutefois, l'une des caractéristiques de cette technologie, la transparence, s'y prête mal puisque la *Blockchain* « *ne peut pas (ou n'a pas intérêt à) stocker des informations comme des résultats d'analyses sanguine ou d'IRM par exemple. De tels documents sont trop lourds pour assurer une blockchain viable et sécurisée* »[2098]. De surcroît, comme le remarque Monsieur Douville, il existe une « *double incompatibilité* »[2099] entre cette technologie et la protection des données, la première étant, selon les termes employés par cet auteur, d'ordre intellectuel et la seconde d'ordre judirique. Il souligne en effet que la *Blockchain* est, par essence, décentralisée, tandis que la protection des données est axée autour de la figure centrale d'un responsable de traitement identifié[2100]. Ensuite, l'incompatibilité juridique tient à la décentralisation mais également au caractère intangible des chaînes de blocs qui ne permettent pas la mise en œuvre des droits des personnes à l'égard du traitement[2101]. Malgré le travail de communication des acteurs du secteur, cette technique présente, pour l'instant, de trop grandes contradictions avec les dispositions du RGPD[2102]. La convergence des techniques pourrait néanmoins permettre une évolution prochaine et une application au *Big data* en santé[2103], la sécurisation des données automatiquement échangées demeurant un domaine prometteur : « *Dans le domaine de la e-santé, l'échange d'informations sur les dossiers des patients tout en préservant le secret médical est crucial. La plus-value des blockchains en la matière a conduit IBM et la Food and Drug Administration (FDA) à tester l'échange sécurisé de données médicales* »[2104]. L'Estonie

---

[2098] *Blockchain Partner*, Etude *Blockchain et Santé*, p. 9 disponible sur <https://blockchainpartner.fr/wp-content/uploads/2017/06/Sant%C3%A9-Industrie-Pharmaceutique-Blockchain.pdf>, p. 4.
[2099] T. DOUVILLE, « Blockchain et protection des données à caractère personnel », *AJ contrat* 2019, p. 316, spéc. n° 3.
[2100] *Ibid.* n° 3.
[2101] *Ibid.* n° 3.
[2102] Dans le même sens : V. BUTERIN, « Privacy on the blockchain », 15 janv. 2016, <https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/> (dernière consultation le 5 oct. 2019) ; Pour une vision d'ensemble des problématiques au regard du RGPD, v. J. DEROULEZ, « Blockchain et données personnelles. Quelle protection de la vie privée ? », *JCP G* 2017, n° 38, 973, spéc. n° 9 ; C. MARTIN-FORISSIER, « Blockchain et RGPD, une union impossible », 24 août 2017, Laboratoire d'innovation numérique de la CNIL, disponible sur : <https://linc.cnil.fr/fr/blockchain-et-rgpd-une-union-impossible-0> (dernière consultation le 5 oct. 2019) ; CNIL, communiqué, 24 sept. 2018, *JCP E* 2018, act. 738 ; D. LEGEAIS, « Blockchain et données personnelles : réponse de la CNIL », *JCP E* 2018, n° 41, act. 754 ; T. DOUVILLE, « Blockchain et protection des données à caractère personnel », *op.cit.*
[2103] *Blockchain Partner*, Etude *Blockchain et Santé*, p. 9 disponible sur <https://blockchainpartner.fr/wp-content/uploads/2017/06/Sant%C3%A9-Industrie-Pharmaceutique-Blockchain.pdf>, p. 4.
[2104] O. LASMOLES, « La difficile appréhension des blockchains par le droit », *RIDE* 2018/4 (t. XXXII), p. 453.

expérimente, depuis 2015, la *blockchain* pour stocker les dossiers médicaux[2105]. Dans cette optique, il s'agit autant de protéger le secret des données issues de la prise en charge des personnes par des professionnels intervenant dans le système de santé que d'empêcher toute divulgation des données par le professionnel au moyen des technologies. Si les applications de la technologie *Blockchain* dans le domaine de la santé relèvent encore du possible, cette technologie pourrait devenir un outil de la *Privacy by design* et faire l'objet d'une normalisation accrue.

419. La normalisation de la sécurité des systèmes, des réseaux et des échanges dans le domaine de la santé. Ainsi que nous l'avons expliqué plus avant, la sécurité des systèmes d'information participe pleinement de l'approche *by design*. Comme le soulignait Madame Zolynski à propos des objets connectés de la *privacy by design* : « *loin d'être une méthode prédéterminée résultant d'une approche englobante, la PbD doit donc se penser* in concreto*, à l'aune de chaque modèle technique et commercial développé* »[2106]. C'est l'objet même des référentiels et des certifications délivrés par l'ASIP-santé[2107], qui sont élaborés conjointement avec la CNIL[2108] et les acteurs du secteur. La Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) qui sert de socle est composée de plusieurs référentiels et guides répondant à des normes et des standards techniques internationaux[2109] , européens ou nationaux[2110]. Ce corpus est ainsi formé de normes de natures diverses, des

---

[2105] A. WRIGHT et P. DE FILIPPI, « Decentralized Blockchain Technology and the Rise of Lex Cryptographia », abstract, Social Science Research Network (SSRN), 10 mars 2015 (<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> (dernière consultation le 5 oct. 2019)).

[2106] C. ZOLYNSKI, « La Privacy by Design appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel ? », *Dalloz IP/IT 2016*, p. 404.

[2107] L'ASIP-santé, bien que ses missions soient en partie différentes, peut être considéré comme le pendant sectoriel de l'ANSSI. Cette agence a, entre autres, pour mission d'accompagner la transformation numérique du système de santé. Pour ce faire, elle rédige des guides et pose les bonnes pratiques, de sécurité et d'interopérabilité pour faciliter le partage et les échanges de données de santé en toute confiance.

[2108] Soulignons que, dans ses publications généralistes relatives à la sécurité, la CNIL fait référence à des normes techniques internationales (ISO) ainsi qu'aux normes souples rédigées par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) : <https://www.cnil.fr/fr/securite-des-donnees-proteger-le-plus-sensible-de-maniere-specifique> (dernière consultation le 5 oct. 2019). Par ailleurs, la Commission a un pouvoir de certification des personnes (notamment des délégués à la protection des données), certification qui s'opère au regard de la conformité à un référentiel élaboré par la CNIL. Nous aurons l'occasion d'y revenir : v. *infra* n° 468.

[2109] Tels que les normes ISO, normes d'origine privée conçues par l'Organisation internationale de normalisation (ISO), mais les référentiels de l'ASIP font mention de quantité d'autres normes provenant d'organismes divers. L'on peut en trouver des exemples dans tous les référentiels de l'ASIP-santé lesquels contiennent des volets spécifiques portant sur l'étude des normes et standards.

[2110] Il s'agit notamment des normes AFNOR (Association française de normalisation).

référentiels et guides de bonnes pratiques qui constituent les normes de droit souple les mieux identifiées en raison des institutions dont elles émanent[2111] et des normes techniques, d'origine privée ou européenne. Leur objet est de formuler le cadre normatif de la sécurité des réseaux, des systèmes d'information et des échanges dans le domaine de la santé. Nous reviendrons sur ce point au moment traiter de l'enchevêtrement entre les dispositifs normatifs. L'ISO compte actuellement quelques 253 normes techniques relatives à l'informatique en santé, ayant vocation à assurer efficacement l'interopérabilité, la sécurité et la confidentialité des données dans le domaine de la santé[2112]. En somme, toute l'architecture qui soutient le traitement des données dans le domaine de la santé fait l'objet d'une normalisation technique.

420. La sécurité et la confidentialité des données de santé saisies par les normes techniques. Notre intention n'est pas de dresser une liste exhaustive des normes techniques ayant vocation à s'appliquer lors de la mise en œuvre de dispositifs techniques supportant le traitement des données couvertes par le secret, mais d'en donner un aperçu. Il ne s'agit pas, non plus, d'en proposer une étude substantielle approfondie car nous ne disposons pas des outils méthodologiques nécessaires, ces normes sont inintelligibles pour le juriste et, plus généralement, pour les non initiés. Elles sont en effet destinées, à première vue, à des professionnels de l'informatique et de l'information ainsi qu'aux industriels produisant et proposant des dispositifs et solutions techniques aux professionnels de santé, établissements de santé, établissements médico-sociaux et cliniques. L'approche substantielle de ces normes est, en outre, peu investie par les juristes[2113]. Il ne s'agit que d'exemples car l'essentiel, au travers

---

[2111] Les normes produites par les agences et les autorités administratives indépendantes sont un « *instrument des mutations de l'Etat* » (Rapport annuel du Conseil d'Etat, *Le droit souple*, La documentation française, 2013, p. 32 et svt.). Les agences sont toutefois distinctes des autorités administratives, les premières ayant pour fonction de mettre en œuvre les politiques publiques (J. CHEVALLIER, « Les agences : effet de mode ou révolution administrative ? », *in Etudes en l'honneur de Georges Dupuis*, LGDJ, 1997, p. 47). Leur création est « *étroitement liée aux réformes de modernisation de l'administration* » (*Ibid.*), elles peuvent être considérées comme des « *organes déconcentrés* » de l'Etat (O. NAY (ss. la dir.) *Lexique de science politique*, *V° «* Agence », coll. Lexiques, Dalloz) et répondent à l'application des principes du *New public management* (*Ibid.*). Tandis que les secondes ont une fonction de régulation et une indépendance dont ne bénéficient pas les premières. Leur filiation est néanmoins soulignée par le Conseil d'Etat (Rapport du Conseil d'Etat, *Les autorités administratives indépendantes*, La documentation française, 2001, p. 270).

[2112] V. <www.iso.org> (dernière consultation le 5 oct. 2019).

[2113] Ces normes sont peu investies du moins en droit de la santé et en droit du numérique. En droit social, en droit des sociétés et plus généralement en droit économique, certaines normes, notamment ISO, ont fait l'objet de travaux, et plus particulièrement la norme ISO 26000 définissant la responsabilité sociétale des organisations. Elle n'est, certes, pas une norme technique mais elle a été produite par un organisme de normalisation international (F. LARONZE, « La norme ISO 26000, une source de droit en matière sociale ? L'apport de la théorie du droit à la réflexion sur les normes de la RSO », *Droit social* 2013, p. 345 ; M. CAPRON, F. QUAIREL, M.-F. TURCOTTE,

de ces quelques développements, est de souligner l'importance de ces normes, de leur nombre et de la place qu'elles occupent pour les acteurs dans la logique de la *privacy by design*. Au titre des principes fondateurs de la Politique Générale structurant l'ASIP-santé, il est rappelé que la confidentialité requiert la maîtrise des accès aux données « *dans le respect du secret professionnel* »[2114], ainsi que les contours et conditions du secret partagé. Ces exigences ne sont pas uniquement techniques mais déterminent aussi les mesures organisationnelles ayant pour but de prédéterminer le circuit des données afin d'anticiper les risques de violation du secret professionnel et les accès indus, c'est-à-dire les atteintes au secret des données couvertes par le secret.

B - Des mesures organisationnelles normalisées

421. Les mesures organisationnelles, une expression visant le *management*. Il est, aujourd'hui, de plus en plus question de « *management de la sécurité* »[2115] en matière de protection des données à caractère personnel, à tel point qu'un nouveau métier – qui ne peut pas encore être qualifié de discipline – voit le jour : le *data manager*. Il faut, pour tenter de comprendre le mouvement à l'œuvre, revenir à des questions de traduction. Lors de la Conférence *Data protection and Privacy Commissioners* qui s'est tenue à Jérusalem en octobre 2010, réunissant les commissaires à la protection des données[2116], une résolution a été adoptée, la *privacy by design* y étant définie comme : « *the philosophy and approach of embedding privacy into the design, operation and management of information technologies and systems, across the entire information life cycle* »[2117]. L'on comprend donc que le volet organisationnel

---

ISO 26000 : une norme 'hors norme' ? vers une conception mondiale de la responsabilité sociétale, Economica, 2011), et intéresse également d'autres branches du droit (M.-J. DEL REY, « L'ISO 26000, une démarche « développement durable » à portée des collectivités », *AJCT* 2012, p. 370).

[2114] ASIP-santé, *Principes fondateurs Politique Générale de Sécurité des Systèmes d'Information de Santé* (PGSSI-S), V1.0, juill. 2013 : <https://esante.gouv.fr/sites/default/files/media_entity/documents/Principes_Fondateurs_PGSSI.pdf> (dernière consultation le 5 oct. 2019). Sur la signification de cette expression.

[2115] L.- M. AUGAGNEUR, « Le management juridique de la cybersécurité en matière d'« e-santé » », *RLDI* janv. 2017, n° 133.

[2116] Cette conférence fait partie des instances internationales ayant pour vocation d'harmoniser, dans la mesure du possible, la protection des données à caractère personnel. L'on compte, outre la Conférence internationale des commissaires à la protection des données, des instances politique telles que l'OCDE, le Conseil de l'Europe et l'APEC (*Asian-Pacifique economic cooperation*).

[2117] *Resolution on Privacy by design, 32nd International Conference on Data protection and Privacy Commissioners*, Jerusalem, 27-29 octobre 2010, p. 2.

de l'approche *by design* consiste dans le *management des données, de l'utilisation des techniques et des systèmes*. La définition donnée au terme *management* est celle d'un « *ensemble des méthodes d'organisation efficace (définition et partage des responsabilités) et de gestion rationnelle (en fonction d'objectifs ou de programmes fixés) employées dans la direction d'une affaire, d'une entreprise* »[2118]. Il s'agit d'*organiser*, mais également de *gérer* puisque l'anglais utilise *gestion* comme synonyme de *management*[2119]. Si le terme de *management* n'apparaît pas dans la version anglaise, originelle, du RGPD, il nous semble que le sens même des mots suffit à se convaincre que l'approche *by design* suppose la mise en place de méthodes, *process*, d'organisation et de gestion des données. Dans le domaine de la santé, cette inclinaison est visible si l'on prend la peine de consulter les instruments de droit souple pris, notamment, par l'ASIP-santé qui font référence à des normes techniques *mais aussi* à des normes managériales.

422. *Manager* la sécurité et la confidentialité des données, étape préliminiaire : identifier les risques. Le management de la sécurité des données consiste d'abord en un travail d'identification des risques que le traitement des données engendre pour la vie privée des personnes à partir d'une cartographie des données traitées et de la réalisation d'une analyse d'impact relative à la protection des données[2120]. La CNIL propose une méthode et un outil[2121], dont l'acronyme *PIA* est issu de l'anglais *Privacy impact assessment*. Cette analyse permet d'évaluer le risque engendré par le traitement pour la vie privée des personnes afin de déterminer les mesures à mettre en œuvre[2122]. C'est un marqueur de la logique de *compliance*, puisque ces analyses ne sont pas obligatoires pour tous les types de traitement mais, de leur réalisation dépend la capacité du responsable de traitement à démontrer qu'il est en conformité avec les dispositions relatives à la protection des données. Une analogie est possible avec les analyses d'impact en matière d'installations SEVESO qui sont « *destinées à identifier les*

[2118] TLFi, *V°* « Management ». En anglais, « *the process of organizing or controlling something* » (Cambridge Dictionary, *V°* « Management »).
[2119] Cambridge Dictionary, *V°* « Management ».
[2120] Prévu à l'article 35 du RGPD.
[2121] Il s'agit d'un logiciel libre d'accès, disponible sur : < https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil> (dernière consultation le 15 juill. 2019).
[2122] Notons au passage que le *PIA* n'est pas le seul modèle d'analyse d'impact, il en existe d'autres qui peuvent être utilisés dans le domaine de la santé comme par exemple EBIOS qui est une méthode crée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

risques à leur source et examiner les différentes mesures disponibles pour les atténuer »[2123]. A la suite des lignes directrices rédigées par le G29[2124], la CNIL a publié une liste de traitements pour lesquels elle estime que l'étude d'impact est *nécessaire* et au titre desquels figurent, en premier lieu, les traitements de données à caractère personnel issues de la prise en charge des personnes par des professionnels intervenant dans le système de santé[2125]. A partir de cette

---

[2123] B. FAUVARQUE-COSSON et W. MAXWELL, « Protection des données personnelles », *D.* 2018, p. 1033.

[2124] Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, 4 avr. 2017.

[2125] La liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise est disponible sur <https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-avec-aipd-requise-v2.pdf>. Au sein de cette liste figurent : 1° *les traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes*, à titre d'exemple : les traitements « de santé » mis en œuvre par les établissements de santé (hôpital, CHU, cliniques, etc.), le dossier « patients », les algorithmes de prise de décision médicale, les dispositifs de vigilance sanitaire et de gestion du risque, les dispositifs de télémédecine, la gestion du laboratoire de biologie médicale et de la pharmacie à usage intérieur, etc., le traitement portant sur les dossiers des résidents pris en charge par un centre communal d'action sociale (CCAS) ou par un établissement d'hébergement pour personnes âgées dépendantes (EPHAD) ; 2° *Traitements portant sur des données génétiques de personnes dites « vulnérables » (patients, employés, enfants, etc.)* et par exemple : la mise en œuvre d'une recherche médicale portant sur des patients et incluant le traitement de leurs données génétiques ; le traitement utilisé pour la gestion d'une consultation de génétique dans un établissement de santé ; 3° *Traitements ayant pour finalité la gestion des alertes et des signalements en matière sociale et sanitaire*, par exemple : le traitement utilisé par une agence sanitaire pour la gestion d'une crise sanitaire ou d'une alerte sanitaire ; 4° *Traitements des données de santé nécessaires à la constitution d'un entrepôt de données ou d'un registre*, tels que l'entrepôt de données de santé mis en œuvre par un établissement de santé ou une personne privée, pour servir des finalités de recherche ; 5° *Traitements de données biométriques aux fins d'identifier une personne physique de manière unique parmi lesquelles figurent des personnes dites « vulnérables » (élèves, personnes âgées, patients, demandeurs d'asile, etc.)* comme par exemple : le traitement basé sur la reconnaissance de l'empreinte digitale ayant pour finalité le contrôle de l'identité des patients ; 6° *Traitements ayant pour finalité l'accompagnement social ou médico-social des personnes,* comme le traitement mis en œuvre par un établissement ou une association dans le cadre de la prise en charge de personnes en insertion ou réinsertion sociale et professionnelle, le traitement mis en œuvre par les maisons départementales des personnes handicapées dans le cadre de l'accueil, l'hébergement, l'accompagnement et le suivi de ces personnes, le traitement mis en œuvre par un centre communal d'action sociale dans le cadre du suivi de personnes atteintes de pathologies chroniques invalidantes en situation de fragilité sociale. Notons que, selon la CNIL, les patients sont des personnes « vulnérables ». S'il est certain que la qualification de *personne vulnérable* n'est pas celle connue en matière pénale et qui constitue une circonstance aggravante de certaines infractions contre les personnes, rien ne permet d'en interpréter le sens. Un élément de réponse se trouve dans les lignes directrices du G29 concernant l'analyse d'impact relative à la protection des données (Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, 4 avr. 2017). Les lignes directrices sont rédigées au regard du RGPD, dont le considérant 75 précise que l'évaluation du risque que présente le traitement pour les personnes varie au regard des situations, au titre desquels figure, entre autres, la perte de confidentialité des données protégées par le secret ainsi que la vulnérabilité des personnes. Sur la base de ce considérant, le G29 précise ce qu'il faut entendre par *personnes vulnérables* : « *Données concernant des personnes vulnérables (considérant 75): le traitement de ce type de données est un critère en raison du déséquilibre des pouvoirs accru qui existe entre les personnes concernées et le responsable du traitement, ce qui signifie que les premières peuvent se trouver dans l'incapacité de consentir, ou de s'opposer, aisément au traitement de leurs données ou d'exercer leurs droits. Peuvent être considérés comme des personnes concernées vulnérables, les enfants (qui peuvent être*

analyse les mesures organisationnelles prennent la forme d'une gestion interne et d'une « *contractualisation externe de la répartition des missions et des responsabilités* »[2126].

423. Normes ISO « Systèmes de management de la sécurité de l'information ». C'est sur le plan de la gestion interne des systèmes d'information qu'interviennent les normes managériales. Le management de la sécurité des systèmes d'information fait l'objet d'une normalisation internationale. Une série de normes – qui intègre des instruments nationaux de droit souple dans le domaine de la santé – a en effet été conçue par l'Organisation internationale de normalisation, il s'agit de la famille de normes ISO/IEC 27000. Certaines normes internationales ciblent spécifiquement la gestion de la sécurité et de la confidentialité des données de santé, telles que la norme ISO 27799 qui est une norme concernant « la gestion de la sécurité dans le domaine de la santé à l'aide de l'ISO/CEI 27002 ». Par ailleurs, une norme spécifique au management de la protection des données a récemment vu le jour[2127].

§ 2 - La sécurité et la confidentialité des systèmes et des échanges dans le domaine de la santé : enjeux politiques des normes technico-managériales

424. Nous avons évoqué la mise en réseau des données issues de la relation de soins ainsi que les incitations à rendre les systèmes d'informations informatisés, interopérables[2128]. Ce mouvement est soutenu par un projet politique européen au regard duquel les normes technico-

---

vus comme incapables de s'opposer ou de consentir sciemment et de manière réfléchie au traitement de leurs données), les employés, les segments les plus vulnérables de la population nécessitant une protection particulière (personnes souffrant de maladie mentale, demandeurs d'asile et personnes âgées, patients, etc.) et, en tout état de cause, toutes autres personnes pour lesquelles un déséquilibre dans la relation avec le responsable du traitement peut être identifié. » (*Ibid.,* p. 12). Le déséquilibre – concernant le traitement des données à caractère personnel dans le domaine de la santé – tient au fait que la personne prise en charge par un professionnel intervenant dans le système de santé ne peut en général que s'opposer au traitement de ses données. Ensuite, et surtout, même si le traitement de leurs données a pour finalité leur propre suivi et donc leur propre intérêt, nous avons vu que les données collectées ont d'autres utilités et peuvent également être réutilisées. Bien que les personnes disposent encore d'un droit d'opposition, il apparaît qu'elles n'ont pas la maîtrise des données, certains de leurs droits sur les données (portabilité, effacement) connaissant des atténuations en raison de la finalité d'intérêt public.

[2126] *Ibid.* On peut par exemple évoquer, à ce titre, les contrats d'hébergement avec des hébergeurs de données de santé bénéficiant d'une certification.

[2127] V. *infra* n° 461.

[2128] V. *supra* n° 372 et svt.

managériales sont des outils d'harmonisation adéquats **(A)**. Au niveau national, la mise en œuvre de cette politique s'appuie également sur des normes de ce type **(B)**.

A - Des instruments d'harmonisation

425. Stratégie européenne pour la construction d'un marché unique numérique. A l'époque de l'élaboration de la loi informatique et libertés, les enjeux internationaux du traitement des données et l'importance de l'innovation techniques pour la souveraineté nationale étaient déjà importants[2129]. Depuis, ils n'ont fait que croître, en prenant une autre dimension puisque c'est désormais au niveau européen qu'existent les enjeux. Il s'agit notamment de faire barrage aux GAFAM ainsi qu'à la puissance numérique grandissante de la Chine[2130]. Ainsi, l'une des priorités de l'Union depuis 2010 est la construction d'un « marché unique numérique », date de la première stratégie numérique[2131]. Cette stratégie a été reconduite en 2015[2132]. Elle est guidée par des objectifs multiples qui visent à « *mieux exploiter le potentiel des technologies de l'information et de la communication (TIC) afin de favoriser l'innovation, la croissance économique et le progrès* »[2133]. Dans le domaine de la santé, il s'agit de favoriser

---

[2129] V. *supra* n° 315.

[2130] Un avis récent du CESE (Conseil économique, social et environnemental) retrace les enjeux politiques internationaux : B. THIEULIN (rapporteur), *Pour une politique de souveraineté européenne du numérique*, mars 2019. Si la question portait, au début des années 1980, sur la maîtrise des dispositifs techniques, le *Big data* et la course à l'intelligence artificielle ont amplifié la concurrence mondiale et le discours sur « le retard » en matière de technologie est à nouveau à l'ordre du jour, certains évoquent même l'émergence d'une « *géopolitique de la donnée* » : v. T. BERTHIER et O. KEMPF, « Vers une géopolitique de la donnée », *in L'Union numérique européenne*, série Réalités industrielles, 2016/3, *Annales des Mines*, pp. 13-18.

[2131] « Stratégie numérique pour l'Europe » adoptée le 10 mai 2010, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions, COM (2010) 245 final.

[2132] « Stratégie pour un marché unique numérique », Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions, Stratégie pour un marché unique numérique en Europe, COM (2015) 192 final.

[2133] C. CASTETS-RENARD, V. NDIOR et L. RASS-MASSON, « Le marché unique numérique : quelles réalités matérielles et conceptuelles ? », *D.* 2019, p. 956. La question économique est centrale dans la lutte engagée contre les GAFAM et celle-ci passe nécessairement par l'innovation. Le rapport du député Cédric Villani est un bon exemple de l'importance de l'innovation industrielle pour l'économie numérique. Un élement de langage renseigne en effet sur la volonté de développer l'industrie numérique : il y est question de « *champions* » du numérique à l'échelle nationale et européenne (C. VILLANI, Rapport au premier ministre, *Donner du sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*, 28 mars 2018, pp. 27-28). Encore au titre des questions centrales pour préserver la souveraineté numérique, des auteurs évoquent « *celles de la création de champions européens, de la croissance du secteur numérique en Europe et d'enjeux davantage liés aux acteurs économiques qu'au seul consommateur. L'enjeu est d'autant plus crucial qu'une captation croissante de la valeur d'un grand nombre d'activités non numériques, et des emplois afférents, peut s'opérer par les grandes*

« *l'échange transfrontière de données sanitaires au sein de l'Union européenne* » et « *la disponibilité de données de santé comparables et de grande qualité pour la recherche et l'innovation afin de générer de nouvelles connaissances et de proposer des solutions numériques les plus adaptées dans le domaine des soins* »[2134]. Il ne s'agit pas là d'une nouveauté mais du prolongement d'un plan d'action pour la santé pris en 2004 par la Commission et d'une directive sur les soins transfrontières[2135]. La *transformation numérique* des services de santé et de soins de santé au niveaux national constitue donc une condition de l'existence de ce marché unique. Or, un tel objectif ne peut être réalisé que si les citoyens et les acteurs du monde de la santé ont *confiance dans le numérique*[2136], condition qui passe notamment par la garantie de la sécurité et de la confidentialité des données à caractère personnel, c'est-à-dire, s'agissant des données à caractère personnel dans le domaine de la santé : assurer le maintien du secret des données issues de la prise en charge des personnes. L'harmonisation des moyens nécessaires à cette fin doit alors s'effectuer à l'échelle européenne. En outre, cette harmonisation au niveau européen favorise la réutilisation des données issues de la prise en charge des personnes par le système de santé, affermissant leur statut de *communs*.

426. Harmonisation et politique européenne des données. Les premiers instruments contribuant à instaurer la confiance et participant à l'harmonisation dans l'espace européen sont

---

plateformes » (X. MERLIN et M. WEILL, « Quel avenir numérique pour l'Europe ? », Série Réalités industrielles 2018/1, *Annales des Mines,* pp. 42-45).

[2134] N. DE GROVE-VALDEYRON, « Politique de santé de l'Union européenne et transformation numérique des soins : quels enjeux pour quelle compétence ? », *Rev. UE* 2019, p. 39.

[2135] Retraçant le cheminement vers le marché unique numérique : v. N. DE GROVE-VALDEYRON, « Politique de santé de l'Union européenne et transformation numérique des soins : quels enjeux pour quelle compétence ? », *op. cit.* ; concernant spécifiquement la directive : L. DUBOUIS, « La directive n° 2011/24/UE relative à l'application des droits des patients en matière de soins de santé transfrontaliers », *RDSS* 2011, p. 1068, n° 6.

[2136] « *La transformation numérique des soins est complexe. Elle se fera progressivement, uniquement si elle emporte la confiance des citoyens, pour autant qu'une volonté politique des États se dégage en faveur de celle-ci et que tous les acteurs tant au niveau des États que de l'Union s'engagent dan*s un « effort concerté » *à* « travailler ensemble » » (N. DE GROVE-VALDEYRON, « Politique de santé de l'Union européenne et transformation numérique des soins : quels enjeux pour quelle compétence ? », *Rev. UE* 2019, p. 39). Evoquant également la confiance comme condition de l'accélération du numérique en santé, v. F. EON, « L'accélération du numérique en santé : enjeux et conditions de son succès », *RDSS* 2019, p. 55. Plus généralement, l'expression « confiance dans le numérique » est omniprésente dans le discours politique depuis quelques années.

le RGPD[2137] et le règlement relatif à la cybersécurité[2138]. Toutefois, si le premier permet de prétendre à un niveau de protection des données à caractère personnel relativement uniformisé dans les pays de l'Union européenne, les obstacles à la création d'un marché unique numérique demeurent nombreux. Du point de vue purement technique, l'interopérabilité des dispositifs techniques, dont l'intérêt sur le plan interne a pu être souligné, est un premier défi. Sur ce point, l'Union se place, comme dans d'autres domaines, tels que le développement de l'intelligence artificielle, en « chef d'orchestre » misant sur une coordination des politiques nationales[2139] puisque le domaine de la santé relève de la compétence des Etats membres[2140]. La sécurité et la confidentialité des données constituent évidemment l'un des autres défis centraux de cette harmonisation. Or, si le règlement européen définit un cadre général de protection des données à caractère personnel, l'harmonisation apparaît toutefois périlleuse pour la sécurité et de la confidentialité des données à caractère personnel issues de la prise en charge des personnes par un professionnel soumis au secret. Se retrouvent ici les limites de la législation nationale et du RGPD, dont la marge de manœuvre constitue un risque d'éparpillement[2141]. Par ailleurs, la cybersécurité, sur le plan européen, est en pleine construction et sa régulation est principalement axée sur la normalisation et les efforts de développement d'une certification commune. Ainsi, l'objectif de circulation des données issues de la prise en charge sur le territoire national vers d'autres Etats membres, tout en garantissant aux personnes le respect du *secret*, ne peut être

---

[2137] « *Les données, y compris les données de santé, qui constituent un facteur-clé pour la transformation numérique, ne connaissent pas de frontières et ne sont pas gérées de façon identique dans tous les systèmes nationaux sous réserve de la protection uniforme découlant du règlement général relatif à la protection des données* » (N. DE GROVE-VALDEYRON, « Politique de santé de l'Union européenne et transformation numérique des soins : quels enjeux pour quelle compétence ? », *op. cit.*). Dans le même sens et soulignant la « dimension marché intérieur » du RGPD, v. C. BARREAU, « Le marché unique numérique et la régulation des données personelles », *in L'Union numérique européenne*, Série Réalités industrielles 2016/3, *Annales des Mines*, pp. 37-41.

[2138] PE et Cons., Règlement (UE) 2019/881, relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013 (règlement sur la cybersécurité), 17 avril 2019, *JOUE* 7 juin 2019, L 151/15.

[2139] A. BENSAMOUN, « Stratégie européenne sur l'intelligence artificielle : toujours à la mode éthique... », *D.* 2018, p. 1022.

[2140] TFUE, art. 168, § 7 : « *L'action de l'Union est menée dans le respect des responsabilités des États membres en ce quiconcerne la définition de leur politique de santé, ainsi que l'organisation et la fourniture de services de santé et de soins médicaux. Les responsabilités des États membres incluent la gestion de services desanté et de soins médicaux, ainsi que l'allocation des ressources qui leur sont affectées* ».

[2141] V. en ce sens C. BARREAU, « Le marché unique numérique et la régulation des données personnelles », *op. cit.*

opérationnel que par un recours soutenu à la normalisation, ce que nous avons pu esquisser au travers des quelques développements relatifs à la *privacy by design* et à la cybersécurité. D'autres textes contribuent toutefois à tracer les linéaments d'une harmonisation pour certains dispositifs techniques : le règlement européen relatif à la signature et l'identification électronique et aux services de confiance (eIDAS)[2142] et la directive « *Network and Information Sécurity* »[2143] (NIS).

427. Le marché unique numérique et les *données santé.* Une communication de la Commission publiée en avril 2018[2144] rappelle les lignes directrices de la politique de l'Union en matière de santé numérique. Il est également fait mention des obstacles majeurs au marché unique numérique dans le domaine de la santé qu'a mis en avant la consultation publique relative à la transformation de la santé et des soins dans le marché numérique : « *Les domaines qui posent le plus de problèmes sont l'accès aux données de santé, la diversité des dossiers de santé informatisés, le manque d'interopérabilité technique et l'accès aux services de santé numérique. Cette consultation a également mis en évidence des préoccupations liées au partage de données par voie électronique, à savoir le risque d'atteinte à la vie privée, les risques en matière de cybersécurité et la qualité et la fiabilité des données* »[2145]. Au regard de ces freins, la Commission propose une harmonisation qui s'appuie sur des normes européennes pour la qualité des données, la fiabilité et la cybersécurité ; les dossiers de santé et l'interopérabilité. Elle précise, sans évoquer explicitement la *Privacy by design*, que les garanties appropriées au partage des données doivent « *être fournies par des moyens technologiques pour les infrastructures conformes aux règles en matière de protection des données* »[2146]. La Commission entend notamment s'appuyer sur les technologies innovantes telles que les

---

[2142] Règlement du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché unique intérieur et abrogeant la directive 1999/93/CE, *JOUE* du 28 août 2014, L 257/73.

[2143] Directive (UE) 2016/1148 du parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, *JOUE* 19 juill. 2016, L 194/1.

[2144] « Permettre la transformation numérique des services de santé et de soins dans le marché unique numérique ; donner aux citoyens les moyens d'agir et construire une société plus saine », Communication de la commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions adoptée le 25 avr. 2018, COM (2018) 233 final.

[2145] *Ibid.,* p. 4.

[2146] « Permettre la transformation numérique des services de santé et de soins dans le marché unique numérique ; donner aux citoyens les moyens d'agir et construire une société plus saine », Communication de la commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions adoptée le 25 avr. 2018, COM (2018) 233 final, p. 5.

blockchains et les techniques les plus récentes de gestion des identités en favorisant les mécanismes de certification[2147]. Ce virage implique évidemment une normalisation technique dont la certification n'est que, si l'on peut dire, la vitrine. Bien sûr, le marché unique numérique en santé ne suppose pas seulement la circulation des données de santé, il s'étend aux patients[2148] et par exemple aux dispositifs médicaux[2149]. Ce marché va donc être mis en oeuvre sur la base des quatre libertés de circulation mais demeure principalement axés sur la coopération des Etats et leur politique publique[2150] pour les raisons d'articulation des compétences évoquées en amont[2151]. La normalisation constitue donc un instrument essentiel de la conduite de la politique de l'Union pour parvenir à construire un marché unique du numérique dans le domaine de la santé. Ce modèle de gouvernance n'est pas nouveau au sein de l'Union européenne. Monsieur Van Waeyenberge a retracé le contexte dans lequel la normalisation européenne, dans le cadre de la « nouvelle approche », a permis la réalisation du marché intérieur[2152]. La normalisation apparaît, selon cet auteur, comme « *un instrument d'harmonisation des politiques publiques dans le cadre de la* « Nouvelle Approche » *pour laquelle la réglementation fixe un cadre, et la normalisation fournit des exigences techniques permettant de revendiquer la conformité*

[2147] *Ibid.* p. 7.
[2148] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (*JO L* 88 du 4 avril 2011).
[2149] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avr. 2017 relatif aux dispositifs médicaux (*JO L* 117 du 5 mai 2017) ; Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro (*JOL* 117 du 5 mai 2017).
[2150] N. DE GROVE-VALDEYRON, « Politique de santé de l'Union européenne et transformation numérique des soins : quels enjeux pour quelle compétence ? », *op. cit.* C'est la méthode dite de « de coordination ouverte » qui a pour « *objectif d'avancer dans la voie de l'hamonisation entres les Etats membres sans les domaines où l'Union ne possède pas de compétnces spécifiques et là où les blocages politiques ne permettent pas d'avancer selon les voies des procédures de décisions classiques* » (B. FRYDMAN, « Prendre les standards et les indicateurs au sérieux », *in Gouverner par les standards et les indicateurs : De Hume aux Rankings*, coll. Penser le droit, Bruylant, 2013, p. 45 et svt).
[2151] V. ce sens notamment M. THONNET « Santé, numérique, droit-s et Europe : interactions et conséquences », *in* I. POIROT-MAZERES (ss. la dir.) , *Santé, numérique et droit-s*, Actes du colloque des 7 et 8 septembre 2017, Université Toulouse 1 Capitole, coll. IFR actes de colloques, Pressses de l'Université Toulouse I Capitole, LGDJ, 2018, p. 61 et svt.
[2152] A. VAN WAEYENBERGE, « Les normes ISO, CEN et celles issues de consortiums privés : bric à brac ou système pour l'Union européenne », *in* B. FRYDMAN et A. VAN WAEYENBERGE, *Gouverner par les standards et les indicateurs : De Hume aux rankings*, *op. cit.*, p. 10 et svt.

réglementaire »[2153], ce qui est d'ailleurs explicitement rappelé au sein du règlement (UE) n° 1025/2012 relatif à la normalisation européenne[2154].

L'avis récent du Conseil économique, social et environnemental[2155] permet de compléter l'ébauche de ce qui se joue actuellement sur le plan européen. Il y est notamment proposé, afin de permettre le bon fonctionnement du marché unique européen, de procéder à une « *accélération du processus de normalisation en matière de technologies numériques à l'échelle de l'UE : alors que les normes s'élaborent souvent aujourd'hui en dehors de l'UE sous l'impulsion des acteurs industriels, au risque de saper la compétitivité industrielle européenne, il s'agirait de donner à l'Union la capacité d'identifier les normes technologiques qu'elle juge essentielles pour le passage au numérique de son industrie et de ses services* »[2156]. Il s'agit désormais de voir, comment, sur le plan national, les normes techniques sont également mobilisées comme outils de gouvernance des données dans le domaine de la santé.

B - Des instruments de l'action publique pour le numérique en santé

428. Stratégie nationale du numérique en santé. La création d'un marché unique du numérique en santé n'est possible que si les Etats développent leurs propres politiques de transformation numérique, mais l'enjeu n'est pas seulement celui de l'Union. La souveraineté numérique est également un enjeu national qui se traduit, comme au niveau européen, par une course à l'innovation industrielle. La France a mis en œuvre plusieurs stratégies pour le numérique en santé[2157], afin de pouvoir garantir l'interopérabilité, qui conditionne le partage et

---

[2153] O. PEYRAT et J.-F. LEGENDRE, « Quel est l'apport d'une norme volontaire dans le domaine du numérique ? Pourquoi les acteurs s'y interessent-ils ? », *in Normaliser le numérique ?* série *Enjeux numériques*, Annales des Mines, 5 mars 2019, p. 9.

[2154] Consid. 19, 22 et 25 PE et Cons., Règlement (UE) nº 1025/2012 du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du parlement européen et du conseil et abrogeant la décision 87/95/CEE du conseil et la décision nº 1673/2006/CE du parlement européen et du conseil.

[2155] B. THIEULIN, *Pour une politique de souveraineté européenne du numérique*, *op. cit.*

[2156] *Ibid.* p. 33.

[2157] Plusieurs plans nationaux dessinent la stratégie française du numérique en santé, dont par exemple : le programme hôpital numérique, lancé en 2012 et piloté par la Direction générale de l'offre de soin et dont le déploiement était confié conjoitement à la délégation et à la stratégie des systèmes d'information de santé à l'Agence nationale d'appui à la performance des établissements de santé et médico-sociaux et à l'Agence des systèmes d'informations partagées en santé (ASIP-Santé) ; le programme « Territoire de Soins Numérique » 2014-2017 ; la Stratégie nationale E-santé 2020 ; et plus récemment le plan Ma Santé 2022 qui contient un volet numérique important.

l'échange des données sur l'ensemble du territoire, et d'harmoniser les mesures de sécurité et de confidentialité. Il s'agit, selon le discours politique, à la fois de « *protéger et décloisonner les données* »[2158]. La *gouvernance du numérique* passe donc par le fait d'assurer de manière uniforme la *conformité* aux dispositions relatives à la protection des données et, partant, d'assurer par les moyens techniques et organisationnels le respect du secret professionnel et la protection des données couvertes par le secret professionnel.

429. Des normativités diverses, instruments des politiques publiques pour la confiance dans le numérique en santé. Les instruments de l'accélération du numérique en santé sont évoqués dans les documents publics relatifs à la stratégie nationale du numérique en santé : référentiels et normes techniques et de gestion. La souplesse de ces instruments permet une adaptation rapide aux évolutions techniques[2159] mais cette « *normativité plus proche du réel* »[2160] permet surtout une gouvernance efficace[2161] dans la mesure où leur élaboration ne répond pas à une approche classique. Qu'il s'agisse des référentiels ou guides de bonnes pratiques dispensés par l'ASIP-santé ou des normes technico-managériales nationales, européennes ou internationales, elles répondent toutes à un *mode participatif d'élaboration*, trait saillant de la gouvernance[2162]. Si les premières sont des marques du passage de la

---

[2158] Edito de la ministre des Solidarités et de la santé, Dossier d'information, Conférence ministérielle du 25 avril 2019, Feuille de route « Accélération du virage numérique » Ma Santé 2022, p. 3.

[2159] Sur les intérêts des normes techniques (désignées sous le terme générique de *standards*) pour la gouvernance internationale en raison de leur flexibilité et de leur souplesse, v. L. BOISSON DE CHAZOURNES, « Standards, régulation internationale et organisations », *in* B. FRYDMAN et A. VAN WAEYENBERGE (ss. la dir.) , *Gouverner par les standards et les indicateurs : De Hume aux rankings*, *op. cit.*, p. 73 et svt.

[2160] L'expression est empruntée à un auteur qui l'utilise davantage pour qualifier ce qu'il nomme la normativité en flux dont il explique qu'elle participe de la gouvernance par les indicateurs (E. NICOLAS, « Chapitre 10. De la norme aux flux normatifs », *in* J. LE GOFF et S. ONNEE (ss. la dir.), *Puissance de la norme. Défis juridiques et managériaux des systèmes normatifs contemporains*, coll. Gestion en liberté, EMS Editions, 2017, p. 187) mais les indicateurs et les normes techniques ont en commun cette adaptabilité aux mouvements de la réalité.

[2161] Evoquant plus largement « *les techniques normatives du quotidien* » Catherine Thibierge explique que ces types de normativités, dont les normes techniques, sont des instruments des politiques publiques (C. THIBIERGE, « Les « normes sensorielles » », *RTD civ.* 2018, p. 567). L'Organisation internationale de normalisation et la Commission Electronique internationale font elles-mêmes la *promotion* de cette fonction des normes techniques v. ISO/IEC, *Le recours et la référence aux normes ISO et IEC dans les politiques publiques*, 2015, disponible sur < https://www.iso.org/files/live/sites/isoorg/files/store/fr/PUB100358_fr.pdf > (dernière consultation le 10 août 2019).

[2162] La gouvernance désigne un mode de gouvernement ouvert qui se caractérise par une approche qui part « *davantage de la base que du sommet* » (*Gouvernance européenne*, *un livre blanc*, COM (2001) 428 final, p. 12 et 4.

règlementation à la régulation[2163], les secondes sont les outils idéaux de la compliance au RGPD grâce au caractère volontaire de leur application. L'on peut ainsi lire dans le document de présentation de la Stratégie nationale E-santé 2020 que la sécurité des systèmes d'information s'accompagne de la mise en œuvre de la Politique Générale de Sécurité des Systèmes d'Information de Santé[2164] – que nous avons déjà cité afin de mettre en lumière la normalisation de la sécurité des systèmes, des réseaux et des échanges dans le domaine de la santé et dont nous verrons qu'elle s'accompagne de normes technico-managériales internationales. L'intérêt de la normalisation dans la transformation numérique du système de santé national est exprimé çà et là dans le discours politique. Il est notamment prévu, dans le cadre de la stratégie *Ma santé 2022*, de normaliser sur l'ensemble du territoire national la généralisation de l'identification des acteurs du système de santé – identification nécessaire afin de vérifier que les données sont bien transmises à des personnes autorisées[2165]. Il en est de même pour les services et outils qui intègreront l'Espace numérique de Santé, lesquels devront être labellisés au regard de normes relatives à la sécurité et à l'interopératbilité[2166] ; il encore précisé qu'un « *référentiel et un dispositif de certification devront être élaborés en concertation avec les parties prenantes concernées. Ce référentiel et ce dispositif s'appuieront sur un ensemble de normes (ISO) et d'exigences déjà existantes, dans l'objectif d'accompagner la modernisation des établissements de santé dans un cadre de qualité reconnue* »[2167]. Lors de son intervention de présentation de la stratégie pour l'accélération du virage numérique dans le domaine de la santé, Madame la Ministre Agnès Buzin souligne encore qu'il s'agit de « *mettre en place des actions concrètes pour que les systèmes d'information évoluent vers plus de sécurité et d'interopérabilité tout en ne les figeant pas dans des normes qui immobiliseraient les*

[2163] La régulation fonctionne « *par persuasion d'un modèle* » là ou la règlementation opère par un « *commandement sans réplique* » (J. CARBONNIER, *Sociologie juridique*, coll. Quadrige, PUF, 2004, p. 146).
[2164] Ministère des affaires sociales et de la santé, *Stratégie nationale e-santé 2020. Le numérique au service de la santé et de l'efficience du système de santé*, 4 juillet 2016, p. 16. Notons à titre indicatifs, car cela dépasse le cadre de notre étude, que la stratégie vise également à utiliser les données à des fins de régulation notamment en matière de veille sanitaire. Cela répond à la logique de gouvernance par les indicateurs et participe, dans un secteur certes bien précis, du *mathématical turn* décrit par David Restrepo Amariles dans le champ plus vaste du développement de la banque mondiale (D. RESTREPO AMARILES, « *The matematical turn* : l'indicateur Rule of Law dans la politique de développement de la Banque Mondiale », *in* B. FRYDMAN et A. VAN WAEYENBERGE (ss. la dir.) , *Gouverner par les standards et les indicateurs : De Hume aux rankings*, *op. cit.*, p. 193.
[2165] Ma santé 2022, Feuille de route « Accélérer le virage numérique », Dossier d'information, Conférence ministre, 25 avril 2019, p. 14, disponible sur <https://solidarites-sante.gouv.fr/IMG/pdf/190425_dossier_presse_masante2022_ok.pdf > (dernière consultation le 10 août 2019).
[2166] *Ibid.,* p. 9.
[2167] *Ibid.,* p. 23.

initiatives ». Faire le lien entre les instruments de normalisation et la politique nationale permet de souligner l'importance de l'étude du phénomène de normalisation non pas seulement en tant que normes ayant pour objectif de réaliser la *privacy by design* mais comme *instrument susceptible de créer de la confiance dans les dispostifs techniques* en ce qu'elles contribuent à garantir la sécurité et la confidentialité et donc le respect du secret des données couvertes par le secret professionnel dans le domaine de la santé. Générer la confiance est, en outre, l'une des conditions qui préside à l'objectif de faire des données produites à l'occasion des soins des *communs*. Il faut désormais présenter brièvement les acteurs qui participent de la gouvernance du numérique en santé.

430. Les acteurs étatiques en charge d'élaborer « *un socle de confiance* »[2168] dans le numérique en santé. La sécurité et la confidentialité des traitements de données ne peuvent être assurées que si les systèmes d'information supportant les traitements et assurant les échanges répondent aux exigences de sécurité. Les moyens techniques et organisationnels doivent ainsi permettre « *l'adaptation des systèmes informatiques et des pratiques* »[2169]. L'ASIP-santé, agence de l'Etat, assure le rôle d'expert en matière de sécurité des systèmes d'information de santé. Comme d'autres agences, elle participe à la gestion du risque[2170], le risque étant ici informationnel[2171]. Elle prend part à la réalisation des politiques de santé en mettant en place « *le socle technique et juridique indispensable pour permettre le*

[2168] C'est ainsi que l'ASIP-santé présente ses missions : v. < https://esante.gouv.fr/asip-sante/qui-sommes-nous> (dernière consultation le 7 oct. 2019). Sur ce qu'implique la construction de la confiance dans le numérique en santé.

[2169] L. CLUZEL-METAYER, « Les téléservices publics face au droit à la confidentialité des données », *RFAP*, 2013/2, n° 146.

[2170] Sur le rôle des agences dans la gestion du risque (et particulièrement en matière sanitaire et environnementale), v. V. LASSERRE, *Le nouvel ordre juridique. Le droit de la gouvernance*, LexisNexis, 2015, n° 61 et svt.

[2171] Le risque informationnel se traduit, en matière de données à caractère personnel et particulièrement dans le domaine de la santé, comme le risque d'atteinte à la vie privée (C. ZOLYNSKI, « La Privacy by Design appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel ? », *Dalloz IP/IT* 2016, p. 404 ; E. RIAL-SEBBAG, « Chapitre 4. La gouvernance des Big data utilisées en santé, un enjeu national et international », *Journal international de bioéthique et d'éthique des sciences* 2017/3, vol. 28, p. 39). L'analyse du risque en matière de système d'information a une filiation étroite avec le domaine de l'assurance puisque c'est dans ce domaine que la promotion de la sécurité des SI s'est développée dans les années 1980. Sans faire de déduction hâtive, l'on ne peut que remarquer le lien entre ce fait et la logique actuarielle qui guide actuellement les dispositions relatives à la protection des données (A propos de l'analyse des risques en matière de système d'information v. *Lamy droit du numérique* (collectif), Partie 6, Titre 2, « Comment sécuriser les systèmes et les réseaux ? », n° 2862 et svt).

développement de la santé numérique »[2172] , développement initié par la politique européenne et nationale évoquée en amont. A ce titre, l'ASIP-santé élabore, avec la CNIL et d'autres acteurs[2173], des référentiels, et procède à la certification et à la labellisation de produits dans le domaine de la sécurité des systèmes d'information et des dispositifs utilisés en santé[2174]. Elle a, entre autres, mis en place un référentiel d'interopérabilité et de sécurité des systèmes d'information en santé[2175] et défini une politique générale de sécurité des systèmes d'information de santé, laquelle rassemble des « *référentiels d'exigences, des guides de bonnes pratiques et propose un cadre commun de niveau de sécurité des SI du secteur de la santé* »[2176]. Ces instruments participent de la démarche *Privacy by design* en ce qu'ils permettent notamment aux industriels de développer des produits en tenant compte des exigences de sécurité et de confidentialité, de même que la certification permet de garantir que le respect des dispositions relatives à la protection des données et les exigences de sécurité sont assurées dès la conception et dans l'architecture des réseaux[2177]. L'expression employée dans le vocabulaire des techniciens de l'informatique, « *security et privacy by design* »[2178], est révélatrice : elle rappelle que la sécurité et la confidentialité sont deux facettes d'un même objectif. A côté de l'ASIP-santé, d'autres acteurs publics ont un rôle dans la conduite de la politique de transformation numérique de la santé, comme c'est le cas de la Haute autorité de santé et de l'ANSM, notamment pour les dispositifs médicaux connectés, et, évidemment, la CNIL.

431. Conclusion du premier chapitre. Des normes étrangères au droit sont produites afin d'assurer la réservation des données ou, du moins, d'assurer l'état secret. La cybersécurité est

---

[2172] M. GAGNEUX, « Santé numérique : l'interopérabilité au service des usages de demain », *I2D – Information, données & documents* 2016/3, vol. 53, p. 46).

[2173] La politique générale de securité des systèmes d'information de santé a notamment été élaborée avec la Caisse nationale de solidarité pour l'autonomie (CNAM) et l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

[2174] « *L. 1110-4-1 du code de la santé publique issu de la loi n° 2016-41 du 26 janvier 2016, prenant la suite de la loi Hôpital Patients Santé et Territoires de 2009 consacre une assise législative unique aux référentiels de sécurité et d'interopérabilité que les responsables de systèmes d'information sont tenus de respecter. Ils sont définis par l'ASIP Santé et approuvés par voie d'arrêté pris par le ministre en charge de la santé après avis de la CNIL et publiés au Journal officiel* » (J. BOSSI MALAFOSSE, « Le règlement européen et la protection des données de santé », *Dalloz IP/IT* 2017, p. 260). Nous reviendrons sur l'article L. 1110-4-1 du Code de la santé publique tel qu'il a été modifié par la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (*JORF* n° 0172 du 26 juillet 2019).

[2175] Dont le corpus documentaire figure sur le site de l'ASIP-Santé : <https://esante.gouv.fr/interoperabilite/ci-sis> (dernière consultation le 7 oct. 2019).

[2176] Disponible sur <https://esante.gouv.fr/securite/pgssi-s/espace-de-publication> (dernière consultation le 7 oct. 2019).

[2177] O. TAMBOU, « L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ? », *RLDI*,1er avril 2016, n° 125.

[2178] Les 22 et 23 janvier 2019 a eu lieu la 11ème édition du Forum International de la Cybersécurité sur le thème ««« Security et Privacy by design ».

un domaine totalement investi par les normes techniques, mieux adaptées aux enjeux du cyberespace. Le concept de *Privacy by design,* en tant qu'il implique d'intégrer le respect de la vie privée des personnes dès la conception des objets techniques, constitue également un socle pour la prolifération de ces normes. Bien sûr, la machine ne peut encore fonctionner sans l'humain mais même les comportements humains, les usages que ces derniers font des technologies, sont désormais normalisés. Il importe que ce que la machine fait l'humain ne le défasse pas. La normalisation managériale consiste en une approche en termes de risque, humains et techniques. Le domaine de la santé est particulièrement concerné, la sensibilité des données impose au responsable de traitement de procéder à une analyse de risque.

Les raisons de cette normalisation tiennent encore aux enjeux économiques et politiques européens et nationaux dans un contexte de concurrence mondiale. Il s'agit de maximiser les utilités des données pour soutenir l'innovation et donc l'économie, tout en préservant la confiance des individus. La réalisation de ces objectifs est en partie assurée par les normes technico-managériale. Au niveau européen, ces normes permettent une harmonisation sur tout le territoire de l'Union dans des domaines où elle n'a qu'une compétence d'appui. Sur le plan national, les normes de droit souple constituent un maillage dense visant à créer la « confiance dans le numérique ». L'ASIP-santé est au premier plan de la mise en œuvre de cette politique.

Chapitre 2 - L'influence de la diversification des dispositifs normatifs

432. La concurrence des normes, effet d'un enchevêtrement normatif. Les développements qui précèdent nous conduisent à revenir sur la question de la place du droit dans l'espace normatif : il est devenu de plus en plus difficile de trouver un consensus sur la définition du droit[2179] et, partant, de distinguer les règles juridiques dans un monde saturé de normes[2180]. Ce mouvement amène naturellement à en évoquer un autre, lié. La doctrine – dont, parmi les plus cités, Jean Carbonnier – a depuis longtemps constaté des phénomènes d'internormativité[2181]. Selon cet auteur « *entre le droit et les autres systèmes normatifs, des rapports se nouent et se dénouent, des mouvements, des conjonctions, des conflits se produisent. Ce sont là des phénomènes autonomes : les phénomènes d'internormativité* »[2182]. Le terme d'*internormativité* a, à sa suite, été largement utilisé par les juristes pour désigner ces rapports mais comme le souligne Monsieur Ost, l'idée du premier auteur était de décrire « *la capacité de l'ordre juridique de* « faire siennes » *des normes empruntées aux systèmes normatifs les plus divers, les marquant ainsi de son sceau, notamment en assortissant généralement leur violation d'une sanction organisée* »[2183]. Or, les rapports entre les différents systèmes normatifs – si l'on s'accorde à considérer qu'il existe des *ordres* ou des *systèmes* de cette nature[2184] – ne consistent pas seulement en une intégration, par le droit, des normes ou des autres dispositifs normatifs[2185], mais nécessiteraient sans doute d'être « *multilatéralisés* »[2186]. Le même auteur évoque ainsi une « *intrication des logiques* »[2187], raison pour laquelle il préfère employer l'expression

---

[2179] On prendra comme illustration la multitude de définitions du droit données par une quarantaine d'universitaires de renom dans deux numéros de la revues *Droits* (*Droits*, n°10 et n°11, 1989 et 1990).
[2180] C. THIBIERGE *et alii*, *La densification normative. Découverte d'un processus*, Mare&Martin, 2013. Monsieur Ost explique que cet état de fait ne signifie pas la disparition du droit (F. OST, *A quoi sert le droit ? Usages, fonctions, finalités*, coll. Penser le droit, Bruylant, 2016, p. 6). D'un point de vue méthodologique, l'hypothèse d'une complète dilution du droit dans l'ensemble de la normativité sociale aurait pu conséquence d'empêcher toute tentative d'analyse : « *si d'emblée* « tout est dans tout », *on voit mal comment on pourrait progresser* » (*Ibid*., p. 115).
[2181] J. CARBONNIER, « Les phénomènes d'internormativité », *in* J. CARBONNIER, *Essais sur les lois*, Defrénois, 1979, pp. 253-270.
[2182] *Ibid.*
[2183] F. OST, *A quoi sert le droit ? Usages, fonctions, finalités*, *op. cit.*, p. 114.
[2184] Notons que Monsieur Ost utilise le terme de *dispositif normatifs* : « […] *ces autres dispositifs normatifs, la religion, le politique, l'économie...* » (*Ibid.,* p. 104).
[2185] Ce qui conduit déjà à affirmer que le droit connaît de nouvelles sources.
[2186] F. OST, *A quoi sert le droit ? Usages, fonctions, finalités*, *op.cit.*, p. 114.
[2187] *Ibid.* p. 118.

« *enchevêtrement normatif* »[2188] à celle d'internormativité. Ce phénomène d'entrelacement n'est qu'une des façons de penser les rapports entre les différents dispositifs normatifs. Avant de l'envisager, Monsieur Ost explique que ces dispositifs sont en concurrence au sein d'une « *lutte globale pour la culture* »[2189]. Il considère néanmoins que si cette lutte peut se solder par « *une hégémonie sans partage* »[2190] de l'un de ces dispositifs ou s'exprimer par une « *étanchéité parfaite* »[2191] entre eux, seule l'hypothèse de leur enchevêtrement est réaliste[2192]. Un exemple illustratif de ce phénomène de concurrence et d'enchevêtrement des normes est la montée en puissance des normes techniques et managériales[2193]. Il s'agit désormais, pour percevoir le phénomène au regard de notre objet, de resserrer quelque peu notre analyse.

La protection du secret des données issues de la prise en charge des personnes dans le système de santé et le respect du secret professionnel sont assurés par des normes dont la nature interroge car, selon la vision du droit que l'on emprunte, ces normes peuvent être considérées comme appartenant à d'autres systèmes de normes. Si nous avons jusqu'alors procédé à des

---

[2188] *Ibid.* p. 111 et svt.

[2189] Ne souhaitant pas dénaturer les propos de l'auteur s'agissant que ce qu'il entend par cette expression nous souhaitons les reproduire ici : « *J'ai précisé d'emblée que le droit n'avait pas le monopole des finalités extrinsèques retenues (ce qui, du reste, constitue un motif supplémentaire de ne pas les identifier au droit) très bien ; mais alors on devra se demander quels sont les autres dispositifs normatifs (macrodiscours sociaux) qui les poursuivent également et ces autres dispositifs normatifs, la religion, le politique, l'économie..., ne poursuivent-ils pas eux-mêmes d'autres inégalités, qui entrent en concurrence avec les premières ? et puis encore : dans leur quête commune, ces macrodiscours sociaux collaborent-ils harmonieusement, ou se livrent-ils une guerre plus ou moins déclarée ? Cet ensemble de questions, dont on devine qu'elles dépassent les compétences d'un seul homme, se réclamerait-il même de l'interdisciplinarité, touche au problème du contrôle global de la culture d'une société donnée – j'entends par « culture » la synthèse la plus vaste qu'il soit possible de concevoir de l'ensemble de ses productions langagières, scientifiques, spirituelles, normatives et artistiques autrement dit, la question est de savoir quel discours global « donne le ton » dans une culture donnée à tel moment de son histoire . Quel est le dispositif dominant, quelles sont les finalités qu'il poursuit, et que deviennent les autres discours et pratiques durant cette période den dominance ? Je pars de l'hypothèse que l'homme en société développe un certain nombre de besoins, mais aussi de capacités, qui débouchent sur un petit nombre de dispositifs primitifs (discours, pratiques, institutions, professions, réalisations, principes de jugement, etc .): besoins et capacités de spiritualité débouchant sur les religions, les sagesses et les systèmes éthiques ; besoins et capacités d'interactions débouchant, dans la société, sur les coutumes et les mœurs, et, dans la cité, sur le politique ; besoins et capacités de connaissance produisant les savoirs traditionnels, puis les sciences ; besoins et capacités d'imaginaire et de fiction générant la littérature et les arts ; besoins et capacités d'échanges débouchant sur l'économie ; besoins et capacités d'objets et de procédés à l'origine des techniques... Je ne m'aventurerai pas à décider si certains besoins sont plus primitifs que d'autres, et si oui, dans quel ordre ils apparaissent (à supposer que partout s'observe la même progression)* » (F. OST, *A quoi sert le droit ? Usages, fonctions, finalités*, *op. cit.*, pp. 104-105).

[2190] *Ibid.* p. 106 et svt.

[2191] *Ibid.* p. 109 et svt.

[2192] *Ibid.* p. 106.

[2193] L'ouvrage de référence sur la question, auquel nous nous réfèrerons est celui de B. FRYDMAN et A. VAN WAEYENBERGE (ss la dir.), *Gouverner par les standards et les indicateurs. De Hume au rankings*, coll. Penser le droit, Bruylant, 2014.

articulations entre des normes dont la nature juridique ne fait pas de doute, d'autres normes, dont la nature pose question, sont désormais à l'œuvre dans les interstices laissés par le retrait progressif du secret professionnel. L'on constate, entre ces normes, un entrelacement, qu'il faut tenter d'expliquer **(section 1)**. Au travers de certaines de ces normes, le droit a vocation à migrer dans les objets techniques. Ce mouvement, dont l'analyse relève de la théorie du droit, est encore relativement peu étudié. Il nous faudra en décrire les linéaments et se risquer à une évaluation au regard de la notion de « secret médical » **(section 2)**.

Section 1 - L'interaction des normativités en matière de protection des données dans le domaine de la santé

433. Nous avons déterminé qu'il existait des secrets professionnels de « premier rang » et des secrets professionnels de « second rang »[2194]. L'on observe que la technique de pseudonymisation réalisées grâce aux techniques de l'information, permet de hiérarchiser les secrets, ce phénomène pourrait correspondre à une forme d'interaction normative **(paragraphe 1).** L'on remarque ensuite un enchevêtrement des normes techniques et des normes juridiques, au niveau national et européen **(paragraphe 2)**.

§ 1 - La pseudonymisation, moyen de hiérarchisation des secrets professionnels

434. La particularité de la régulation opérée par les autorités administratives indépendantes tient dans l'intervention *ex ante* du régulateur, c'est-à-dire « *en partant de ce qui est avant* ». Le passage de la régulation à la *compliance*, qui consiste en une co-régulation entre les acteurs et le régulateur. Toutefois, dans les développements qui vont suivre, il importe peu de chercher à déterminer les conséquences du passage de la régulation à la *compliance*. En toutes hypothèses, l'obligation de sécurité et de confidentialité, que sa mise en œuvre conditionne le traitement ou que le fait de « *ne pas avoir mis en place un dispositif efficace pour prévenir le risque* »[2195] engage la responsabilité du responsable du traitement, impose que des moyens soient pris par le responsable de traitement. C'est la façon dont le droit s'est saisi de ces techniques, et particulièrement les conséquences que cela emporte sur la qualification des

[2194] V. *supra* n° 305.
[2195] A. GAUDEMET, « Qu'est-ce que la compliance ? », *Commentaire* 2019/1, n° 165, p. 110.

données de santé, qui nous intéresse. Nous avons expliqué, à l'occasion de l'examen des décisions et avis de la CNIL, que le secret professionnel constituait un *outil* pour les acteurs et pour le régulateur (qui se plaçait comme tel en raison de la permanence de son action) afin de mettre en œuvre la confidentialité. La soumission au secret professionnel des destinataires est alors un critère d'appréciation du respect de l'obligation de sécurité et de confidentialité par le responsable de traitement[2196]. Nous avons ajouté qu'il en est résulté une généralisation du secret professionnel à des fins de réutilisation de ces données couvertes par le secret. La technique intervient alors comme un mode de hiérarchisation des secrets professionnels permettant de différencier les droits d'accès aux données au regard du risque de réidentification des personnes.

A - L'utilisation de la pseudonymisation

435. L'anonymisation et la pseudonymisation. La notion d'anonymisation a été évoquée à plusieurs reprises au cours des précédents développements[2197]. Le terme, s'il est relativement récent[2198], renvoi au fait de rendre anonyme, un document, une image, une vidéo, des données. Il s'agit de supprimer les éléments d'identification de la personne à laquelle se rattachent les informations, quelle que soit leur forme. La suppression de ces éléments peut s'effectuer manuellement, avec ou sans l'aide de l'outil informatique, par suppression de ces éléments sur un document ou une image. Ce procédé, lorsqu'il est étudié dans le cadre traditionnel des droits de la personnalité, consiste en « *un mode de conciliation des intérêts en présence* »[2199]. Dans le contexte du traitement de données, l'anonymisation emporte pour conséquence de soustraire le traitement aux dispositions organisant la protection des données à caractère personnel : dès lors qu'elles sont anonymes, elles ne peuvent être qualifiées de données à caractère personnel. Il importe toutefois que toute réidentification ultérieure soit impossible[2200]. C'est pourquoi la CNIL considère que l'anonymisation est un moyen de préserver le « secret médical »[2201] et la

---

[2196] V. *supra,* n°186.
[2197] Afin de la différencier de la liberté de demeurer anonyme (*supra* n° 117) et au regard de la définition des données à caractère personnel (*supra* n° 144).
[2198] Le mot n'est entré dans le dictionnaire *Le Robert* que depuis 2006 et depuis 2012 dans le *Larousse*.
[2199] Concernant par exemple les images, v. A. LEPAGE, *Rép. civ.*, *V°* « Droits de la personnalité », sept. 2009 (actu. mai 2018), n° 358.
[2200] V. *supra* note n° 725.
[2201] La CNIL utilisait encore la formule s'agissant de la transmission des données de santé aux assurances maladies complémentaires : « *Dans la mesure où les données de santé figurant dans les feuilles de soins électroniques relèvent de l'intimité de la vie privée, il convient de concilier l'accès des complémentaires santé à ces données*

condition première de l'*open data* dans le domaine de la santé[2202]. La pseudonymisation est définie par le RGPD[2203] et consiste à retirer les variables directement identifiantes. Celle-ci participe à la confidentialité en ce qu'elle permet de réduire le risque de ré-identification[2204] et, partant, *d'atteinte au secret*, sans pour autant l'évacuer totalement[2205]. Il n'existe pas une mais des techniques de pseudonymisation, toutes ne présentant pas le même risque de réidentification des personnes concernées par les données[2206]. S'agissant particulièrement du traitement des données de santé à caractère personnel, les techniques de pseudonymisation sont davantage sollicitées.

436. Pseudonymisation des données à caractère personnel dans le domaine de la santé : 1er temps. Le codage des données comme méthode de pseudonymisation a été mis en œuvre dès les années 1980 afin de permettre la transmission de données couvertes par le secret ou afin de satisfaire les demandes de transmission de données par une administration dans des hypothèses où la loi ne prévoyait pas explicitement de permission ou d'autorisation de révéler. Certaines mesures, qui ne consistaient pas en une pseudonymisation[2207] – mais avaient vocation à différencier l'accès aux données d'identification et aux données de santé – étaient recommandées par la CNIL, notamment pour permettre l'accès aux données issues de la relation de soin à des professionnels ne participant pas aux soins, sans qu'il soit nécessaire de

---

avec le respect du secret médical […] *À cet effet, un rapport a été établi à la demande du ministre de la Santé en mai 2003 sur ces questions. Il préconise plusieurs solutions juridiques et techniques, parmi lesquelles l'expérimentation d'un procédé de transmission anonyme des données de santé aux assureurs complémentaires* » (CNIL, *Rapport d'activité* 2004, p. 55).

[2202] Rappelons que l'*open data* peut être rattaché au mouvement d'ouverture des données publiques fondé sur la loi n° 78-753 du 17 juillet 1978 relative au droit d'accès aux documents administratifs dont l'article 6 limite la communication des documents administratifs.

[2203] RGPD, art. 4, 5°.

[2204] RGPD, consid. 28.

[2205] Conseil d'Etat, Etude annuelle 2014, *Le numérique et les droits fondamentaux*, coll. Les rapports du Conseil d'Etat, La documentation française, 2014, p. 175, note 289.

[2206] Sont traditionnellement présentés : le hachage, le hachage à clef secrète, le chiffrement déterministe, le codage et la tokenization. A propos de ces techniques, v. notamment G 29, avis 05/2014 sur les techniques d'anonymisation, 10 avr. 2014, WP 216.

[2207] Le terme est d'apparition récente dans la doctrine de la Commission. Les premières occurrences, au sein des avis et décisions, apparaissent en 2009 tandis que les rapports n'en font mention qu'à partir de 2013. Le G29 en fait mention dans ses travaux relatifs à la notion de données de santé en 2007 (G 29, avis 4/2007 sur le concept de données à caractère personnel, 20 juin 2007, WP 136, p. 19), puis dans son avis sur les techniques d'anonymisation en 2014 (G 29, avis 05/2014 sur les techniques d'anonymisation, 10 avr. 2014, WP 216).

ménager une dérogation au secret professionnel[2208]. Le codage était également utilisé et consistait à remplacer l'identité des personnes par un code avant transmission des données, les professionnels de santé prenant en charge les patients conservant alors la table de correspondance contenant l'identité rattachée au code désignant les individus[2209]. La CNIL considérait alors qu'il s'agissait d'une anonymisation. L'évolution des techniques a ensuite imposé de les appréhender comme des techniques de pseudonymisation. De moyen palliatif, la technique est progressivement devenue un instrument de hiérarchisation des secrets.

437. Pseudonymisation et secrets professionnels. Les données issues de la prise en charge des personnes par un professionnel intervenant dans le système de santé revêtent une double qualification : ce sont des données à caractère personnel sensibles et des informations couvertes par le secret en raison de leur source. Lors de l'étude de l'infraction sanctionnant la violation

---

[2208] Parmi de nombreux exemples, Délibération n° 86-112 du 25 novembre 1986 portant avis sur le projet de décision du directeur du Centre hospitalier général d'Auch, concernant la mise en œuvre d'un traitement relatif à la gestion administrative et médicale des malades (GAMMA - Filière PROFILS) Demande d'avis n° 104.209 : « *Considérant que cette conception technique, dans la mesure où elle ne permet pas une séparation des données relatives à l'identité des personnes et des renseignements proprement médicaux, impose l'adoption de dispositifs particuliers de sécurité afin de garantir le respect du secret médical et de la vie privée des patients* » ; Délibération n° 88-46 du 26 avril 1988 portant sur le projet d'arrêté du directeur général de l'Assistance publique de Paris concernant la mise en œuvre, à l'Hôpital Robert Debré, d'un système de gestion administrative et médicale des patients dénommé *patient care system* : « *Considérant que cette conception technique, dans la mesure où elle ne permet pas une séparation des données relatives à l'identité des personnes et des renseignements proprement médicaux, impose l'adoption de dispositifs particuliers de sécurité afin de garantir le respect du secret médical et de la vie privée des patients* ».

[2209] Pour ne donner que quelques exemples : c'est le choix qui a été fait lors de l'expérimentation du PMSI, la décision de la CNIL précisant que les données « *sont identifiées par un numéro dont la correspondance est conservée localement par le médecin précité de la clinique et où d'autre part, les dates d'entrée et de sortie des patients sont recueillies* » (Délibération n° 92-061 du 9 juin 1992 portant avis sur la création à titre expérimental d'un système national d'informations médico-administratives dont la finalité principale est de déterminer en fonction des pathologies et des modes de prise en charge, une classification des prestations d'hospitalisation (expérience PMSI dans les cliniques). S'agissant par exemple de la transmission de données collectées par les médecins lors des examens de santé gratuits proposés aux assurés et à leurs familles et réalisés par les centres d'examens de santé des caisses nationales d'assurances maladies, il était prévu « *que dans les cas où il est fait appel à un laboratoire d'analyses extérieur au centre, la transmission par ce laboratoire des résultats d'analyse pourra s'effectuer par réseau commuté ; que les résultats seront transmis sous forme codée et sans indications nominatives dans le fichier "boîte aux lettres" du système propre à l'exploitation du traitement* » (Délibération n° 86-123 du 16 décembre 1986 portant avis sur le projet de décision du directeur de la Caisse nationale d'Assurance Maladie relative à l'informatisation de la gestion des centres d'examens de santé (Traitement SAGES)). A propos de la mise en œuvre d'un traitement de données pour les personnes hospitalisées à domicile et afin que les acteurs techniques puissent avoir accès aux données, la CNIL propose que « *les informations relatives aux patients soient transmises sans que leurs noms soient communiqués* » (CNIL, *Rapport d'activité 1994*, p. 321). Encore, évoquant le transcodage « *selon un dispositif de codage irréversible, en des numéros non signifiants qui permettront sans réidentification possible de la personne concernée, d'apparier les données relatives aux différentes prestations qui lui ont été servies* » (Délibération n° 88-73 du 21 juin 1988 portant avis sur le projet de décision du Président de l'Association régioale Rhône-Alpes de recherche en gérontologie relative à une recherh épidémiologique sur la maladie d'Alzheimer).

du secret professionnel, il a été mis en exergue le processus de généralisation du secret professionnel, devenu *secret des données issues de la prise en charge des personnes par un professionnel intervenant dans le système de santé*. A cette occasion, quelques interrogations ont été formulées quant au régime attaché à ces secrets professionnels, fondé sur la nature des données traitées. Nous avons également expliqué qu'à côté du secret partagé consacré par le législateur et inscrit dans le Code de la santé publique, il existe une forme de partage technique forcé dont l'origine se trouve dans la définition de la notion de confidentialité, ainsi qu'une multitude de dérogations au secret professionnel. Le dernier élément de ces évolutions se trouve, selon nous, dans l'utilisation des techniques de pseudonymisation et dans leur normalisation. Les données qui font l'objet d'une pseudonymisation demeurent des données à caractère personnel en raison du risque insuppressible de réidentification[2210], et sont toujours considérées comme des données couvertes par le secret, ce qui a notamment nécessité de créer des dérogations au secret professionnel et une extension du champ d'application de l'infraction.

438. Pseudonymisation, utilités des données, sécurité et réutilisation. Notons par ailleurs, en écho à ce que nous avons évoqué plus avant à propos des *Big data*, que si la masse de données importe, la qualité des données est également essentielle à leur utilisation. Ainsi, « *une donnée peut être soit utile, soit parfaitement anonymisée, mais elle ne peut jamais être les deux* »[2211]. Comme le constate Madame Debiès, les données anonymisées (sous forme de statistiques agrégées) ne présentent que peu d'intérêt pour la recherche, c'est pourquoi il est nécessaire de traiter « *des données d'une granularité plus fine qui vont immanquablement poser la question d'un possible ré-identificaton des personnes et conduire à un contrôle d'accès et des finalités* »[2212]. Si la CNIL rappelle que « *Les données pseudonymes ou pseudonymisées ne doivent pas être définies comme une nouvelle catégorie de données permettant de déroger à*

[2210] La question avait néanmoins fait l'objet de discussion au sein du Parlement européen lors de la discussion sur le règlement européen et dont la CNIL s'était fait l'écho à l'occasion de ces rapports annuels de 2013 et 2014 (Cnil, *Rapport d'activité 2013*, p. 30 ; *Rapport d'activité 2014*, p. 62).

[2211] P. OHM, « Broken promises of privacy : responding to the surprising failure of anonymization », *57 UCLA Law Review*, 2010, p.1704 ; - *Adde* L. MAISNIER-BOCHÉ, « Intelligence artificielle et données de santé », Dossier *Intelligence artificielle et santé*, *Journal de Droit de la Santé et de l'Assurance Maladie (JDSAM)*, n° 17, 2017, p. 25.

[2212] E. DEBIES, « L'incertitude de l'anonymisation face à l'ouverture des données de santé », *in* D. BOURCIER et P. DE FILIPPI (ss. la dir.), *Open data et Big data*. *Nouveaux défis pour la vie privée*, coll. Droit & Science politique, Mare&Martin, 2016, p. 86.

certaines obligations définies par le règlement [, l]*a pseudonymisation constitue uniquement une mesure de sécurité* »[2213], il nous semble toutefois que s'agissant des données issues de la prise en charge des personnes dans le système de santé, la pseudonymisation est également un outil de hiérarchisation des secrets professionnels. Concernant la réutilisation des données issues de la prise en charge des personnes dans le domaine de la santé, la pseudonymisation constitue en effet une garantie jugée appropriée pour permettre de « *déterminer le caractère compatible de la finalité secondaire d'un traitement avec sa finalité initiale* »[2214]. L'on constate ainsi que toutes les personnes soumises au secret professionnel et qui peuvent avoir accès à certaines données – qui sont donc des tiers autorisés – ne traitent néanmoins pas des données personnelles directement identifiables. Une hiérarchisation des secrets professionnels s'effectue donc au regard d'une graduation du risque de réidentification.

439. Point de départ : L'ancien article 55 de la LIL et le codage des données. Nous avons évoqué l'extension du secret professionnel à toutes les personnes susceptibles de réutiliser des données issues des soins et transmises sur le fondement de la dérogation prévue par la loi du 1er juillet 1994[2215]. L'ancien article 55 plusieurs fois modifié – devenu l'article 68 de la LIL à l'occasion de la dernière ordonnance – prévoyait que les données en question devaient être codées avant transmission aux organismes de recherche[2216]. La version actuelle ne contient plus explicitement la mention du codage mais précise simplement que « *lorsque ces données permettent l'identification des personnes, leur transmission doit être effectuée dans des conditions de nature à garantir leur confidentialité* »[2217]. Il convient de retenir de ce premier temps que, malgré la soumission au secret professionnel des personnes susceptibles de réutiliser les données normalement couvertes par le secret et l'édiction du fait justificatif, le codage des données et donc, leur pseudonymisation, est demeurée une condition de transmission[2218].

[2213] CNIL, *Rapport d'activité 2015*, p. 75.
[2214] F. LESAULNIER, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p. 573.
[2215] V. *supra* n° 333. Loi n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* n°152 du 2 juillet 1994 p. 9559.
[2216] Pour un exemple : CNIL, Délibération n° 89-90 du 12 septembre 2009, portant avis sur le projet d'arrêté du président du conseil général Bouches-du-Rhône concernant la mise en œuvre au sein du dispensaire antivénérien d'un traitement relatif à la gestion des données médicaux et à la production de données statistiques.
[2217] LIL, art. 68, al. 2.
[2218] Cette condition était alors accompagnée d'un certain nombre d'exceptions : H.-J. LUCAS et I. DE LAMBERTERIE, *Informatique, libertés et recherche médicale*, coll. CNRS Droit, CNRS éd., 2001, n° 384 ; I. COULIBALY, *La protection des données à caractère personnel dans le domaine de la recherche scientifique*, th. dact., ss. la dir. de E. VERGES et I. DE LAMBERTERIE, soutenue le 25 nov. 2011, Université de Grenoble, p. 418 et svt. A noter que l'auteur n'opère aucune distinction sur la fonction du codage avant 1994 et après.

Partant, le codage nous semble être un instrument de hiérarchisation des secrets professionnels, entre les acteurs soumis au secret, car intervenant dans la prise en charge des personnes, et ceux soumis au secret afin de favoriser la réutilisation des données.

B - Graduation et hiérarchisation

440. Il nous faut à présent décrire spécifiquement ce mouvement **(1)**, mettre en exèrgue les illustrations **(2)** au regard desquelles nous formulerons remarques **(3)**.

1 - Mouvement

441. Pseudonymisation et accès gradué aux données. Le choix effectué par le législateur, à l'occasion de la loi du 26 janvier 2016, de procéder à une différenciation des accès au regard de la qualification des données – des données personnelles de santé aux données anonymes – et des finalités[2219] révèle un processus de hiérarchisation. La limitation des accès va, en effet, croissante au regard de la sensibilité des données et des finalités, de l'*open data* aux accès temporaires puis permanents. A l'occasion d'un article publié en 2009, Monsieur Py a proposé de modifier le texte d'incrimination de l'article 226-13 du Code pénal en procédant à une *hiérarchisation des personnes, des informations et des dérogations*[2220]. Il s'agissait de prévoir une habilitation spécifique des personnes « *pour accéder à tel ou tel niveau d'information* ». En d'autres termes, il s'agissait d'une *double graduation* : graduation des personnes en fonction du besoin qu'elles ont de connaître des informations, et graduation des informations qui peuvent être connues par elles au regard de ce même besoin. Pour illustrer son propos, l'auteur a pris pour exemple la hiérarchisation définissant l'accès aux informations classifiées au titre de la défense nationale[2221]. La logique de graduation des accès aux données issues de la prise en charge des personnes par des professionnels intervenant dans le système de santé est comparable à la hiérarchisation décrite par l'auteur mais, plus qu'une *hiérarchisation du secret* c'est une *hiérarchisation des secrets professionnels* qui est opérée. Ce mouvement est

---

[2219] *Ibid.*
[2220] B. PY, « De la violation du secret professionnel : essai de légistique progressiste », *in* V. MALABAT, B. DE LAMY et M. GIACOPELLI, *La réforme du Code pénal et du Code de procédure pénale.* Opinio doctorum, coll. Thèmes et commentaires, Dalloz, 2009, p. 89 et svt., spéc. p. 94.
[2221] Dont le régime d'accès est prévu aux article R. 2311-1 et svt du Code de la défense.

particulièrement remarquable s'agissant des recherches, évaluations et études dans le domaine de la santé et, de manière plus générale, concernant la réutilisation des données du SNDS.

442. La réutilisation des données issues de la prise en charge des personnes depuis la loi du 20 juin 2018. Il faut, tout d'abord, remarquer que la section portant sur le traitement des données à caractère personnel dans le domaine de la santé, telle que modifiée par la loi du 20 juin 2018 puis par l'ordonnance du 12 décembre 2018[2222], demeure source de confusion. Tandis que la première sous-section annonce les dispositions générales relatives au traitement des données de santé ayant une finalité d'intérêt public, se trouvent dans cette section des dispositions qui ne s'appliquent, en principe, que dans le cadre de la réutilisation des données à des fins de recherche, d'étude et d'évaluation dans le domaine de la santé ainsi que les dispositions justificatives autorisant les professionnels de santé à transmettre des données à caractère personnel qu'ils détiennent. La CNIL a souligné cette imperfection avec insistance[2223], sans que son avis ne soit suivi par le législateur. Il peut s'agir d'une simple maladresse du législateur, il nous semble toutefois que l'économie de la section relève d'une volonté qui va dans le sens de l'élargissement de l'accès des données du SNDS enrichi, tel que promulgué par la loi relative à l'organisaiton et à la transformation du système de santé[2224]. En effet, si l'accès aux données pseudonymisées du SNDS est désormais élargi au traitement présentant un intérêt public, il apparaît que l'exception posée à l'article 68 et autorisant les professionnels de santé à transmettre des données à caractère dans le cadre de traitements présentant une finalité d'intérêt public doit se comprendre comme allant dans le même sens. En

---

[2222] Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel

[2223] « *Etrangement, le projet énonce ensuite toute une série de dispositions directement reprises de l'actuel chapitre IX : d'une part, des mesures destinées à alléger la procédure d'autorisation (« méthodologies de référence », « jeux de données pouvant faire l'objet d'une mise à disposition » ou encore « décisions uniques »), d'autre part, des règles de fond (interdiction de « communication » des données, possibilité pour les professionnels de «transmettre» les données à caractère personnel qu'ils détiennent, condition de présentation « des résultats », etc.). Manifestement, ces dispositions n'ont pas vocation à s'appliquer aux traitements comportant des données de santé en dehors de la recherche tels que les vigilances (pharmacovigilance, matériovigilance, cosmétovigilance, etc.), les mécanismes de surveillance sanitaire ou encore les entrepôts de données. La Commission propose donc de réintégrer l'ensemble des dispositions relatives aux traitements de recherche, d'étude ou d'évaluation dans la section 2, y compris le rôle de l'Institut national des données de santé et ce, tant au regard de ses missions, telles que prévues par le code de la santé publique, que de sa composition. Ne devraient ainsi plus figurer dans la section 1 que le principe général d'autorisation par la Commission des traitements présentant une finalité d'intérêt public et la faculté, pour elle, d'établir des autorisations uniques sur le modèle de ce qu'elle a déjà pu adopter* » (Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978, pp. 24-25).

[2224] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (*JORF* n° 0172 du 26 juill. 2019).

d'autres termes, cette première section a vocation à s'appliquer conjointement aux dispositions figurant au Code de la santé publique et à l'accès élargi au SNDS qui ne sera plus conditionné à la seule recherche. Il convient à présent d'approfondir l'idée d'une hiérarchisation des secrets professionnels.

443. Pseudonymisation et accès aux données de santé. Comme nous l'avons évoqué, toute utilisation ultérieure des données de santé à caractère personnel issues de la prise en charge des personnes par un professionnel soumis au secret entraîne une soumission au secret professionnel. Ainsi, l'article L. 1461-1 du Code de la santé publique prévoit que toutes les personnes responsables de ces traitements, ainsi que celles les mettant en œuvre ou autorisées à accéder aux données à caractère personnel qui en sont issues sont soumises au secret professionnel. De même, l'article 68 de la LIL, ancien article 55, prévoit, outre la permission de révéler, la soumission au secret professionnel de toutes les personnes mettant en œuvre un traitement de données transmises sur le fondement de cet article. Or, dans les deux hypothèses, les données transmises sont pseudonymisées. La mention du codage des données a disparu à la suite de la modification du texte par la loi du 26 janvier 2016 relative à la modernisation du notre système de santé, le législateur souhaitant laisser à la CNIL le soin de déterminer les mesures les plus adaptées pour assurer la pseudonymisation[2225]. La suppression des exceptions aux mesures de codage laisse, quant à elle, supposer que les données transmises doivent systématiquement être pseudonymisées. Ainsi, la soumission au secret professionnel en raison de l'accès aux données ne suppose pas que les personnes mettant en œuvre de tels traitements pourraient prendre connaissance des données directement identifiantes. Cette soumission au secret professionnel relève d'une logique de risque au regard de la sensibilité des données. Les données directement identifiantes ne seront accessibles qu'aux professionnels de santé, tandis que les données pseudonymisées pourront être transmises pour des réutilisations ultérieures. Ce système s'explique notamment par le rôle que joue le consentement de la personne concernée par les données. Il n'est pas une cause justificative, s'agissant tant de l'accès au SNDS qu'au regard de l'article 74 de la LIL, qui prévoient que les personnes peuvent s'opposer à la *levée*

[2225] Outre la pseudonymisation, il s'agit de l'ensemble des moyens à mettre en œuvre pour assurer la confidentialité. « *Les modifications portant sur l'article 55 visent à insérer dans la loi Informatique et libertés la possibilité reconnue à la Cnil d'adopter des recommandations ou des référentiels relatifs aux moyens techniques à mettre en œuvre pour garantir la confidentialité des données lors de leur transmission* » (A. MILON, C. DEROCHE et E. DOINEAU, *Rapport fait au nom de la commission des affaires sociales*, Sénat, session extraordinaire de 2014-2015, 22 juill. 2015, n° 653, p. 468).

du secret. Il s'agit, en quelque sorte, de réserver l'accès aux données directement identifiantes au premier cercle des professions soumises au secret, tandis que le cercle des acteurs intervenant secondairement sur les données n'aura accès, autant que possible au regard de la finalité de la recherche, qu'à des données pseudonymisées. La détermination des mesures de pseudonymisation dépendra ensuite de la gravité du risque de réidentification. Les exemples les plus évidents concernent les traitements de données à des fins de recherche dans le domaine de la santé, mais aussi l'accès aux données du SNDS pour des finalités d'intérêt public.

2 - Illustrations

444. Recherche dans le domaine de la santé et méthodologies de références élaborées par la CNIL. Il n'est pas nécessaire d'expliquer ici, en détail, les conditions de mise en œuvre des recherches dans le domaine de la santé, ce qui aurait pour conséquence, tant les régimes sont complexes, de nous éloigner de notre objet d'étude et d'opérer des confusions déjà fréquentes entre le régime propre à la recherche et celui du traitement des données[2226]. Il convient toutefois de formuler quelques remarques, puisque ces différentes dispositions s'articulent[2227]. Concernant d'abord les recherches qui sont dites « internes », elles sont mises en œuvre à partir de données recueillies dans le cadre du suivi individuel des patients, par les personnels assurant ce suivi et pour leur usage exclusif[2228]. Elles n'impliquent donc pas que d'autres professionnels que ceux prenant en charge la personne aient accès aux données et répondent aux dispositions relatives au secret partagé ainsi qu'au régime général de protection des données en ce qu'elles sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements[2229]. En dehors de cette hypothèse, deux cas de figure se présentent : pour les recherches impliquant la personne humaine, le régime du traitement des données répond en partie au régime prévu par la loi du 5 mars 2012, dite loi

---

[2226] L. TILMAN, « Recherche et utilisation des données médicales : un cadre inadéquat ? », *in* M. BERNELIN et E. SUPIOT (ss la dir.)*, Les frontières entre recherche et* soin, *Cahiers Droit, Sciences & Technologies*, n° 5, PUAM, 2015, pp. 89-98.

[2227] Pour quelques remarques générales sur ce point, v. M. GRIGUER, « Le point sur le nouveau régime des traitements de données personnelles », *Cahiers de droit de l'entreprise*, juill. 2018, n° 4, prat. 20.

[2228] Ces traitements répondent aux dispositions générales du RGPD et de la LIL et non à celles, spécifiques, prévues pour les traitements de données à caractère personnel dans le domaine de la santé (LIL, art. 64).

[2229] Il s'agit alors d'articuler les dispositions prévues aux articles L. 1110-4 et R. 1110-1 et suivants du Code de la santé publique ainsi que les dispositions du RGPD et de la LIL (notamment l'article 44).

Jardé[2230] ; quant aux recherches n'impliquant pas la personne humaine, elles répondent au cadre posé par la loi du 26 janvier 2016. Dans ces deux cas, et pour satisfaire la logique de responsabilisation des acteurs et la diminution drastique des formalités préalables, la CNIL a adopté des méthodologies de référence[2231]. Ces méthodologies nous permettent de confirmer notre hypothèse selon laquelle, par le biais des techniques de pseudonymisation, il est procédé à une hiérarchisation des secrets professionnels.

445. Examen des méthodologies de référence hors des hypothèses de réutilisation de données collectées lors d'une prise en charge. La Commission a élaboré plusieurs méthodologies de références. S'agissant d'abord des méthodologies s'appliquant aux recherches ou études impliquant la personne humaine, il en existe actuellement trois.

La MR 001 concerne les recherches interventionnelles qui comportent une intervention sur la personne non justifiée par sa prise en charge habituelle[2232] et les recherches interventionnelles à risques minimes[2233] ainsi que les recherches non interventionnelles qui impliquent un examen des caractéristiques génétiques[2234], tandis que la MR-003 porte sur les recherches non interventionnelles impliquant la personne humaine. Les deux méthodes précisent d'abord l'origine des données concernant les personnes se prêtant à la recherche. Elles sont collectées auprès de la personne ou de son représentant légal, de bases de données ou d'échantillons biologiques, légalement constituées et ayant fait l'objet des formalités nécessaires auprès des autorités compétentes. Les données qui peuvent être collectées sont nombreuses et, pour certaines, sensibles[2235]. Il importe de souligner que tous les destinataires des données sont

---

[2230] Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine (*JORF* n°0056 du 6 mars 2012, p. 4138) ; Décret n° 2016-1537 du 16 novembre 2016 relatif aux recherches impliquant la personne humaine, (*JORF* n° 0267 du 17 nov. 2016).

[2231] Ces méthodologies sont des outils de droit souple, elles sont prises par la Commission en vertu du pouvoir normatif octroyé par la loi (LIL, art. 8). Ces normes bénéficient toutefois d'une certaine force dans la mesure où les traitements qui ne sont pas conformes aux méthodologies sont nécessairement soumis à une autorisation des la CNIL (LIL, art. 73).

[2232] CSP, art. L. 1121-1, 1°.

[2233] CSP, art. L. 1121-1, 2°.

[2234] CNIL, Délibération n° 2018-153 du 3 mai 2018 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé avec recueil du consentement de la personne concernée (MR 001) et abrogeant la délibération n° 2016-262 du 21 juillet 2016.

[2235] Il peut s'agir de données de santé mais également de données génétiques, relatives à l'origine ethnique, à la vie sexuelle.

soumis au secret professionnel : un renvoi est effectué aux articles 226-13 et 226-14 du Code pénal. Les méthodologies précisent ensuite quels sont les destinataires des données directement identifiantes et ceux des données indirectement identifiantes. Sur ce point, il faut remarquer que sont destinataires des données directement identifiantes les professionnels intervenant dans la recherche et ceux agissant sous leur autorité : il s'agit de l'investigateur, qui est nécessairement un médecin[2236] – historiquement soumis au secret professionnel – ainsi que les personnes l'assistant, qui sont également des professionnels de santé. Sont aussi destinataires des données directement identifiantes les responsables du contrôle et de l'assurance de qualité, que sont les attachés de recherche clinique et les techniciens d'étude clinique. Ces derniers sont soumis au secret professionnel par l'article L. 1121-3 du Code de la santé publique, ils ne peuvent accéder aux données que si la personne concernée ne s'y est pas opposée. S'agissant des personnes destinataires des données *indirectement* identifiantes il s'agit de toutes les personnes dont la soumission au secret professionnel pose des difficultés dans la mesure où le seul texte de désignation est contenu dans la méthodologie de référence, comme c'est le cas du promoteur de la recherche[2237] ou encore du personnel chargé de la collecte, du traitement et de l'analyse des données, dont fait partie le *data scientist*[2238]. Les méthodologies précisent – et c'est sans doute l'information centrale – que « *seuls les professsionnels et leurs collaborateurs intervenant dans la recherche peuvent conserver le lien entre l'identité codée des personnes se prêtant à la recherche utilisée pour associer les données de santé à caractère personnel et leurs nom(s) et prénom(s) (table de correspondances conservée de façon sécurisée)* ». La même logique se retrouve dans la MR-002, qui précise que seul le médecin investigateur conserve la table de correspondance permettant la réidentification des personnes.

446. Les recherches et la réutilisation des données. La méthodologie de référence MR-004 concerne uniquement les recherche n'impliquant pas la personne humaine[2239]. Dans ce cas, les

---

[2236] CSP, art. L. 1121-3.
[2237] CSP, art. L. 1121-1 al. 3 : « *La personne physique ou la personne morale qui est responsable d'une recherche impliquant la personne humaine, en assure la gestion et vérifie que son financement est prévu, est dénommée le promoteur* ». Le promoteur de la recherche est également le responsable du traitement : titre I, 1.1 de la MR-001.
[2238] L'avis n° 130 du Comité consultatif national d'éthique, intitulé « *Données massives (big data) et santé : une nouvelle approche des enjeux éthiques* », évoque l'intervention croissante de ces acteurs et formule quelques inquiétudes au regard du *secret médical*.
[2239] CNIL, Délibération n° 2018-155 du 3 mai 2018 portant homologation de la méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches n'impliquant pas la personne humaine, des études et évaluations dans le domaine de la santé (MR-004).

données sont le plus souvent issues de bases de données constituées antérieurement pour des finalités relevant de la prise en charge sanitaire des personnes. C'est pour ce type de recherche et d'études dans le domaine de la santé qu'avait été édicté l'article 68 (ancien article 55) de la LIL, prévoyant la possibilité pour les professionnels de santé de transmettre leurs données. La méthodologie précise que, lorsque les recherches portent sur des données réutilisées, seules les personnes habilitées initialement à accéder aux données *nominatives*[2240] peuvent détenir la correspondance. Ainsi, les professionnels intervenant directement dans la prise en charge, en équipe de soins ou hors équipe de soins, seront les seuls à pouvoir accéder directement aux données. Il est encore précisé que « *le numéro d'ordre affecté à la personne pour l'étude est différent du numéro identifiant le patient dans la base initiale* »[2241].

447. Examen des autorisations de la CNIL. Les recherches ne répondant pas à ces méthodologies[2242] sont toujours soumises à autorisation, de même que les traitements de données à caractère personnel dans le domaine de la santé répondant à une finalité d'intérêt public. L'on peut donc encore vérifier la logique qui consiste à préserver le « secret médical » – entendu comme le secret des informations relatives aux personnes prises en charge par un professionnel intervenant dans le système de santé – en distinguant parmi les personnes soumises au secret professionnel celles pouvant connaître directement l'identité de la personne à laquelle se rattachent les données de santé et celles ne pouvant accéder qu'aux données présentant un risque de réidentification, c'est-à-dire pseudonymisées. S'agissant, par exemple, des traitements de données à caractère personnel ayant pour finalité la création d'entrepôts de données, ils répondent aux dispositions générales relatives au traitement de données à caractère personnel dans le domaine de la santé prévues aux articles 64 à 71 de la LIL. Les autorisations de la CNIL précisent en effet que seuls les membres de l'équipe de soins telle que définie à l'article L. 1110-12 du Code de la santé publique ont accès à l'ensemble des données identifiantes, tandis que « *Concernant les projets de recherche ultérieurs, les chercheurs et*

[2240] C'est le terme utilisé dans la méthodologie. Il conviendrait toutefois d'utiliser l'expression *données directement identifiantes*.
[2241] CNIL, Délibération n° 2018-155 du 3 mai 2018, préc., 2.2.1.
[2242] Il s'agit en général des traitements incluant des données génétiques, le NIR ou ceux dont l'analyse d'impact révèle l'existence d'un risque résiduel élevé en dépit des mesures prises pour assurer la sécurité et la confidentialité du traitement.

membres des équipes des chercheurs (biostatisticiens, ARC de monitoring, data managers…) n'appartenant pas à l'équipe de soins auront accès aux données indirectement identifiantes de l'entrepôt, dans la limite des données strictement nécessaires et pertinentes au regard de leurs fonctions »[2243].

448. Graduation de l'accès au SNDS, l'exemple topique. Outre les hypothèses d'accès aux données pour des finalités de recherche, le SNDS est désormais accessible pour des traitements de données ayant une finalité d'intérêt public. En toutes hypothèses, l'accès aux données pseudonymisées du SNDS entraîne soumission au secret professionnel[2244]. La logique qui sous-tend la hiérarchisation des secrets professionnels est particulièrement notable dans ce cas puisqu'il n'est pas possible d'accéder aux données directement identifiantes. Si la loi du 26 janvier 2016 prévoyait la possibilité de créer un organisme spécifique habilité à détenir le dispositif de correspondance permettant de réidentifier les personnes à partir des données du système national des données de santé[2245], cette solution n'a jamais été mise en œuvre. Le dispositif a été supprimé par la loi relative à l'organisation et à la transformation du système de santé[2246]. Il faut ajouter que la prise en compte du risque d'atteinte au secret des informations issues de la prise en charge des personnes par un professionnel de santé intervenant dans système de santé est encore visible s'agissant du dispositif prévu pour les accès permanents au SNDS. L'on sait que les personnes relevant des services de l'Etat ou des établissements publics sont, pour la plupart, statutairement soumis au secret professionnel. Pour autant, elles n'ont accès qu'aux seules données pseudonymisées, mais dans des conditions différentes de celles des autres acteurs pouvant bénéficier, pour des finalités d'intérêt public, d'un accès occasionnel. A ce titre, l'article R. 1461-11 du Code de la santé publique[2247] prévoit que l'étendue de l'autorisation d'accès dépend « *des exigences des missions de service public qu'ils remplissent* », cette étendue étant définie par la profondeur historique des données et l'utilisation simultanée de plusieurs variables identifiantes. Ainsi, **les techniques de**

[2243] Par exemple : Délibération n° 2018-295 du 19 juillet 2018 autorisant le Centre Hospitalier Universitaire de Nantes à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité un entrepôt de données de santé, dénommé EHOP. (Demande d'autorisation n° 2129203) ; Délibération n° 2017-013 du 19 janvier 2017 autorisant l'Assistance publique – Hôpitaux de Paris à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité un entrepôt de données de santé, dénommé « EDS » (Demande d'autorisation n° 1980120).
[2244] CSP, art. L. 1461-1, IV, 2°.
[2245] CSP, art. L. 1461-4, II, al. 2.
[2246] Loi relative à l'organisation et à la transformation du système de santé n° 2019-774 du 24 juillet 2019, *JORF* n° 0172 du 26 juillet 2019.
[2247] Actuellement en vigueur et qui n'a subi aucune modification à la suite de la loi relative à l'organisation et à la transformation du système de santé.

pseudonymisation des données constituent un instrument de hiérarchisation des secrets dans la mesure où elles permettent une graduation des données et partant, d'identifier ce à quoi ont accès les personnes au regard du fondement de leur secret professionnel : les professionnels intervenant dans la prise en charge des personnes ont accès aux données directement identifiantes, les services de l'Etat et administration ont accès aux données dont la pseudonymisation présente le plus de risque de réidentification, tandis que les personnes soumises au secret en raison de l'origine des données ont accès aux données pseudonymisées présentant le plus faible risque de réidentification. Les données anonymes font l'objet d'une ouverture complète.

3 - Remarques

449. SNDS, la pseudonymisation renforcée, une contrepartie ? Etant donné que la détermination *a priori* des finalités de traitement est contraire à la nature des *Big data*, le législateur avait opté pour leur suppression. De manière plus générale, un auteur explique que l'anonymisation des données est « *fondamentalement contraire* » aux usages du *Big data*[2248], ce que souligne également le CCNE dans son avis relatif aux données massives et à la santé[2249]. Les risques de réidentification sont d'autant plus importants que la masse de données ira croissante et que les possibilités de croisement seront désormais favorisées[2250]. L'assouplissement du régime d'accès s'accompagne de ce que le législateur considère comme une contrepartie. Il est question de « *renforcer la pseudonymisation* »[2251] des données de santé, l'expression « *pseudonymisation irréversible* »[2252] étant même utilisée. Ces termes sont pour le moins énigmatiques lorsque l'on sait que même des données brutes traitées par les *Big data* peuvent redevenir des données à caractère personnel ; il est dès lors difficile d'imaginer

---

[2248] L. MAISNIER-BOCHÉ, « Intelligence artificielle et données de santé », Dossier *Intelligence artificielle et santé*, *Journal de Droit de la Santé et de l'Assurance Maladie (JDSAM)*, n° 17, 2017, p. 27.
[2249] CCNE, *Données massives et santé : une nouvelle approche des enjeux éthiques*, Avis n° 130, 29 mai 2019, p. 56. Le Conseil souligne en outre que le risque de réidentification ultérieure ne peut plus être exclu.
[2250] Notamment entre les données cliniques et les données médico-administratives (A. MILON, Rapport fait au nom de la commission des affaires sociales sur le projet de loi, adopté par l'assemblée nationale après engagement de la procédure accélérée, relatif à l'organisation et à la transformation du système de santé, 22 mai 2019, p. 179).
[2251] A. MILON, *op. cit.*, p. 100.
[2252] S. RIST et T. MESNIER, Rapport fait au nom de la commission des affaires sociales sur le projet de loi relatif à l'organisation et à la transformation du système de santé, volume II, commentaires d'articles et annexes, 14 mars 2019, p. 100.

comment la pseudonymisation pourrait être *renforcée*. Derrière cet *effet d'annonce* s'opère en réalité la suppression de l'une des dispositions de la loi de modernisation du système de santé[2253] qui prévoyait de confier à un tiers de confiance, distinct du responsable du SNDS, la possibilité de procéder à la réidentification des personnes concernées. Il s'agissait d'un dispositif de correspondance[2254]. Il a pu être mentionné que cette possibilité constituait une *faiblesse* dans le dispositif de sécurité d'un SNDS élargi[2255]. Il faut toutefois remarquer que le fait de supprimer la possibilité de réidentifier les personnes par le biais d'un dispositif de correspondance n'atténue en rien les risques de réidentification liés aux *Big data*. A ce propos, et à la suite de la mise en œuvre de l'*open data* en santé en Australie – de données anonymes et non pseudonymisées –, des chercheurs sont parvenus à réidentifier certaines célébrités pour démontrer la réalité des risques[2256].

450. *Big data is not about data!*[2257] Au-delà du risque de réidentification, les enjeux du *Big data*. C'est à dessein que nous utilisons, presque à l'identique, les mots d'un titre précédent. Reprenant les propos de Mesdames Bensamoun et Zolynski, nous avons rappelé que le *Big data* reposait sur le « *réemploi potentiel des données à l'avenir à des fins que l'on a pu ne pas envisager lors de leur collecte* »[2258], ce qui explique l'ouverture accrue des données issues de la prise en charge des personnes dans le système de santé. De ce premier constat découle le second : il est possible que les données initialement traitées – et qui n'étaient pas des données à caractère personnel – tombent ensuite dans le champ d'application des dispositions relatives

---

[2253] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n° 0022 du 27 janv. 2016.
[2254] CSP, art. L. 1461-4 (supprimé par la loi relative à l'organisation et à la transformation du système de santé).
[2255] Etude d'impact, Projet de loi relatif à l'organisation et à la transformation du système de santé, NOR : SSAX1900401L/Bleue-2, 13 févr. 2019, p. 90. Aucun tiers de confiance n'avait été désigné depuis l'entrée en vigueur de la loi du 26 janvier 2016. Il s'est également avéré que ce dispositif prévu afin de pouvoir avertir les personnes concernées par un risque sanitaire grave n'avait pas d'utilité puisqu'il est possible d'identifier ces personnes dans les systèmes « sources » du SNDS sans recourir au tiers de confiance (les système sources sont les systèmes qui alimentent le SNDS, comme par exemple les bases du PMSI).
[2256] V. TEAGUE, C. CULNANE et B. RUBINSTEIN, « Research reveals de-identified patient data can be re-identified », Université de Melbourne (disponible en ligne sur <https://phys.org/news/2017-12-reveals-de-identified-patient-re-identified.html> (dernière consultation le 8 oct. 2019)).
[2257] Il s'agit du titre de la préface écrite par le statisticien et politologue américain Gary King pour un ouvrage publié par l'université de Cambridge, l'idée sous-jacente consiste à dire que si l'enjeux des données massives n'est pas les données, c'est la masse qui importe : G. KING, « Big Data is not about the data ! », *in* R. MICHAEL ALVAREZ, *Computational Social Science: Discovery and Prediction*,Cambridge University P ress, 2016, p. VII.
[2258] A. BENSAMOUN et C. ZOLYNSKI, « *Cloud computing et Big data. Quel encadrement pour ces nouveaux usages des données personnelles ?* », *Réseaux* 2015/1, n° 189, p. 110.

à la protection des données personnelles. Les *big data* pourraient avoir pour effet d'identifier les personnes même à partir de données brutes[2259]. Pour cette raison, Madame Zolynski et Madame Latreille ont proposé de procéder à une analyse diachronique des traitements[2260]. Le Règlement a apporté une réponse partielle à ce problème par l'adoption d'une logique d'*accountability* et en posant le principe de la *privacy by design*. Il nous semble toutefois que les *Big data* imposent de réinterroger la logique de graduation que nous avons décrite.

451. La pseudonymisation permet ainsi de préserver le secret des données directement identifiantes, que l'on assimile au « secret médical », en opérant une graduation des accès aux données et, partant, une hiérarchisation des secrets professionnels. Ce phénomène pourrait s'analyser comme une forme de distribution des droits sur les données, chaque type d'utilisation et d'accès aux données étant associé à une position hiérarchisée[2261].

§ 2 - L'enchevêtrement normatifs à l'échelle nationale et européenne

452. Outre l'exemple particulier des techniques de pseudonymisation que nous souhaitions développer, l'on constate un enchevêtrement des normes technico-managériales relatives à la sécurité et à la confidentialité des données couvertes par le secret dans le domaine de la santé et des normes juridiques tant au niveau national, qu'européen et international. Les liens entre elles sont particulièrement intriqués dans la mesure où les normes technico-managériales intègrent les instruments juridiques nationaux mais également européens **(A)**. Par ailleurs, une norme récente, à l'élaboration de laquelle la CNIL à participé, intègre le RGPD **(B)**.

[2259] *Ibid.,* p. 111. V. également en ce sens A. BENSAMOUN, « Intelligence artificielle et santé : l'intégration en droit de l'IA médicale », Dossier Intelligence artificielle et santé, *Journal de Droit de la Santé et de l'Assurance Maladie* (JDSAM), n° 17, 2017, pp. 30-33.

[2260] C. ZOLYNSKI et A. LATREILLE, « Big data et protection des données à caractère personnel », *in* N. MARTIAL-BRAZ, M. BEHAR-TOUCHAIS, J. ROCHFELD et C. ZOLYNSKI, *La proposition de règlement européen relatif aux données à caractère personnel*, Société de Legislation Comparée – Trans Europe Experts, 2014, p. 262.

[2261] Le rapprochement peut être fait avec le faisceau de droits tel que conceptualisé par Elinor Ostrom. Nous nous abstiendrons d'affirmer toutefois qu'il serait pertinent, cette question devrait faire l'objet d'une conceptualisation qui dépasse l'objet de notre étude. Pour un résumé de la notion de faisceau de droits, v. F. ORSI, *V°* « Faisceau de droits (*bundle of rights*) », *in* M. CORNU, F. ORSI, J. ROCHFELD (ss la dir.), *Dictionnaire des biens communs*, coll. Quadrige, PUF, 2017.

A - La référence aux normes techniques et managériales dans les normes juridiques

453. La référence aux normes techniques et managériales concerne aussi bien les instruments de l'Union européenne **(1)** que ceux les instruments de droit souple produits au niveau national **(2)**.

1 - La référence aux normes techniques et managériales dans les instruments de l'Union européenne

454. Les normes techniques dans les textes juridiques de l'Union. La politique européenne tendant à créer un espace numérique de santé repose sur l'interopérabilité. Celle-ci doit être technique et sémantique[2262]. Dans son acception technique, elle consiste, selon la définition de l'ISO, dans « *l'aptitude à communiquer, exécuter des programmes ou de transgérer des données entre différentes unités fonctionnelles (systèmes) en n'exigeant de l'utilisateur qu'un minimum de connaissance des caractéristiques uniques de ces systèmes* »[2263]. C'est vers cette exigence que l'effort de normalisation, au niveau européen, s'est porté, et les normes techniques ont vocation à assurer à la fois l'interopérabilité, la sécurité et la confidentialité. Par ailleurs, si le RGPD encourage le recours à des modes de régulation volontaire tels que les codes de conduite[2264], la certification et la labellisation, le règlement relatif à la cybersécurité doit aboutir à un cadre commun de certification qui portera sans doute sur des normes issues tant de normalisateurs institutionnalisés que privés[2265]. Le règlement

---

[2262] La normalisation de l'interopérabilité au plan sémantique est essentielle à la mise en œuvre au projet européen, la « *structuration et l'intelligibilité des données (sémantique) sont les principaux enjeux des échanges et de maîtrise des flux d'information* » (K. BOURQUARD, « Norme numérique et e-Santé », *in Normaliser le numérique*, série Enjeux numériques, Annales des Mines, 5 mars 2019, p. 68).

[2263] ISO/IEC 2382-1:1993. Technologies de l'information – Vocabulaire, Partie 1 : Termes fondamentaux.

[2264] Les codes de conduite dans le domaine de la protection des données émanent des acteurs, responsables de traitement et sous-traitants formant des organismes représentant des catégories (RGPD, consid. 98) et sont une traduction de la démarche de *compliance*. Ces codes, d'ordinaire privés, sont une démonstration de volonté de la part des entreprises de se forger une éthique des affaires. Dans le cadre du RGPD, ils sont encadrés, contrôlés et, comme outils de *compliance*, ont une valeur contraignante (RGPD, art. 40 et 41), ce qui contribue à brouiller la frontière de la juridicité. Pour une étude sur les codes de conduite sous l'angle des sources du droit, v. M. LAROUER, *Les codes de conduite, sources du droit*, préf. P. DEUMIER, coll. Nouvelle Bibliothèque de Thèses, vol. 176, Dalloz, 2018.

[2265] La Commission a pu affirmer clairement qu'elle utilise les normes techniques issues d'organismes de normalisation divers, particulièrement dans le domaine de l'innovation, en fonction de ses intérêts : « *Reconnaître l'importance de normes tant formelles qu'informelles pour l'innovation. Il est nécessaire qu'il existe un processus de normalisation formelle qui respecte pleinement les principes d'ouverture, d'inclusion, de transparence et de*

eIDAS fait actuellement des références explicites à des normes techniques tandis que la coopération dans le cadre la directive NIS conduit également à l'utilisation de normes technico-managériales.

455. eIDAS. Le règlement eIDAS précédemment cité a pour particularité d'être trans-sectoriel, son niveau de généralité implique qu'il « *ne s'intéresse pas au rôle de la personne considérée* »[2266]. Or, pour garantir la confidentialité des données couvertes par le secret, il convient de pouvoir, non seulement, identifier les personnes – ce qui contribue à garantir la confidentialité des données –, mais encore de s'assurer de leur statut, de leur profession ou de leur mission à un moment donné. Les normes techniques interviennent ici à un double niveau. D'une part, le règlement s'accompagne d'un référentiel documentaire qui liste, en plus des décisions et règlements d'éxecution relatifs à l'identification électronique et aux services de confiance, les normes techniques référencées dans les actes d'exécution. Il s'agit de normes ETSI[2267] et d'un organisme de coordination de la normalisation en matière de sécurité des systèmes d'information[2268]. Dans le domaine de la santé, ces normes seront

---

cohérence et permette l'instauration d'un consensus entre toutes les positions nationales et les parties intéressées. Simultanément, d'autres normes, élaborées par les organisations de normalisation reconnues et autres, sont souvent plus réceptives aux technologies innovatrices et jouent donc un rôle important dans l'accélération de leur acceptation par le marché. Afin de profiter des avantages des deux types de normes, de préserver la cohérence du système de normalisation européen et d'optimiser le rôle des experts disponibles, il est important de faciliter une bonne coordination des activités entre les organisations de normalisation formelles et informelles. À cet égard, la coopération avec un grand nombre de forums de normalisation informelle qui a été mise en place par l'ETSI au niveau européen et par l'ISO et la CEI au niveau international doit être considérée comme une bonne pratique » (Communication de la Commission au Conseil, au Parlement européen et au Comité économique et social européen vers une contribution accrue de la normalisation à l'innovation en europe, *Vers une contribution accrue de la normalisation à l'innovation en Europe*, COM (2008) 133 final, 11 mars 2008, p. 7) ; *Adde* A. VAN WAEYENBERGE, « Les normes ISO, CEN et celles issues de consortiums privés : bric à brac ou systèmes pour l'Union européenne ? », *in* B. FRYDMAN et A. VAN WAEYENBERGE (ss. la dir.), *Gouverner par les standards et les indicateurs : de Hume aux rankings*, coll. Penser le droit, Bruylant, 2014, p. 111.

[2266] M. THONNET, « Santé, numérique, droit-s et Europe : interactions et conséquences », *in* I. POIROT-MAZERE (ss la dir.), *Santé, numérique et droit-s*, Actes du colloque des 7 et 8 sept. 2017, Université de Toulouse I Capitole, coll. des actes de colloques de l'Institut Fédératif de Recherche – Mutation des normes juridiques, n° 34, Presses de l'Université de Toulouse 1 Capitole, p. 61 et svt, spéc. p. 71.

[2267] Une série de normes européennes porte sur les profils de signatures électroniques (ETSI TS 103 171 à 174) et une norme comporte la liste des fournisseurs de services de confiance au sens du règlement (PE et Cons., Règlement (UE) n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, du 23 juill. 2014).

[2268] Il s'agit de SO-GIS, groupe formé à la suite d'un accord entre des organisations et agences gouvernementales des pays de l'Union européenne qui les représentent. Cet accord a notamment été crée après la recommandation du Conseil 1995/144/CE du 7 avril 1995, concernant des critères communs d'évaluation de la sécurité des technologies de l'information. Cette coordination est néanmoins très sectorielle et participe difficilement d'une harmonisation cohérente.

nécessairement insuffisantes puisqu'il faudra aller plus loin dans l'identification et identifier précisément le rôle de la personne. Ce sont d'autres normes techniques qui devront alors être mobilisées à cette fin, ce qui, pour l'instant, ne contribue pas à l'harmonisation recherchée.

456. Références aux normes techniques dans les instruments de coordination en matière de cybersécurité. La directive dite « NIS »[2269] pose la première pierre d'un « *cadre juridique commun de la cybersécurité* »[2270], défini afin que soit assuré dans tous les pays de l'Union un niveau élevé de sécurité des réseaux et des systèmes d'information. Elle vise à imposer aux Etats l'adoption d'une politique de coopération en matière de cybersécurité pour permettre la réalisation du marché unique numérique[2271]. L'harmonisation est donc minimale[2272] dans la mesure où la directive ébauche un cadre relatif à la sécurité des réseaux et des systèmes d'information pour les seuls opérateurs de services essentiels et les fournisseurs de service numérique[2273]. Il convient de souligner, par ailleurs, que chaque Etat doit désigner une autorité compétente pour mettre en œuvre la stratégie dont les linéaments sont définis par la directive ; en France il s'agit de l'ANSSI. Cette directive a été transposée en droit français par une loi du 26 février 2018[2274] et, comme le remarque Monsieur Douville, la directive comme la loi ont « *seulement pour objet les réseaux et systèmes d'information, notion qui recouvre les réseaux de communications électroniques, les dispositifs (ou ensemble de dispositifs, interconnectés ou apparentés) qui en exécution d'un programme assurent un traitement automatisé des données numériques et les données numériques transmises, récupérées, traitées ou stockées grâce aux réseaux de communications électroniques et aux dispositifs de traitements* »[2275], ce qui distingue son champ d'application de celui applicable aux fournisseurs de réseaux et services de communications électroniques et aux prestataires de services de confiance[2276]. Ainsi, la loi, reprenant les définitions de la directive, vise exclusivement les opérateurs de services

---

[2269] PE et Cons., Directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, 6 juill. 2016, *JOUE* 19 juill. 2016, L 194/1.
[2270] T. DOUVILLE, « L'émergence d'un droit commun de la cybersécurité », *D.* 2017, p. 2255.
[2271] T. DOUVILLE, « Cybersécurité : transposition de la directive NIS, ses limites et ses conséquences », *JCP E* 2018, n° 15-16, act. 284.
[2272] *Ibid.*
[2273] PE et Cons. UE, dir. (UE) 2016/1148, 6 juill. 2016, art. 1, § 2 d).
[2274] Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (*JORF* n° 0048 du 27 févr. 2018).
[2275] T. DOUVILLE, « Cybersécurité : transposition de la directive NIS, ses limites et ses conséquences », *op. cit.*
[2276] *Ibid.*

essentiels[2277] et certains founisseurs de services numériques[2278]. C'est l'ANSSI qui est chargée de définir la liste – non publiée – des opérateurs essentiels au regard de la liste des services essentiels publiée par un décret du 23 mai 2018[2279]. A la lecture du décret, peuvent notamment être des opérateurs de services essentiels les établissements de santé, publics ou privés, qu'ils soient des prestataires de soins de santé ou des prestataires fournissant un service d'aide médicale d'urgence[2280]. Certains établissements de santé nationaux peuvent donc être concernés par la procédure de la directive qui consiste notamment en une obligation de mise en conformité, d'audit et de déclaration d'incident. Le groupe européen de coopération issu de la directive et dont fait partie l'ANSSI a publié une méthodologie pour le management du risque, principalement issue de normes technico-managériales internationales. Cette méthode est issue de celle utilisée en France depuis 2013 pour la protection des systèmes d'information d'importance vitale depuis la loi de programmation militaire promulguée la même année[2281]. Il s'agit de la Politique de sécurité des systèmes d'information (PSSI), laquelle est principalement basée sur la famille de normes ISO/CEI 27001[2282]. Par ailleurs, tout le corpus des règles organisationnelles et techniques de ces systèmes contient des références à des normes internationales et européennes[2283].

[2277] Les opérateurs de services essentiels sont, selon l'article 4 de la loi de transposition de la directive « *Les opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services* » (Loi n° 2018-133, art. 5).

[2278] Par service numérique est visé « *tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services* » (Loi n° 2018-133, art. 10). Seuls certains opérateurs de services sont visés par la loi, il s'agit des places de marché en ligne, des moteurs de recherche en ligne et des services d'informatique dans les nuage (*Ibid.*).

[2279] Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique (*JORF* n° 0118 du 25 mai 2018).

[2280] Annexe du Décret n° 2018-384 du 23 mai 2018.

[2281] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (*JORF* n° 0294 du 19 déc. 2013, p. 20570).

[2282] V. *infra*, n° ¤.

[2283] V. <https://www.ssi.gouv.fr/entreprise/protection-des-oiv/les-regles-de-securite/> (dernière consultation le 8 oct. 2019).

2 - La référence aux normes techniques et managériales au niveau national

457. Un tableau impressionniste. Indépendamment des règles juridiques clairement identifiables – dont nous avons traité tout au long de notre étude – et qui composent la notion de « secret médical » telle qu'entendue par la doctrine, nous avons expliqué par ailleurs que l'obligation de sécurité et de confidentialité qui pèse sur les responsables de traitement et les sous-traitants imposait la mise en œuvre de moyens techniques et organisationnels. Il a été, à ce titre, évoqué l'importance des guides de bonnes pratiques et référentiels, et la présence de plus en plus évidente des normes technico-managériales. La participation des instances nationales aux travaux de normalisation à toutes les échelles et l'élaboration participative des outils de régulation dessinent un paysage complexe et mouvant. Il s'agit à présent d'identifier, au moins partiellement, la multiplication des renvois aux normes techniques dans les instruments de droit souple ainsi que les références à la normalisation, de plus en plus évidentes, dans les textes législatifs. La mise en œuvre de la sécurité et de la confidentialité des données à caractère personnel dans le domaine de la santé s'apparente de plus en plus, pour reprendre l'expression de Monsieur Frydman, à un « *bestiaire normatif* »[2284].

458. Les références dans les instruments de droit souple applicables au domaine de la santé numérique. L'interaction entre les normes techniques et les règles juridiques se perçoit d'abord au travers des références qui sont faites dans les instruments de droit souple forgés par l'ASIP-santé. Concernant les hébergeurs de données de santé[2285], l'ASIP-santé diffuse un référentiel pour la certification, les organismes accrédités pouvant ensuite certifier les hébergeurs qui y prétendent. La procédure consiste en une évaluation de conformité au référentiel. En France, le COFRAC (Comité français d'accréditation) est notamment accrédité pour délivrer ces certifications, comme c'est le cas d'autres organismes européens. Le rôle des organismes d'accréditation est un marqueur de l'importance des normes technico-managériales puisque le référentiel s'appuie presque entièrement sur des normes ISO relatives à la sécurité des systèmes d'information et à la protection des données[2286]. Il faut enfin noter qu'héberger

---

[2284] B. FRYDMAN, « Comment penser le droit global ? », *in* B. FRYDMAN et J.-Y. CHEROT (ss la dir.), *La science du droit dans la globalisation*, coll. Penser le droit, Bruylant, 2012, p. 18.
[2285] CSP art. L. 1111-8. Avant la loi de modernisation de notre système de santé du 26 janvier 2016 (loi n° 2016-41 du 26 janvier 2016) et l'ordonnance du 12 janvier 2017 prise en vertue de celle-ci
[2286] Par exemple : ISO 27001 « système de gestion de la sécurité des systèmes d'information » ; ISO 20000 « système de gestion de la qualité des services » ; ISO 27018 « protection des données à caractère personnel ».

des données de santé sans avoir la certification – ou l'accréditation avant la loi du 26 janvier 2016 – constitue une infraction pénale[2287].

Le cadre de l'interopérabilité des systèmes d'information de santé (CI-SIS) est digne d'être également mentionné. Ce dernier est défini par un référentiel technique de l'ASIP-santé qui s'appuie sur des normes et standards internationaux et nationaux et contribue à normaliser l'interopérabilité technique, « *qui porte sur le transport des flux et sur les services garantissant l'échange et le partage des données de santé dans le respect des exigences de sécurité et de confidentialité des données personnelles de santé* »[2288]. Ensuite, les référentiels qui composent la PGSSI-S définissent, entre autres, les exigences techniques et organisationnelles de sécurité et de confidentialité, non seulement en ce qui concerne les SI mais également pour tous les dispositifs techniques et les outils – tels que la Carte professionnelle de santé – participant ainsi à identifier, authentifier et habiliter les personnes et leur permettre d'accéder aux données ou de les faire circuler. Ces référentiels sont formés sur la base de normes techniques et managériales qui sont, en grande partie, des normes ISO ou ETSI, mais s'y trouvent aussi des normes issues d'autre organismes de normalisation privés[2289]. Il est, par ailleurs, intéressant de noter que le document portant sur les principes fondateurs de cette politique générale affirme que « *Tout acteur de santé est responsable de la sécurité des informations qui lui sont confiées* […]. *Le développement des technologies de l'information* ***nécessite de reformuler l'application du secret professionnel*** *pour les nouveaux usages de l'information dans le domaine de la santé* »[2290]. Cette reformulation éclaire, à notre sens, le glissement qui s'opère au contact des normes technico-managériales. Il s'agit en effet *d'appliquer* le secret professionnel, tandis que le texte d'incrimination ne fait que décrire un comportement prohibé.

459. Management de la sécurité des données dans le domaine de la santé. La première étape du management des risques en matière de traitement de données consiste, nous l'avons

---

L'ASIP-santé précise en outre que la certification délivrée aux hébergeurs « *est complétée de quelques points de contrôles adaptés à la particulière sensibilité des données de santé* » (ASIP-santé, Communiqué de presse, *Pourquoi passer directement à la certification ?*, 9 févr. 2018)

[2287] CSP, art. L. 1115-1.

[2288] <https://esante.gouv.fr/interoperabilite/ci-sis> (dernière consultation le 8 oct. 2019).

[2289] En général sur le fondement des référentiels et guides de bonne pratique mis en œuvre par l'ANSSI, qui sont eux-mêmes assis sur de telles normes. V. *infra*, n°¤.

[2290] ASIP-santé, Principes fondateurs, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), juill. 2013, V 1.0., p. 14 (Nous soulignons).

vu, dans la mise en œuvre des études d'impact. De notre point de vue, quant à l'obligation *d'assurer le respect du secret professionnel*, d'une part, et de garantir le respect du secret des données couvertes par ce secret, d'autre part, il s'agit : d'identifier les personnes pouvant accéder aux données, de les authentifier et ensuite de les habiliter à y accéder ; de fixer *a priori* le circuit des données directement identifiantes dans la limite des exigences légales du secret partagé telles que prévues par le Code de la santé publique et au regard du *partage technique* explicité en amont. Pour ce faire, il est nécessaire de mettre en place la certification des identités et de respecter les politiques d'habilitation des accès[2291]. Il faudra, en toutes hypothèses, « *établir des mécanismes qui organisent efficacement les pratiques et qui en assurent l'effectivité par des audits réguliers* »[2292]. Si la *privacy by design* requiert la mise en œuvre de mesures techniques et organisationnelles, il est toutefois difficile pour le juriste de concevoir avec exactitude ce qui relève de la technique et ce qui relève de l'organisation, donc du management. C'est que les deux moyens d'assurer la sécurité et la confidentialité sont *intrinsèquement liés*, et que les sources des normes qui déterminent ces moyens en fonction de « *l'état des connaissances* »[2293] sont identiques. Ce sont encore principalement les référentiels et guides de l'ASIP-santé qui prescrivent les moyens de gestion estimés les plus appropriés.

Au sein des référentiels et guides de l'ASIP-santé qui composent, pour la grande majorité, la Politique Générale de Sécurité des Systèmes d'Information de Santé, se trouve par exemple un référentiel d'identification des acteurs sanitaires et médico-sociaux[2294] et des seuls acteurs de santé[2295]. L'identification des personnes dans le contexte de la sécurité est liée à l'authentification pour la mise en œuvre des droits d'accès au système d'information. Les référentiels listent les enjeux de l'identification : celle-ci permet d'accorder un accès au système aux seules personnes autorisées – c'est-à-dire au regard des dispositions du Code de la santé publique –, de différencier les possibilités d'accès aux services et aux données de santé en fonction des droits attachés à l'identité de ces utilisateurs, et de pouvoir imputer les actions à leur auteur. Ainsi « *la qualité de l'authentification d'un acteur de santé conditionne donc la*

[2291] *Ibid.*
[2292] *Ibid.*
[2293] Art. 25 du RGPD.
[2294] ASIP-Santé, *Référentiel d'identification des acteurs sanitaires et médico-sociaux*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), déc. 2014, V1.0.
[2295] ASIP-Santé, *Référentiel d'authentification des acteurs de santé*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), déc. 2014, V2.0

maîtrise des accès au SIS (SI de Santé) ». La PGSSI-S comporte également un *référentiel d'imputabilité* qui permet de mettre en place un *dispositif d'imputabilité* « *capable d'établir des traces, de les conserver et de les rendre accessibles à des personnes autorisées* [et qui] *répond principalement à deux besoins : vérifier l'utilisation du système d'information et augmenter la confiance des utilisateurs (ex. montrer qu'une information n'a été consultée ou modifiée que dans le cadre d'une action légitime, …); produire des preuves électroniques dans le cadre d'une action en justice* »[2296]. Cette démarche est justifiée en ce que « *le besoin d'imputabilité est d'autant plus important que le système d'information est partagé par un nombre important d'utilisateurs disposant de rôles et d'habilitations distinctes augmentant le risque de mésusage* »[2297]. Au titre des guides et des référentiels, doivent aussi être cités le Guide pratique des règles pour les dispositifs connectés d'un système d'information de santé[2298], le Guide des mécanismes de protection de l'intégrité des données stockées[2299] et le Guide de gestion des habilitations d'accès au système d'information[2300]. Dans tous les exemples donnés, les exigences techniques fixées par l'ASIP-santé sont accompagnées d'exigences relatives à la gestion des accès, de l'échange, du partage, du transport de données, ce qui correspond à des normes de management. Enfin, pour déterminer les mesures organisationnelles appropriées, l'ASIP-santé s'appuie sur la suite ISO/CEI 27000[2301] qui englobe un corpus de normes

---

[2296] ASIP-Santé, *Référentiel d'imputabilité*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), déc. 2014, V1.0, p. 7.
[2297] *Ibid.*
[2298] ASIP-Santé, *Guide Pratique Règles pour les dispositifs connectés d'un Système d'Information de Santé*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), nov. 2013, V1.0. Remarquons que le terme d'*imputabilité* est déconnecté de son origine juridique qui renvoie au « *caractère de ce qui peut être mis au compte d'une personne comme une faute* […] » (*V°* « Imputabilité », *in* G. CORNU (ss la dir.), *Vocabulaire juridique*, 9e éd., coll. Quadrige, PUF, 2011). L'imputabilité vise ici la traçabilité, c'est-à-dire la possibilité de savoir qui a effectué quelle action au sein du système, il n'est donc pas question de faute mais de suivi et d'enregistrement des actions.
[2299] ASIP-Santé, *Guide des mécanismes de protections de l'intégrité des données stockées*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), janv. 2017, V1.0.
[2300] ASIP-Santé, *Guide gestion des habilitations d'accès au SI*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), janv. 2017, V1.0.
[2301] ASIP-santé, *Principes fondateurs Politique Générale de Sécurité des Systèmes d'Information de Santé* (PGSSI-S), juill. 2013, V1.0.

ISO/CEI[2302]. Elle contient des normes de management de l'information et forme un *système de Management de la Sécurité de l'Information*[2303].

460. Les normes technico-managériales et les logiciels intégrant un dispositif médical, une réflexion conjointe de tous les acteurs. Si les dispositifs médicaux font l'objet d'une normalisation importante quant à leur qualité intrinsèque[2304], la réflexion sur la cybersécurité et la confidentialité de ces outils lorsqu'ils intègrent un logiciel – qu'ils soient ou non connectés[2305] – est récente. Des initiatives ont été prises afin de mener une réflexion au niveau national et à destination principale des industriels, les démarches étant toutes guidées par une volonté de développer la *privacy* et la sécurité dès la conception des dispositifs. Un groupe de travail sous l'égide du Conseil Stratégique des Industies de santé et réunissant plusieurs instances publiques et privées a proposé le recours à la normalisation comme mode de régulation pour garantir la cybersécurité des objets connectés et des applications mobiles en

---

[2302] Commission électrotechnique internationale.

[2303] Pour n'en citer que quelques unes : ISO/CEI 27001 : Norme d'exigences des SMSI, permettant la certification (publiée en 2005, révisée en 2013) ; ISO/CEI 27002 : Guide des bonnes pratiques en SMSI (précédemment connu sous le nom de ISO/CEI 17799, et avant BS 7799 Partie 1 (renuméroté en ISO/CEI 27002:2005 en juill. 2007, dernière révision en 2014) ; ISO/CEI 27003 : Guide d'implémentation d'un SMSI, publié le 3 févr. 2010 révisée en 2017 (Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information) ; ISO/CEI 27004 : Norme de mesures de management de la sécurité de l'information (publiée le 12 juill. 2009, révisée en 2016) ; ISO/CEI 27005 : Norme de gestion de risques liés à la sécurité de l'information (publiée le 4 juin 2008, révisée en 2018).

[2304] Ce qui est d'ailleurs rappelé dans le règlement européen relatif aux dispositifs médicaux : « *Compte tenu du rôle important de la normalisation dans le domaine des dispositifs médicaux, le respect des normes harmonisées définies dans le règlement (UE) nº 1025/2012 du Parlement européen et du Conseil devrait être un moyen pour les fabricants de prouver qu'ils respectent les exigences générales en matière de sécurité et de performances et les autres exigences légales, notamment celles en matière de gestion de la qualité et des risques, énoncées dans le présent règlement* » (Cons. 22, PE et Cons. Règlement (UE) n° 2017/745 du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE).

[2305] Le dispositif médical est défini par le règlement européen comme « *tout instrument, appareil, équipement, logiciel, implant, réactif, matière ou autre article, destiné par le fabricant à être utilisé, seul ou en association, chez l'homme pour l'une ou plusieurs des fins médicales précises suivantes: diagnostic, prévention, contrôle, prédiction, pronostic, traitement ou atténuation d'une maladie ; diagnostic, contrôle, traitement, atténuation d'une blessure ou d'un handicap ou compensation de ceux-ci ; investigation, remplacement ou modification d'une structure ou fonction anatomique ou d'un processus ou état physiologique ou pathologique ; communication d'informations au moyen d'un examen in vitro d'échantillons provenant du corps humain, y compris les dons d'organes, de sang et de tissus, et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens. Les produits ci-après sont également réputés être des dispositifs médicaux : les dispositifs destinés à la maîtrise de la conception ou à l'assistance à celle-ci ; les produits spécifiquement destinés au nettoyage, à la désinfection ou à la stérilisation des dispositifs* » (art. 2.1., PE et Cons. Règlement (UE) n° 2017/745).

santé[2306]. Le Conseil national de l'Ordre des médecins, dans son livre blanc dédié à la e-santé, a proposé également le recours à une régulation par les standards à l'échelle européenne[2307]. L'ANSM s'est saisie de la question, mais son intervention concerne plus spécifiquement les risques que des attaques extérieures pourraient générer pour les patients utilisant ce type de produit[2308]. Ses recommandations portent donc principalement sur les autres critères de la cybersécurité que sont la disponibilité et l'intégrité des données[2309]. Enfin, la Haute autorité de santé a formulé des recommandations de bonnes pratiques – après des travaux menés conjointement avec l'ANSSI et la CNIL – portant plus largement sur les objets connectés en santé, dont les dispositifs médicaux. Le rôle des normes techniques y est souligné à tous les niveaux[2310]. Le rapport de l'ANSM publié à l'état de projet en juillet 2019 renvoie, pour ce qui concerne la sécurité et la confidentialité des données à caractère personnel, aux travaux de l'ANSSI, laquelle participe activement aux travaux de normalisation nationaux, européens et internationaux[2311].

461. Interopérabilité, sécurité et confidentialité. Il nous faut enfin, pour compléter ce tableau qui n'a pas vocation à être exhaustif, apporter deux précisions. La première tient aux missions de la Plateforme des données de santé créée par la loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé[2312]. L'article 41 de la loi modifiant l'article L. 1462-1 du Code de la santé publique afin de préciser les missions du groupement d'intérêt public « Plateforme des données de santé » qui se substitue à l'Institut national des

---

[2306] Plus largement, les travaux du groupe ont proposé le recours au *droit souple*. La normalisation y est explicitement envisagée à plusieurs reprises par les différentes instances ayant participé à la réflexion (v. GT 28 CSF, Rapport : *Créer les conditions d'un développement vertueux des objets connectés et des applications mobiles en santé*, 2016, disponible sur <https://solidarites-sante.gouv.fr/IMG/pdf/rapport-gt28-octobre-2016-vf-full.pdf> (dernière consultation le 8 oct. 2019)).

[2307] CNOM, *Santé connectée. De la e-santé à la santé connectée*, Livre Blanc, janv. 2015, p. 25 et 29. V. également A. MENDOZA-CAMINADE, « Big data et données de santé : quelles régulations juridiques », *RLDI* 2016, n° 127.

[2308] Un comité scientifique spécialisé temporaire sur la cybersécurité des logiciels dispositifs médicaux a été créé au sein de l'ANSM.

[2309] ANSM, Recommandations (Projet), *Cybersécurité des dispositifs médicaux intégrant du logiciel au cours de leur cycle de vie*, juill. 2019, p. 14.

[2310] Par exemple, pour la mise en œuvre de l'interopérabilité, la place des normes issues du consortium privé *Health Level 7*, également sollicitées par l'ASIP-santé.

[2311] ANSSI, *Rapport d'activité 2015*, p. 14.

[2312] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (*JORF* n° 0172 du 26 juillet 2019).

données de santé, précise que l'une des missions de la Plateforme est de « *diffuser les normes de standardisation pour l'échange et l'exploitation des données de santé, en tenant compte des standards européens et internationaux* »[2313]. Ces normes visent l'interopérabilité, laquelle doit permettre de garantir l'échange, le partage, la sécurité et la confidentialité[2314] des données de santé à caractère personnel, comme le mentionne encore l'article L. 1110-4-1 du Code de la santé publique. La place de cet article – suivant directement l'article relatif au « secret médical » – et sa modification par la loi du 24 juillet 2019 attestent du rôle essentiel de la normalisation comme moyen d'assurer le secret, porté par une *logique incitative* consistant à « *instituer une certification de la conformité des logiciels de santé aux référentiels d'interopérabilité et de sécurité par des organismes de certification privés dûment accrédités par le comité français d'accréditation. Les éditeurs pourront solliciter cette certification sur une base volontaire* » et « *conditionner à l'obtention de ce certificat le bénéfice de fonds publics pour l'acquisition du logiciel concerné, notamment dans le cadre du fonds régional d'intervention (FIR) ou des grands programmes ministériels tels que le plan "Hôpital numérique" (HOP'EN), le plan "e-parcours", l'incitation financière pour l'amélioration de la qualité (IFAQ)* »[2315]. Il nous semble que le mouvement que nous avons essayé de décrire déploie une autre de ces faces. L'interopérabilité et la sécurité des dispositifs techniques, qui consiste dans la confidentialité des données, leur disponibilité et leur intégrité vont constituer des indicateurs de performance et de qualités des établissements et des industries françaises dans le domaine de la santé numérique.

B - La référence au RGPD dans la norme technique

462. La norme ISO 27701 et les normes de management. Si l'on ne peut, car l'exercice nécessiterait un travail approfondi et pluridisciplinaire, se prononcer sur l'impact juridique ou

---

[2313] CSP, art. L. 1462-1.

[2314] Concernant spécifiquement l'interopérabilité des dossier médicaux à l'échelle européenne : « *Les systèmes de dossiers de santé informatisés et les solutions d'interopérabilité doivent garantir la confidentialité des données à caractère personnel concernant la santé et être conformes à tous les aspects de la législation relative à la protection des données, dès la phase de conception* » (Recommandation (UE) 2019/243 DE LA COMMISSION du 6 février 2019 relative à un format européen d'échange des dossiers de santé informatisés, *JORF* 11 fév. 2019, L 39/18, Annexe).

[2315] A. MILON, Rapport fait au nom de la commission des affaires sociales sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif à l'organisation et à la transformation du système de santé, 22 mai 2019, p. 191.

la réception des normes ISO/CEI relatives au management des systèmes d'information par les acteurs du numérique en santé, il a été souligné leur place au sein des référentiels et guides de bonnes pratiques, ce qui confirme leur fonction de levier de création de la confiance dans le numérique en santé. Il faut également noter qu'une norme récente à été ajoutée à cette série, la norme ISO/IEC 27701, dite « *management de la protection de la vie privée* »[2316], dont l'objectif est la conformité au RGPD. La CNIL a participé à l'élaboration de cette norme. Monsieur Grall, actuel chef de service du département d'expertise technologique de la CNIL, estime – dans la lignée de nos propos précédents – que cette norme doit contribuer à accompagner les responsables de traitement vers la *compliance*. Il affirme ainsi que « *les organisations doivent prouver aux autorités, à leurs partenaires, clients et collaborateurs qu'elles sont dignes de confiance. Or cette norme contribuera fortement à inspirer cette confiance* »[2317]. En somme, il est désormais évident que le management de la sécurité des données et de la protection de la vie privée va contribuer à la protection du secret des données issues de la relation de soin.

Section 2 - Gestion du risque et migration des normes

463. Contexte. Nous avons expliqué que la sécurité et la confidentialité formaient un couple : la sécurité des dispositifs techniques supportant le traitement des données conditionne en partie le respect de la confidentialité puisqu'elle entend préserver les données des atteintes ; par ailleurs, l'obligation de confidentialité, puisqu'elle consiste à s'assurer que seules les personnes autorisées accèdent aux données, exige du responsable de traitement de veiller à *l'application* du secret professionnel. Assurer la sécurité des systèmes, des données et des services, par rapport aux actions des tiers, et garantir la confidentialité des données couvertes par le secret, c'est-à-dire remplir la fonction de secret « moyen » sont les deux facettes de ce que recouvre la garantie du « secret médical ». La mise en œuvre des mesures techniques nécessaires à garantir, entre autres, cette double exigence doit être assurée dès la conception, c'est-à-dire être intégrée aux dispositifs et dans l'architecture des réseaux. En d'autres termes, cette mise en œuvre implique à la fois d'utiliser des techniques adaptées aux risques identifiés, mais également de penser l'architecture technique des dispositifs, de sorte à prévenir les atteintes à la sécurité et à

[2316] ISO/IEC 27701:2019 Techniques de sécurité – Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée – Exigences et lignes directrices, août 2019.
[2317] <https://www.iso.org/fr/news/ref2419.html> (dernière consultation le 8 oct. 2019).

la confidentialité des données couvertes par le secret. Les moyens mis en œuvre sont donc bien des secret « moyen ». Cette mise en œuvre est un des aspects de la *Privacy and security by design*, l'autre aspect consistant dans les mesures organisationnelles qui impliquent un management de la sécurité et de la protection des données. Ces mesures s'appliquent à l'échelle des organisations ou des entreprises dont le fonctionnement dépend du traitement des données et du système d'information qui le supporte. Dans le système de santé, ce sont les structures du système de santé et médico-social, et les modes de coopération – réseaux de santé, Groupement Hospitalier de Territoire – dans toute leur diversité[2318], mais aussi les organisations formées spécialement aux traitements des données issues du système de santé dans le contexte du *Big data*, telles que la Plateforme des données de santé. Le développement d'une « *culture de la gestion des risques* »[2319] implique la mise en œuvre d'une politique de sécurité. Dans le domaine de la santé, elle est en partie formalisée sur la base d'un référentiel de l'ASIP-santé et consiste notamment dans la gestion des habilitations d'accès, l'identification et l'authentification des personnes ainsi que la traçabilité des accès. Nous avons pu constater que ces deux types de moyens – techniques et organisationnels – faisaient l'objet d'une normalisation qualifiée de « technico-managériale ». Nous avons tracé les linéaments d'un phénomène où s'enchevêtrent des normes que l'on qualifie de juridiques – dont le droit souple émanant des agences de l'Etat – et des normes technico-managériales. Il importe de compléter la description de ce mouvement pour y inscrire notre objet d'étude : le secret comme moyen de protection. Nous souhaitons préciser que les développements n'auront pas pour objet d'affirmer mais simplement de tenter, là encore, d'esquisser la direction possible du phénomène. Pour partager les utilités des données tout en assurant le secret, c'est une approche managériale et collective qui est mise en œuvre **(paragraphe 1)**. Enfin, l'implémentation du secret dans les choses aurait pour conséquence de rendre inutile, au moins pour assurer le secret des données, la norme juridique du secret professionnel **(paragraphe 2)**.

[2318] Pour un panorama des structures de coopération v. notamment C. EVIN, « Les nouveaux outils d'une politique territoriale de santé : un mille-feuille qui a besoin d'une mise en cohérence », *RDSS* 2017, p. 107.
[2319] Ph. PUCHERAL, A. RALLET, F. ROCHELANDET et C. ZOLYNSKI, « La Privacy by design : une fausse bonne solution aux problèmes de protection des données personnelles soulevés par l'Open data et les objets connectés ? », *Legicom* 2016/1, n° 56, pp. 89-99.

§ 1 - Une approche managériale et collective du secret des données à caractère personnel dans le domaine de la santé

464. Un changement d'échelle. La perte de maîtrise des informations par les professionnels de santé[2320] s'accompagne nécessairement d'une forme de transfert des responsabilités dans le contexte d'une coopération accrue des acteurs du système de santé et médico-social, et d'une « *médecine de parcours* »[2321], personnalisée et prédictive, portée par les *Big data*. Le traitement des données s'effectue à des échelles de plus en plus importantes et, en dehors des hypothèses de traitement de données à l'échelle d'un cabinet d'exercice libéral, le responsable de traitement sera, le plus souvent, une personne morale (établissement public ou privé, fondation, association, groupement d'intérêt public), ce qui accroît le recours à la sous-traitance. Si les données issues de la prise en charge des personnes sont considérées comme un « *bien commun* »[2322], la garantie du secret de ces données devient une *question collective*, d'autant que leur traitement en masse peut révéler des informations non plus seulement sur une personne déterminée mais sur d'autres individus. La méthodologie *by design* de la protection des données et de la sécurité « *promeut le principe de prévention comme clé de voûte de la* compliance *des projets reposant sur l'usage des données personnelles en ce qu'elle impose un devoir d'action au responsable de traitement tenu de se conformer à la réglementation dès la conception du système et tout au long du développement du produit ou du service* »[2323]. Cette anticipation implique, selon Madame Zolynski, une gestion et une veille du risque informationnel[2324] par les responsables de traitement, d'une part, et par les industriels, d'autre part. Elle nécessite, en outre, l'adoption d'instruments de régulation plus efficaces, lesquels consistent, dans le secteur de la santé, en des référentiels et guides de bonnes pratiques et des normes technico-managériales. Ces normes sont « *pensées collectivement par les acteurs du secteur en*

[2320] V. *supra* n° 363 et svt.
[2321] « *La mise en oeuvre d'une médecine de parcours impose une meilleure coordination territoriale entre l'ensemble des offreurs de soins afin de faciliter la continuité des prises en charge : entre les établissements de spécialisations et de niveaux de recours différents et naturellement aussi entre ces établissements et les professionnels de santé, sociaux et médico-sociaux* » (C. EVIN, « Les nouveaux outils d'une politique territoriale de santé : un mille-feuille qui a besoin d'une mise en cohérence », *op. cit.*).
[2322] V. *supra* n° 379 et svt.
[2323] C. ZOLYNSKI, « La Privacy by Design appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel ? », *Dalloz IP/IT* 2016, p. 404.
[2324] *Ibid.*

adéquation avec les pratiques et leur évolutivité découlant de l'accélération des cycles d'innovation »[2325]. Ce qui se dessine, en ce qui concerne notre objet d'étude, nous semble correspondre à une gestion collective du secret des données à caractère personnel dans le domaine de la santé **(B)**. Plus généralement, la convergence entre management et droit dans le domaine de la protection des données est un symptôme de ce processus **(A)**.

A - Le *Data management* et la gouvernance des données

465. ***Law and management*, gestion du risque juridique et *compliance*.** L'approche dite *Law and mangement* participe du rapprochement entre le droit et l'univers économique. Dans la doctrine française, elle reste néanmoins dans l'ombre de l'analyse économique du droit dont l'étude est bien plus investie[2326]. L'approche Droit et management est un « *courant d'analyse original visant à mettre en évidence les ressorts juridiques de la performance des entreprises* »[2327]. Adopter cette approche a pour intérêt de déterminer « *la probabilité que survienne un événement extérieur à la volonté de l'entreprise, susceptible de modifier sa situation juridique et d'avoir des répercussions économiques pour elle* »[2328]. Dans cette optique, les auteurs ont opéré une classification des risques juridiques au regard de leurs conséquences, de leurs sources ou de leur gravité pour l'entreprise[2329]. A la recherche du profit, l'entreprise considère ainsi le droit comme un instrument au service de cette finalité : « *Dans la défense de leurs intérêts particuliers les entreprises peuvent instrumentaliser le droit pour en faire un levier majeur de leur développement* »[2330]. La *compliance* peut alors s'avérer être une stratégie

---

[2325] *Ibid.*

[2326] « *Apparue dans les années soixante dans les universités américaines, elle consiste à appliquer les outils d'analyse et les critères de jugement des économistes à l'explication et à l'évaluation des règles juridiques. L'apport central de ce champ de recherche est donc d'utiliser la théorie microéconomique afin de prédire comment les agents réagissent aux prix implicites contenus dans les règles et les normes juridiques, tout comme la théorie microéconomique cherche à expliquer comment les agents réagissent aux prix explicites du marché. À titre d'illustration, l'économiste du droit cherche à mesurer si des sanctions plus sévères et plus certaines découragent les actes délictueux et si les règles d'indemnisation des victimes, via la responsabilité civile, incite les agents à adopter un niveau de précaution socialement efficace. Il s'agit donc d'une approche dynamique du droit qui invite à repenser la fonction régulatrice des institutions et des règles juridiques*. » (B. DEFFAINS, Le défi de l'analyse économique du droit : le point de vue de l'économiste, *LPA* 2005, n° 99, p. 6 ; v. également sur l'analyse économique du droit : S. FEREY, *Une histoire de l'analyse économique du droit*, Bruylant, 2008).

[2327] A. MASSON et H. BOUTHINON-DUMAS, « L'approche « Law & Management » », *RTD com.* 2011, p. 233.

[2328] A. MASSON et H. BOUTHINON-DUMAS, « L'approche « Law & Management » », *op. cit.*

[2329] *Ibid.* ; *Adde* H. BIDAUD, P. BIGNON, et J.-P. CAILLOUX, *La fonction juridique et l'entreprise*, Eska, 1995.

[2330] A. MASSON et H. BOUTHINON-DUMAS, « L'approche « Law & Management » », *op. cit.* Dans une réflexion bien plus vaste, Monsieur Ost mentionne cette approche instrumentale du droit, enseignée dans les écoles de management (F. OST, *A quoi sert le droit ? Usages, fonctions, finalités*, coll. Penser le droit, Bruylant, 2016, p. 86).

intéressante pour les entreprises qui, developpant une politique de gestion des risques, construisent une culture juridique au sein de leur organisation. Comme l'explique Madame Frison-Roche, « *La répression, d'essence* ex post*, est transférée dans l'entreprise qui s'auto-surveille, s'auto-évalue et s'auto-sanctionne ou/et s'auto-dénonce. Cela peut correspondre à une politique de l'entreprise, si les buts poursuivis par les régulations ainsi internalisées sont également poursuivis par l'entreprise à travers l'adoption spontanée de codes de conduite, et ce d'autant plus qu'elle adopterait une responsabilité sociétale ou mettrait en œuvre en tant qu'actionnaire une volonté politique « responsable »* »[2331].

466. ***Digital law and management*. La conformité au RGPD présentée comme un enjeu stratégique pour les entreprises.** Si l'entrée en vigueur du RGPD et la *mise en conformité* des structures aux dispositions relatives au traitement des données à caractère personnel a fait l'objet d'une production doctrinale importante, la couverture médiatique a également été retentissante. Il s'est créé, en peu de temps, un véritable *business* de la mise en conformité au RGPD[2332], et la concurrence s'avère aussi normative[2333]. Le règlement n'imposant que la *mise en œuvre des mesures techniques et organisationnelles*, il revient donc aux responsables de traitement de déterminer la stratégie la mieux à même de prévenir les risques inhérents à leur traitement une fois ceux-ci identifiés. Au-delà des difficultés qu'elle présente pour les responsables de traitement, la *compliance* dans le domaine de la protection des données est présentée comme un atout concurrentiel[2334]. Normes technico-managériales, label et

---

[2331] M.-A. FRISON-ROCHE, « Compliance et personnalité », *D.* 2019, p. 604 ; *Adde* V. LEFEBVRE-DUTILLEUL, « La conformité, droit vivant », *in* C. ROQUILLY (ss la dir.), *La contribution des juristes et du droit à la performance de l'entreprise. Management juridique et culture juridique de l'entreprise*, coll. Pratique des affaires, Joly éd., 2011, p. 307 : « *La mise en place d'une politique de* compliance *contribue à identifier et corriger les dysfonctionnements internes. Facteur de sécurité et de différentiation concurrentielle, la conformité est aussi à terme source de performance durable* ».

[2332] C'est surtout la presse spécialisée qui s'est faite l'écho du phénomène : J.-F. CAILLARD, « Le RGPD, et si c'était aussi une opportunité de business ? », *Forbes Magazine*, 13 avr. 2018 ; S. ROLLAND, « Protection des données : le chaotique business de la conformité RGPD », *La tribune*, 25 mai 2018.

[2333] En témoigne notamment le *catalogue* de normes publié par l'AFNOR et intitulé *guide* : AFNOR, *Protection des données personnelles : l'apport des normes volontaires* », avr. 2018. Notons au passage que la présentation du guide mentionne l'implication de la CNIL, et Monsieur Grall, chef du service d'expertise technologique de la CNIL, précise que « *Demain, ces normes seront incontournables pour mettre en place un système de management en sécurité informatique, cadre de progrès qui devra notamment intégrer la protection des données personnelles* » (<https://normalisation.afnor.org/actualites/protection-donnees-personnelles-guide-afnor-recense-normes-incontournables/> (dernière consultation le 8 oct. 2019)).

[2334] Quelques exemples : « *L'étude d'impact constituera par ailleurs un outil stratégique de développement. L'entreprise ayant réalisé un PIA présentera un avantage concurrentiel par rapport aux autres. Dans un contexte*

certification sont alors le signe extérieur de la *confiance* que l'on peut attribuer à certains acteurs plutôt qu'à d'autres.

467. Gestion du risque informationnel. En matière de protection des données, « *les entreprises doivent intégrer la protection des données personnelles dans leurs politiques et pratiques, comme un élément de leur responsabilité sociale. Le principe de* privacy by design *est alors l'autre principe directeur de la* compliance »[2335]. Ajoutons que la sécurité des systèmes d'information participe de la même démarche. Le *management* de la protection des données consiste alors dans « *l'adoption de stratégies internes à l'entreprise de façon à y associer les salariés, et des procédures de monitoring* »[2336]. La gestion du risque lié à la sécurité des dispositifs techniques et à la confidentialité des données[2337] s'est donc développée, depuis l'entrée en vigueur du RGPD, dans toutes les structures publiques ou privées. L'on évoque alors la « gouvernance des données » comme synonyme de la gestion ou du management. Si la mise en œuvre d'une gestion des données à caractère personnel contribue à maîtriser un risque juridique pour l'entreprise, il s'agit également de maîtriser le *risque informationnel*[2338]. Le risque visé n'est pas celui de la pratique de l'intelligence économique[2339] et ne consiste pas à

---

de recrudescence de la cybercriminalité et de failles de sécurité des systèmes d'information, le PIA apparaît comme une garantie de conformité non négligeable » (G. HAAS et A. DUBARRY, « Confidentialité et protection des données », *Dalloz IP/IT* 2017, p. 322) ; « *Les entreprises doivent s'efforcer de vivre la « contrainte régulatoire » comme une exigence pouvant leur procurer un avantage concurrentiel distinctif* » (Entretien, « Réussir la mise en œuvre du RGPD : l'enjeu majeur de cette année pour la CNIL.- 3 questions à Marie-Laure DENIS, présidente de la Commission nationale de l'informatique et des libertés », *Comm. com. électr.* 2019, n° 6, entretien 6) ; R. GOLA, « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *Legicom* 2017/2, n° 59, pp. 29-38.

[2335] K. FAVRO, « La démarche de compliance ou la mise en œuvre d'une approche inversée », *Legicom* 2017/2, n° 59, Pp. 21-28.

[2336] *Ibid.*

[2337] Dans notre cas, il s'agit de s'assurer l'application du secret professionnel des acteurs du système de santé et de garantir la confidentialité contre les atteintes.

[2338] C. ZOLYNSKI, « La Privacy by Design appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel ? », *op. cit.*

[2339] L'intelligence économique est un mode de gestion stratégique des informations. Au sein d'une entreprise, elle combine le renseignement, l'influence et la protection de l'information. L'information y est utilisée comme un pouvoir mais également comme un risque pour l'entreprise. L'intelligence économique recèle ainsi une fonction de protection de l'information : « *La fonction de protection (ou gestion du risque informationnel) sert à protéger les informations détenues ou émises par l'entreprise, notamment de leur appropriation par les concurrents. La fonction de gestion du risque informationnel préserve ainsi l'asymétrie d'information au profit de la firme qui gère ce risque. Elle revient à assurer la sûreté et la sécurité informationnelle de l'entreprise. Là encore, pas de sensationnalisme. La gestion des brevets fait partie de l'arsenal défensif d'une entreprise et protège la connaissance technique (avec quelques paradoxes liés à la révélation du contenu technique lors de la publication du brevet). Les clauses de confidentialité, les restrictions d'accès aux locaux, les fire-walls constituent des exemples d'outils à la disposition des managers pour protéger les informations* » (S. LARIVET, « L'intelligence économique : un concept managérial », *Market Management* 2006/3, vol. 6, p. 23).

protéger les informations stratégiques de l'entreprise mais les données à caractère personnel traitées. « *Les risques principaux attachés à la génération de telles données sont communs à l'ensemble de ces supports et concernent un ensemble de mésusage des données tels que la possible ré-identification des données anonymisées, les atteintes à la confidentialité ou encore de potentielles discriminations. Il s'agit donc bien ici d'un risque particulier, de type « informationnel » lié au potentiel mésusage de la donnée* »[2340]. Si les données à caractère personnel peuvent également avoir une valeur stratégique pour les structures responsables de traitement, la gestion du risque informationnel se fait dans « *l'intérêt des êtres humains institués en personnes titulaires de droits* »[2341].

B - La mise en œuvre de la gestion collective des données

468. Management de la sécurité et de la confidentialité des données dans le secteur de la santé, confiance et souveraineté numérique nationale et européenne. La rupture de confidentialité des données couvertes par le secret professionnel, qu'elle soit due à un mésusage, à un acte intentionnel (révélation ou réidentification) ou à une atteinte extérieure à la structure est alors appréhendée à la fois comme un risque juridique et comme un risque informationnel géré dans l'intérêt des patients. L'évaluation des risques est obligatoire dans certains cas, le traitement des données à caractère personnel dans le domaine de la santé étant particulièrement concerné. L'on sait par ailleurs que, dans le secteur de la santé, la gestion de la sécurité et de la confidentialité fait l'objet d'une politique publique dont le *droit souple* et les normes techniques sont le levier. Les responsables de traitement sont ainsi fortement guidés, incités financièrement, à se tourner vers les agences de l'Etat et les autorités administratives indépendantes afin de définir leur politique de gestion des systèmes d'informations, de même que les entreprises de services e-santé sont incitées à rechercher dans les instruments de droit souple les normes les plus efficaces dans la diminution des risques. Pour les hébergeurs de données, la certification est obligatoire et implique le respect de normes internationales de management des systèmes d'information. La gestion des données à caractère personnel dans le domaine de la santé a ainsi pour but d'inspirer la confiance à grande échelle, non plus seulement

---

[2340] E. RIAL-SEBBAG, « Chapitre 4 : La gouvernance des Big data utilisées en santé, un enjeu national et international », *in Données de masse, gouvernance et droit*, *Journal international de bioéthique et d'éthiques des sciences* 2017/3, vol. 28, p. 45.
[2341] M.-A. FRISON-ROCHE, « Compliance et personnalité », *D.* 2019, p. 604.

à l'égard des professionnels qui ne maîtrisent plus le cycle de vie des données produites dans le cadre du parcours des individus, mais à l'égard de tout le système de santé et du secteur industriel du numérique en santé – du soin à la recherche et l'innovation.

Si la confiance est une « *richesse pour l'entreprise* »[2342], elle l'est aussi pour assurer la souveraineté nationale et européenne sur les données de santé. Le Comité consultatif national d'éthique, dans son avis relatif aux données massives en santé, souligne la place de la gestion collective des données dans la construction de la confiance. Il rappelle, allant dans le sens de nos développements généraux, que « *La transdisciplinarité accroît l'importance de* ***l'organisation*** *et de la gouvernance des données (recueil, annotation, hébergement) pour qu'elles favorisent les découvertes médicales et qu'elles puissent être utilement réutilisées. Cette gouvernance doit être assurée sous la responsabilité des acteurs, qui doivent* « mettre en œuvre **les mécanismes et les procédures internes** permettant de démontrer le respect des règles relatives à la protection des données ». *C'est en quelque sorte un contrat de* ***confiance*** *entre les personnes qui acceptent de confier leurs données et* ***l'organisation qui en assure le devenir et l'accès*** »[2343]. Ces propos font écho à la notion de *communs*, puisqu'il s'agit d'organiser une *gouvernance* – ou gestion commune – de ces données tout en construisant la confiance des acteurs et des personnes concernées.

469. Le délégué à la protection des données, plus petit dénominateur commun de la gestion des données à caractère personnel dans le domaine de la santé. Le délégué à la protection des données occupe une place centrale dans cette transformation organisationnelle visant la gestion des données à caractère personnel dans le domaine de la santé. Sa désignation est rendue obligatoire dans quasiment tous les contextes de traitement du système de santé. En effet, la désignation d'un délégué à la protection des données est obligatoire pour les organismes publics[2344], ce qui concerne tous les établissements publics, médicaux et médico-sociaux. Cette désignation est encore obligatoire lorsque les activités de base du responsable de traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées[2345]. Sont donc également concernés

---

[2342] Evoquant l'importance d'une bonne gestion ou gouvernance des données dans le cadre d'une démarche de *mise en conformité* : B. FAUVARQUE-COSSON et W. MAXWELL, « Protection des données personnelles », *D.* 2018, p. 1033.
[2343] CCNE, Avis n° 130, *Données massives en santé : une nouvelle approche des enjeux éthiques*, 29 mai 2019, p. 60. Nous soulignons.
[2344] RGPD, art. 37, § 1.
[2345] *Ibid.*

les hébergeurs de données de santé et les établissements privés. Le considérant 91 du RGPD donne une indication spécifique sur le point de savoir ce qu'est un traitement à grande échelle : le « *traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel* »[2346]. Comme le précise le Groupe 29, l'exemple est un cas extrême et une série de critères est à prendre en compte[2347]. Il apparaît que les réseaux de santé et les autres formes d'exercice collectif sont fortement susceptibles d'être concernés, d'autant qu'ils opèrent un suivi régulier et systématique[2348] des personnes concernées par les données[2349]. Enfin, la désignation d'un délégué à la protection des données est obligatoire aussi bien pour les responsables de traitement que pour les sous-traitants de données particulières visées à l'article 9 du RGPD, donc pour les données de santé, traitées à grande échelle, sans qu'il ne soit plus exigé un suivi régulier et systématique. En dehors des hypothèses d'exercice individuel, la désignation d'un délégué à la protection des données est donc exigée dans presque toutes les hypothèses de traitement de données à caractère personnel dans le domaine de la santé. Il est intéressant de souligner, afin de compléter notre analyse, que le délégué à la protection des données assure un rôle de gestion des données au sein des structures, et que sa généralisation dans les structures de santé publiques ou privées et les entreprises de prestations de services dans le domaine de la santé est significative de la gestion collective des données à l'échelle nationale et européenne. Leur indépendance[2350] est un marqueur fort de cette évolution sur le

---

[2346] RGPD, consid. 91.

[2347] « […] *le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative par rapport à la population concernée ; le volume de données et/ou le spectre des données traitées ; la durée, ou la permanence, des activités de traitement des données ; l'étendue géographique de l'activité de traitement* » (G29, *Lignes directrices concernant les délégués à la protection des données (DPD)*, 13 déc. 2016, version révisée et adoptée le 5 avr. 2017, 16/FR WP 243 rev.01, p. 9).

[2348] *Ibid.,* p. 10.

[2349] Ce peut être également le cas des logiciels intégrant un dispositif médical dès lors, par exemple, que le responsable du traitement est l'éditeur du logiciel et qu'il opère ainsi le traitement de toutes les données et définit les finalités du traitement.

[2350] RGPD, art. 38, § 3 et consid. 97. « *Dans l'exercice de leurs missions au titre de l'article 39, les DPD ne doivent pas recevoir d'instructions sur la façon de traiter une affaire, par exemple, quel résultat devrait être obtenu, comment enquêter sur une plainte ou s'il y a lieu de consulter l'autorité de contrôle. En outre, ils ne peuvent être tenus d'adopter un certain point de vue sur une question liée à la législation en matière de protection des données, par exemple, une interprétation particulière du droit* » (G29, *Lignes directrices concernant les délégués à la protection des données (DPD)*, *op. cit.*, p. 18).

plan général et se confirme particulièrement par la généralisation de leur désignation dans le domaine de la santé. Ils sont, de surcroît, les interlocuteurs principaux des personnes concernées par les traitements[2351], ce qui conduit à confirmer que la gestion des données couvertes par le secret professionnel incombe de moins en moins au professionnel de santé.

470. Pluridisciplinarité significative des délégués à la protection des données. Le délégué à la protection des données a pour fonction principale de faire appliquer le RGPD. Pour ce faire, il est amené à prendre position sur « *toutes les questions relatives à la protection des données à caractère personnel* »[2352] et donc sur la sécurité des dispositifs techniques et la confidentialité des données. Dans le domaine de la santé, il est donc également l'interprète des dispositions relatives au secret professionnel qui guident la confidentialité : textes de désignation, textes d'incrimination, faits justificatifs, conditions du secret partagé. Il doit également disposer de solides connaissances relatives aux normes techniques et managériales, lesquelles permettent cette *application*, et avoir de véritables compétences en gestion des risques et des données. Ces constats sont tout autant valables pour les nombreux métiers qui émergent à l'occasion de la course globale pour l'innovation dans le domaine des *Big data*. Dans le contexte d'une « *Europe de la compliance* »[2353], la gestion des risques et, en ce qui nous concerne, la gestion des risques liés à la protection des données, se pose à tous les niveaux et à tous les stades du cycle de vie de celles-ci. Tandis que l'on pourrait penser que les juristes sont les plus à même d'y occuper des fonctions clés, il apparaît que leur formation universitaire ne les y prépare généralement pas.

471. Remarques générales sur la place et la formation des juristes. Il est, d'abord, rarement – voire jamais – question, dans les facultés de droit françaises, de la place des normes technico-managériales. Les interactions normatives, leur signification et la concurrence des normes y sont encore trop occultées. La raison est sans doute à trouver dans la persistance d'une culture fortement imprégnée du positivisme, le droit étant encore enseigné au travers des

---

[2351] RGPD, art. 13 et 14.
[2352] G29, *Lignes directrices concernant les délégués à la protection des données (DPD)*, *op. cit.*, p. 18
[2353] Madame Frison-Roche fait notamment le constat de l'extension des domaines de la *compliance*, non plus seulement pour la prévention des risques systémiques dans le cadre des marchés, mais également pour la protection des personnes (M.-A. FRISON-ROCHE, « Un droit substantiel de la compliance, appuyé sur la tradition européenne humaniste », *Pour une Europe de la compliance*, coll. Thèmes et commentaires, Dalloz, 2019, p. 13, spéc. p. 27 et svt).

critères classiques de la juridicité[2354]. Les transformations qui s'opèrent sont l'occasion de rappeler les propos de Monsieur Frydman lorsqu'il explique l'intérêt d'une étude pragmatique[2355] des interactions entre les normes : « […] *il nous apparaît nécessaire et urgent que le juriste s'émancipe d'une conception par trop étroite, formelle et rigide de la juridicité, afin de porter son regard, son intérêt et ses études dans le champ plus vaste de la normativité, dans toute la diversité de ses formes et de ses techniques. Il serait grand temps et d'ailleurs très excitant de compléter la théorie du droit par une théorie des normes, qui en analysera les modes d'élaboration et d'application, les institutions spécifiques, la dynamique et les conflits, etc.* »[2356]. S'inscrivant aussi dans une conception pragmatique du droit[2357], Messieurs Jamin et Xifaras ont pu formuler le regret que « *le droit dans les livres* » – l'approche technicienne – soit la voie d'enseignement empruntée dans les facultés de droit, au détriment du « *droit en action* »[2358], c'est-à-dire du droit tel qu'il se présente aux professionnels qui le pratiquent. S'interrogeant sur l'intérêt d'un savoir « *stratifié, organisé, différencié selon les disciplines* »[2359], les auteurs rappellent que les membres du Conseil d'Etat et certains avocats d'affaires n'ont pas effectué leur formation dans des facultés de droit, ces derniers étant de plus en plus issus d'écoles de commerce, et ayant suivi, au mieux, une formation d'une année de droit par le biais d'une passerelle[2360]. Il faudrait, pour que les étudiants ne se désolent pas « *de ne pas jouer de rôle vraiment stratégique là où ils sont employés* »[2361], qu'il leur soit fourni un

---

[2354]V. *supra* n° 398 et svt.

[2355] Consistant à se défaire d'une approche basée sur les ordres juridiques et à choisir une approche « *plus modeste, mais également plus proche des réalités de la pratique* » et qui « *consiste à observer comment s'opère sur le terrain, dans certaines situations qe l'on définira comme des contestes d'actions, la rencontre entre, d'une part, des normes techniques et managériales et, d'autre part, des règles juridiques* » (B. FRYDMAN, *Prendre les standards et les indicateurs au sérieux* », *in* B. FRYDMAN et A. VAN WAEYENBERGE (ss. la dir.), coll. penser le droit, Bruylant, 2014, p. 62).

[2356] *Ibid.* p. 65.

[2357] La philosophie pragmatique principalement développée par Charles Sanders PIERCE et John DEWEY a donné naissance à plusieurs courants de pensée du droit : sur ce sujet, v. B. FRYDMAN, « Le droit comme savoir et comme instrument d'action dans la philosophie pragmatique », *Revue de la recherche juridique* 2017-5, n° 31, coll. Cahiers de méthodologie juridique, p. 1805.

[2358] C. JAMIN et M. XIFARAS, « Sur la formation des juristes en France. Prolégomènes à une enquête », *Commentaires* 2015/2, n°150, pp. 385-392, spéc. p. 387.

[2359] Selon l'expression de O. BEAUD et R. LIBCHABER, « Où va l'Université ? Les chemins de la liberté », *JCP G*, 2014, I 1264, n° 7, p. 2227.

[2360] *Ibid.,* p. 389.

[2361] *Ibid.,* p. 388.

enseignement réellement pluridisciplinaire[2362]. En l'absence d'une telle évolution, les juristes de formation courent le risque d'être évincés de postes qui, comme dans le domaine du numérique, ne requièrent pas seulement des compétences juridiques. Le cas du délégué à la protection des données en est une bonne illustration.

Dans le domaine de la santé, la *mise en conformité* nécessite une connaissance du RGPD, mais aussi du cadre juridique du secret professionnel et de leur articulation, ce qui n'est pas une tâche aisée. La *compliance* impose encore, nous l'avons dit, une vision *stratégique* de la gestion des données, fondée sur le risque et le maniement des normes technico-managériales, des labels et certifications mais également de la technique. Le règlement européen précise d'ailleurs que le délégué à la protection des données doit être désigné *« sur la base de ses qualités professionnelles et, en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir* [ses] *missions* »[2363]. Une étude réalisée par le ministère du travail, publiée en mai 2019[2364], présente le profil des délégués à la protection des données un an après l'entrée en vigueur du RGPD. Il en résulte que les compétences en gestion de projet et en informatique sont *autant* requises que les compétences juridiques[2365]. L'on y apprend également que les juristes ne représentent que 31,1 % des profils tandis que 34 % sont des informaticiens et 34,9 % sont issus d'autres domaines d'expertise[2366]. Il n'est pas dans notre intention de prôner une plus grande intervention des juristes dans la fonction, mais de remarquer que cette tendance semble devoir s'accentuer avec les *Big data* et l'intelligence artificielle. L'intérêt pour les profils variés, cumulant des compétences stratégiques, techniques et juridiques, ne pourra que se développer dans ces domaines, aussi bien dans l'industrie que dans les services du numérique. Les facultés de droit en ont pris, en partie, conscience puisque certaines proposent désormais des formations spécifiques[2367]. Il ne s'agit pas, néanmoins, d'une refonte profonde de la formation

---

[2362] *Ibid.,* p. 392 ; D. JUTRAS et C. JAMIN, « À quoi servent les études de droit ? Correspondance outre-Atlantique », *JCP G* 2014, 639, p. 1098.
[2363] RGPD, art. 37, § 5.
[2364] Afpa Direction Prospective Métier, *Règlement Général sur la Protection des Données Le métier de Délégué à la Protection des Données (DPO) 1 an après – Premiers Résultats*, disponible sur <https://travail-emploi.gouv.fr/IMG/pdf/rgpd-metier-dpo-premiers-resultats-072019.pdf> (dernière consultation le 26 août 2019).
[2365] *Ibid.,* p. 4.
[2366] *Ibid.,* p. 2.
[2367] Ces formations se distinguent, en général, par la diversité de leurs enseignements et de leurs intervenants. Par exemple, le diplôme universitaire « Délégué à la protection des données », proposé par l'Université Paris II, sous

universitaire. Dans ce contexte, il nous semble que le maniement – complexe – des règles juridiques du RGPD et du secret professionnel, leur articulation avec les normes managériales, techniques et les instruments de droit souple qui participent désormais du secret des données à caractère personnel dans le domaine de la santé risque d'être laissé à l'interprétation de professionnels dont les compétences dominantes ne sont pas juridiques. Autant que former les professionnels intervenant dans le système de santé aux problématiques juridiques[2368], il s'agit désormais de former les juristes à d'autres disciplines. Dès lors, les particularités de la protection des données à caractère personnel dans le domaine de la santé devraient, à notre sens, inciter les facultés à adapter l'enseignement dispensé dans leurs formations de droit de la santé. Ces propos trouvent un écho particulier dans le phénomène de *migration des normes dans les objets*.

§ 2 - Le secret dans les choses

472. Un « autre » droit dans les choses. L'hypothèse d'un droit implémenté dans les dispositifs techniques, suppose d'avoir identifié ce qu'est le droit. Les propos qui vont suivre révèlent donc d'une certaine vision de ce qu'est le droit[2369]. Pour autant, notre intention n'est nullement de formuler des affirmations sur ce point. Nous aurions pu emprunter l'expression

---

la direction de Madame Fauvarque-Cosson et de Monsieur Audit, comprend des enseignements en gestion du risque, en sécurité informatique, ainsi qu'en science des données. Parmi les profils des enseignants, des juristes mais plus généralement des personnes ayant des formations variées : sciences de l'information, mathématiques, management, commerce, ingénierie. Cette formation vise néanmoins un public professionnel et, sans exclure les juristes, elle ne leur est pas principalement destinée. Un autre exemple peut être mentionné : une formation de deux ans (Master) issue d'un partenariat entre la faculté de droit et la *business school* de l'Université catholique de Lyon, formation transversale en droit et en management du numérique.

[2368] C. ZORN, *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, coll. « Santé, qualité de vie et handicap », PUN, 2010, p. 443 et n° 17, 126 et 168).

[2369] Sans doute pourrait-on considérer que l'implémentation de normes dans les choses n'est pas du droit. L'on peut se référer aux propos, d'un autre ordre, de Monsieur Jeuland dans son essai de conception d'une théorie relationiste du droit. A l'occasion d'un développement sur la pensée de Jacques Ellul à propos du système technicien, l'auteur imagine ce que pourrait être la position du premier sur le droit au regard d'une théorie qui penserait le droit comme relation plutôt qu'à partir de la norme : « *Si l'on admet que le droit « construit la réalité sociale » le fait que la technique rende la société irréelle* [pour Jacques Ellul le système technicien se construit à coté de la société] *signifie qu'elle s'attaque au droit, qu'elle rend irréel le droit ou le recouvre. C'est ce qui arrive avec, par exemple, le dispositif technique qui empêche de faire démarrer sa voiture si le degré d'alcool dans le sang dépasse la norme légale. L'éthylotest est en effet branché sur le démarreur. Il n'y a plus dès lors besoin de policier ou de juge.* […]. *Bien sûr, il resterait des tribunaux et du droit, mais de manière subsidiaire et secondaire* » (E. JEULAND, *Théorie relationiste du droit. De la* French Theory *à une pensée européene des rapports de droit*, LGDJ, 2016, p. 152).

« *migration des normes vers les objets techniques* », telle que présentée lors d'un récent colloque ayant eu lieu à l'Université Nice Sophia-Antipolis[2370]. Il nous importe toutefois de décrire le changement mis en lumière par d'autres. Pour ce faire, quelques repères doivent être tracés au préalable.

C'est sous l'expression *Ambient law* que Madame Hildebrandt décrit ce qui lui semble être l'avenir du droit dans le *monde digital*[2371]. Elle suggère en partie la même idée que l'expression empruntée à Monsieur Lewkowicz de *droit dans les choses*, celle d'une implémentation du droit dans les dispositifs techniques comme possible futur du droit. A l'origine, l'expression *droit dans les choses* a été employée par Michel Villey et nous ramène à la question de l'ontologie du droit et à la théorie du droit naturel classique, que ce dernier auteur avait défendu une dernière fois dans un discours publié sous ce titre, qu'il prononça à l'occasion d'un colloque portant sur les controverses autour de l'ontologie du droit[2372]. Le *droit dans les choses* tel que l'envisage Monsieur Lewkowicz en introduction du cycle de conférence du Centre Perelman de philosophie du droit de l'Université de Bruxelles intitulé *Le futur du droit : big data, algorithmes et robotisation*[2373] n'est pas celui du droit naturel classique, ni d'ailleurs celui de l'Ecole moderne du droit naturel. Il peut toutefois être appréhendé comme une nouvelle étape susceptible d'affecter notre conception du droit[2374], illustrant la « *fonction*

[2370] Le colloque présenté sous la direction de Madame Parachekova-Racine était intitulé *Technonormativités : des objets connectés à l'IA*. La première partie des interventions est présentée sous le titre « *Migration des normes vers les objets techniques* » (*Technonormativités : des objets connectés à l'IA* (sous la direction de I. PARACHEKOVA-RACINE, organisé dans le cadre du programme *Droit et objets connectés* et de la 2nde édition des rencontres entre l'Ecole de Nice et l'Ecole de Bruxelles, 27 et 28 sept. 2018, Faculté de droit et de sciences politiques, Nice).

[2371] V. particulièrement M. HILDEBRANDT, « A vision of ambient law », *in* R. BROWNSWORD et K. YEUNG (ss. la dir.), *Regulating Technologies*, *Legal Futures, Regulatory Frames and Technological Fixes*, Hart Publishing, 2008, p. 175 et svt.

[2372] Ce colloque, qui s'est tenu les 26 et 27 mai 1988, était organisé sous la direction de Messsieurs Amselek et Grzegorczyk, et a fait l'objet d'une publication où l'on retrouve le discours d'ouverture de Michel Villey : M. VILLEY, « Le droit dans les choses », *in* P. AMSELEK et C. GRZEGORCZYK (ss. la dir.), *Controverses autour de l'ontologie du droit*, PUF, 1989.

[2373] Cette intervention est disponible en ligne en format vidéo. Aucune publication n'étant, à notre connaissance, disponible, c'est sur cette intervention que nous nous appuierons pour illustrer certains de nos propos (G. LEWKOWICZ, « Le droit dans les choses, le futur du droit ? », Ouverture d'un cycle de conférence organisé par le Centre Perelman de Philosophie du Droit de l'Université libre de Bruxelles, disponible sur <https://www.youtube.com/watch?v=PseF2AZABjM> (dernière consultation le 24 août 2019).

[2374] Nous renvoyons à un article de Monsieur Frydman à l'occasion duquel il retrace, dans une présentation essentielle, les avatars du droit naturel dans la construction des représentations du droit : B. FRYDMAN, « Les métamorphoses d'Antigone », *Droit & Philosophie* 2016, n° 8, pp. 111-167.

épistémique du droit naturel »[2375] mise en exergue par Monsieur Frydman. La réflexion sur le phénomène en cours n'en est qu'à ses débuts, comme le suggère cet auteur dans ces propos :

> « *Voici donc, à la faveur de la révolution des technologies de l'information, de l'intelligence artificielle et de la robotisation, que les projets les plus fous imaginés par la « science du droit »*, *la formalisation du droit et l'établissement d'un système intégral de régulation de la société, seraient sur le point de se réaliser conjointement. La masse devenue ingérable des textes réglementaires et des décisions serait numérisée et les règles confiées à des logiciels qui les adapteraient en temps réel et assureraient leur exécution automatique par le moyen d'algorithmes directement en prise sur les phénomènes, les objets et les sujets à réguler. Instruits par notre parcours, nous ne sommes guère surpris par ce nouvel épisode du feuilleton, à la longue un peu répétitif, de la science du droit, reprise en mains par les informaticiens et les ingénieurs, sur le point de renverser la République des lettres par l'empire du chiffre*. *Mais si nous avons bien suivi la série, nous savons que ce dernier rebondissement en date annonce probablement des transformations à terme considérables et radicales de la conception du droit ou de ce qui en tiendra lieu, de ses voies et de ses moyens* »[2376].

473. Effet normalisant de la la technique. ***Code is law*.** Nos derniers développements auront, cette fois encore, une portée plus générale visant à décrire un mouvement dans lequel s'inscrit, au moins partiellement, le secret des données à caractère personnel dans le domaine de la santé. Le rôle de la technique dans la protection des données à caractère personnel a été précédemment évoqué : la sécurité et la confidentialité des données *by design* se traduisent par des choix architecturaux[2377], de fonctionnalités (pseudonymisation), de technologies

---

[2375] « *Le concept de droit naturel, dans le triple rapport qu'il entretient avec la réalité, la rationalité et l'universalité, exprime de manière privilégiée la prétention à la constitution d'un savoir dans le domaine juridique. Il représente, pour parler comme Michel Foucault, une instance de véridiction du discours juridique. Il fonde et il nourrit, sous les formes successives qu'il emprunte, la vocation du droit à se présenter et à se constituer comme science et comme discipline* » (*Ibid.*, p. 122).

[2376] B. FRYDMAN, « Les métamorphoses d'Antigone », *op.cit.*, pp. 166-167.

[2377] R. GOLA, « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *Legicom* 2017/2, n° 59, pp. 29-38, spéc. p. 34.

(cryptographie)[2378]. L'effet normalisant de l'architecture est connu, il suffit d'évoquer l'architecture panoptique du milieu carcéral imaginée par Jeremy Bentham pour s'en convaincre. L'architecture est pensée par le philosophe et juriste anglais comme un moyen d'obtenir des individus un certain comportement et, se faisant, de prévenir plutôt que de punir « *en agissant principalement sur les inclinations des individus afin de les détourner du mal et de leur imprimer la direction la plus utile à eux-mêmes et aux autres* »[2379]. Plus proche de nous, il faut citer l'exemple fameux, depuis les travaux de Monsieur Lessig, de l'architecture technique du cyberespace[2380]. Selon cet auteur, il existe quatre principaux modes de régulation utilisés conjointement : la loi, les normes, le marché et l'architecture[2381]. Dans le cyberespace, l'architecture est remplacée par le code. Ce code – ou architecture – prédéfinit le type d'acte que nous pouvons y accomplir, les espaces d'expression, l'accès à telle ou telle information. Le code est le mode de régulation du cyberespace[2382]. Comme l'expose encore Monsieur Lewkowicz, certains objets du quotidien sont construits en intégrant une norme de comportement, comme c'est le cas des sécurités pour enfant sur les objets présentant un danger[2383]. Ces normes techniques ont pour objectif de transférer les normes de comportement

---

[2378] Dans un guide publié en 2018 la CNIL rappelle les actions techniques et de gestion minimales à mettre en œuvre pour la sécurité et la confidentialité des données à caractère personnel sous forme de fiches thématiques : Authentifier les utilisateurs ; gérer les habilitations ; tracer les accès et gérer les incidents ; sécuriser les postes de travail ; sécuriser les postes de travail ; protéger le réseau informatique interne ; sécuriser les serveurs ; sécuriser les sites web ; sauvegarder et prévoir la continuité d'activité ; archiver de manière sécurisée ; encadrer la maintenance et la destruction des données ; gérer la sous-traitance ; sécuriser les échanges avec d'autres organismes ; protéger les locaux ; encadrer les développements informatiques ; chiffrer, garantir l'intégrité ou signer. S'agissant de l'encadrement des dévoloppements informatiques, la CNIL rappelle la nécessité d'intégrer la sécurité et la confidentialité dès la conception, qui doit se traduire par des choix d'architecture technique, de fonctionnalités et de technologies (CNIL, Guide « La sécurité des données personnelles », 2018, p. 24).

[2379] J. BENTHAM, *Traités de législation civile et pénale*, coll. Bibliothèque Dalloz, Dalloz, 2010, p. 331.

[2380] Appliqué à l'internet, « *L'architecture technique s'entend de l'ensemble des éléments ou artefacts techniques, tels les matériels, les logiciels* […] *et les configurations qui déterminent l'accès et les droits d'utilisation des ressources du cyberespace* ». Cette définition est également transposable à l'architecture technique des systèmes d'information, de réseaux moins étendus qui, par ailleurs, utilisent tous l'internet pour fonctionner en réseaux (P. TRUDEL, « Quel droit et quelle régulation dans le cyberespace ? », *in Les promesses du cyberespace. Médiations, pratiques et pouvoirs à l'heure de la communication électronique*, *Sociologie et sociétés*, 2000, vol. 32, n° 2, pp. 190–210, *spéc.* p. 202).

[2381] L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books ed., 1999.

[2382] « *This regulator is code – the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned. It affects who sees what, or what is monitored. In a host of ways that one cannot begin to see unless one begins to understand the nature of this code, the code of cyberspace regulates* » (L. LESSIG, « Code Is Law. On Liberty in Cyberspace », *Harvard Magazine*, 1 janv. 2000, disponible sur <https://www.harvardmagazine.com/2000/01/code-is-law-html > (dernière consultation le 27 août 2019)).

[2383] G. LEWKOWICZ, « Le droit dans les choses, le futur du droit ? », *op. cit.*, à partir de 15 :11 min.

dans les objets[2384]. L'auteur identifie un tournant, dans le sens des travaux de Madame Hildenbrandt[2385] : celui de la réplique numérique du monde[2386], qui permet d'affirmer que le processus en cours et celui de la *migration du droit dans les choses*.

474. Réplique numérique du monde. Choix de l'architecte. *Code as law*. Si l'architecture des objets et des espaces a un effet normalisant – que cette architecture soit ou non du code comme dans le cyberespace –, la conformité qu'elle implique n'est pas la conformité à la règle de droit. En toute hypohtèse, dès lors que la technique a un effet normalisant, elle n'est pas neutre[2387]. Monsieur Lessig formulait une mise en garde contre les « dangers » de cette capacité du code à intégrer ou à supplanter certaines valeurs protégées par le droit et dont nous pourrions perdre le contrôle[2388], car dans le cyberespace, l'architecture/code dépend des personnes qui codent et des incitations qu'elles reçoivent[2389]. Pour comprendre le tournant qui s'opère et la

---

[2384] *Ibid.* à partir de 15:55 min.

[2385] M. HILDEBRANDT, « A vision of ambient law », *in* R. BROWNSWORD et K. YEUNG (ss. la dir.), *Regulating Technologies*, *Legal Futures, Regulatory Frames and Technological Fixes*, Hart Publishing, 2008, p. 175 et svt.

[2386] G. LEWKOWICZ, « Le droit dans les choses, le futur du droit ? », *op. cit.* à partir de 16 :49 min.

[2387] L'illusion de la neutralité technique a été combattue par Jacques Ellul, qui considère qu'il n'y a pas, d'un côté, la technique, et de l'autre, les usages qui en sont faits, si bien que l'on pourrait dire que, si la technique est utilisée pour un dessein ou un autre (usage), cela relève du fait de l'homme. De même, Jacque Ellul estime qu'orienter la technique en fonction de motifs d'ordre moral est impossible, puisque la technique a pour caractéristique fondamentale de rejeter tout jugement moral : elle est nécessaire et ne vise que l'efficacité. Selon lui, « *Il ne faut jamais dire : d'un côté la technique, d'un autre des abus ; mais presque toujours rendre compte qu'il y a d'un côté et de l'autre des techniques différentes, répondant à des nécessités diverses, mais inséparablement unies* » (J. ELLUL, *La technique ou l'enjeu du siècle*, Economica, 1954, p. 89). Sous couvert de neutralité, la technique aurait acquis une autonomie, elle formule ses propres *règles*. Il estime ainsi qu'elle n'est pas neutre mais *ambivalente,* à la fois bonne et mauvaise. En toutes hypothèses il considère que la technique répond à ses propres *règles* et en déduit ce qu'il considère comme un principe : « *l'homme est placé devant un choix exclusif, utiliser la technique comme elle doit l'être selon les règles techniques, ou ne pas l'utiliser du tout ; mais impossible d'utiliser autrement que selon les règles techniques* » (*Ibid.,* p. 91). Madame Hildebrandt admet, quant à elle, l'une des *lois* formulées par Melvin Kranzberg, notamment celle selon laquelle la technique n'est ni bonne, ni mauvaise, ni neutre : « *technologies are neither good not bad but never neutral. By that I mean that technology's interaction with the social ecology is such that technical developments frequently have environmental, social, and human consequences that go far beyond the immediate purposes of the technical devices and practices themselves, and the same technology can have quite different results when introduced into different contexts or under different circumstances* » (M. KRANZBERG, «Technology and History: "Kranzberg's Laws" », *Technology and Culture* 1986, vol. 27, n° 3, pp. 544-560, spéc. p. 545). La technique dépend du contexte social, cuturel et géographique dans lequel elle est créée et utilisée.

[2388] « *For unless we understand how cyberspace can embed, or displace, values from our constitutional tradition, we will lose control over those values. The law in cyberspace – code – will displace them* » (L. LESSIG, « Code Is Law. On Liberty in Cyberspace », *op. cit.*).

[2389] Prenant l'exemple du respect de la vie privée: « *Thus whether the certification architecture that emerges protects privacy depends upon the choices of those who code. Their choices depend upon the incentives they face » (Ibid.). Cette position peut-être rapprocher de celle de Madame Hildebrandt qui considère que la société civile et*

migration du droit dans les choses, il faut prendre en compte l'évolution des technologies et plus particulièrement l'émergence des *Big data*. Monsieur Lewkowicz évoque une réplication numérique du monde, à coté du « monde » il y aurait désormais un « monde intelligent »[2390]. Cette idée est celle notamment exprimée par Madame Hildebrandt. L'auteur explique comment le *monde intelligent* suppose l'immediateté des réactions[2391] face à un droit qui n'a rien d'immédiat[2392], ni dans sa formation, ni dans son interprétation, ses procédures, son application[2393]. Elle prône donc l'adaptation du droit comme moyen de préserver les valeurs

---

les gouvernements doivent prendre conscience que la technologie n'est pas neutre mais dépend des choix de construction, « […] citizens who suffer or enjoy the effects of new technological infrastructures, like for instance Ambient Intelligence (AmI), should be able to influence decisions regarding the funding, designing and marketing of such emerging technologies. Instead of endorsing a paralysing technological determinism (akin to a fatalist acceptance of natural disaster) civil society and its government should realise that technologies are neither good not bad but never neutral, acknowledging that technologies can be constructed in different ways, with different normative implications » (M. HILDEBRANDT, « A vision of ambient law », *op. cit*., p. 176).

[2390] G. LEWKOWICZ, « Le droit dans les choses, le futur du droit ? », *op. cit.*, 18 :44 min. L'utilisation du qualificatif « intelligent » pour signifier ce dédoublement (voire un remplacement) et viser les conséquences de l'utilisation des *Big data*, des algorithmes et de l'intelligence artificielle sature désormais le langage : *smart contract*, *smart grits*, *smartphone, smart home*, *smart city*, …

[2391] Sur cette question l'on se reportera à l'étude des rapports entre sciences du comportement, gouvernance algorithmique et *big data*, notamment celle de Madame Rouvroy et de Monsieur Berns, lesquels constatent également un « *dédoublement du réel* » dans lequel, selon eux, se déploie le « *comportalisme numérique* » : *« rationalité (a)normative et (a)politique reposant sur la récolte, l'agrégation et l'analyse automatisées de données en quantité massive de manière à modéliser, anticiper et affecter par avance les comportements possibles* » (A. ROUVROY et T. BERNS, « Gouvernementalité algorithmique et perspectives d'émancipation », *Reseaux* 2013/1, n° 177, pp. 163-169, spéc. p. 173). V. également M. HILDEBRANDT et K. DE VRIES (ss. la dir.), *Privacy. Due Process and the Computational Turn. The Philosophy of Law meets the Philosophy of Technology*, Oxford, Routledge, 2013. Pour une réflexion générale sur les techniques de normalisation et leurs rapports d'opposition au droit, ces dernières étant sans finalités, v. F. OST, *A quoi sert le droit ? Usages, fonctions, finalités*, *op. cit.*, p. 297 et svt.

[2392] A ce sujet, Monsieur Ost explique que le droit « *travaille la matière même du temps* […]. *Ce faisant, les fictions opératoires du droit contribuent à créer un univers porteur de sens, tout comme ses délais et ses supensions ménagent la possibilité de la réflexion, de la réponse, et, en fin de compte, de la communication* » (*Ibid.,* p. 321-322).

[2393] L'auteur confronte l'approche linéaire du temps du droit moderne et l'immédiateté des réactions du monde numérique : « *The questions raised by the digital age regard the linear sense of time inherent in modern law, confronted with the segments and points defining its digitalised environments […] ; the slow accumulation of legal texts like statutes, treaties, case law and doctrine that need to be studied and interconnected, confronted with instant online access to of all the sources of the law […]; the delay and duration inherent in procedural safeguards that embody protection against hasty judgements, confronted with series of real time decisions taken by multi-agent systems in smart environments; the care with which legal theory has constructed and sustained the theoretical legitimisation and critical assessment of the positive law, confronted with a world in which models replace theory; the hermeneutical practice of law (always involved in interpreting both the facts of the case and the legal norms that should apply), confronted with a world in which simulation rather than interpretation turns out to be the best way to anticipate future events; the emphasis on meaning as a reference to the world outside law (semantics), confronted with an emphasis on links and networks (syntaxis) and the actual consequences of doing things one way or another (pragmatics)* […] » (M. HILDEBRANDT, « A vision of ambient law », *op. cit.*, p. 186).

constitutionnelles – rejoignant ainsi les propos de Monsieur Lessig[2394] – par son *incarnation*[2395] dans les dispositifs techniques.

475. La vocation des normes techniques, migration du secret dans les choses. L'effet normalisant des dispositifs techniques tient au fait que l'on *limite le type d'actes* qui peuvent être effectués par les individus dans un environnement donné – informatique en ce qui nous concerne – ou lorsqu'ils utilisent une chose[2396]. Les *scenarii* possibles sont pré-écrits dans les logiciels, les systèmes d'information, les dispositifs. Ainsi, la lecture de certaines informations par une personne qui n'est pas autorisée à en prendre connaissance peut être empêchée – cryptage avec clefs de déchiffrement, impossibilité d'imprimer des données, de les extraire –, comme peut être empêché son accès à des systèmes d'information ou à certaines ressources de ce système – carte professionnelle de santé, mot de passe – avec plus ou moins d'efficacité. Ces *scenarii* peuvent donc être écrits de manière à empêcher à des tiers de prendre connaissance de données couvertes par le secret ou d'empêcher que la personne soumise au secret puisse effectuer certaines actions, volontaires ou non (mésusage). Il sera donc, par exemple, impossible de commettre l'infraction de violation du secret professionnel par le moyen des dispositifs techniques ainsi conçus. Il peut ainsi être affirmé que le secret des données à caractère personnel dans le domaine de la santé est déjà, en partie, assuré par la technique.

En faisant le choix de la *compliance,* c'est-à-dire d'une autorégulation – partielle puisque la CNIL intervient tout de même *ex ante* et *ex post* –, le législateur européen impose simplement que soient mises en œuvre les mesures organisationnelles et techniques nécessaires à la sécurité et à la confidentialité des données. Nous l'avons vu, ces mesures sont précisées par les normes techniques et managériales. Afin que les dispositifs techniques respectent le droit, dans la perspective d'assurer la securité et la confidentialité des données dès la conception, les normes techniques vont implémenter dans la machine le contenu des règles de droit[2397] qui s'imposent d'ordinaire aux acteurs. Monsieur Lewkowicz souligne, à ce propos, que le travail

---

[2394] Utilisant l'expression « *digitalised law* », *Ibid.* p. 186; L. LESSIG, « Code Is Law. On Liberty in Cyberspace », *op. cit.*

[2395] Traduction littérale du terme « *embodiement* » utilisé par l'auteur (M. HILDEBRANDT, « A vision of ambient law », *op. cit.*).

[2396] G. LEWKOWICZ, « Le droit dans les choses, le futur du droit ? », *op. cit.*, à partir de 12:35 min.

[2397] Lorsqu'elles sont prises en considération de ces règles et pour leur exécution.

d'implémentation, de *transposition* du droit dans les dispositifs techniques est délégué aux industriels, aux ingénieurs et aux techniciens[2398]. L'on peut, sur ce point, réitérer nos propos sur la formation des juristes et l'importance – si l'on adhère à la vision du droit qui conditionne la possibilité de concevoir un droit dans les choses – d'une formation pluridisciplinaire afin qu'ils puissent prendre part au débat relatif aux modalités de *transfert* du droit dans les dispositifs techniques[2399].

476. Les effets possibles sur le droit ? Il est difficile d'évaluer les conséquences que pourrait avoir ce transfert du droit vers les dispositifs techniques. A admettre la possibilité d'un tel transfert, plusieurs problématiques se posent. Monsieur Lewkowicz souligne que cette transposition peut avoir pour conséquence de rigidifier la règle et de la préciser[2400]. Si l'on prend l'exemple du secret professionnel, *l'application* automatique peut avoir des conséquences importantes sur l'existence du choix offert au professionnel de révéler ou non une information lorsqu'il existe une permission de révéler[2401]. Dans le cadre du secret partagé, selon la manière dont est structuré un système d'information, il se peut que toutes les données qui concernent un patient et qui sont traitées par le système soient accessibles par l'ensemble de l'équipe prenant en charge le patient. Cette hypothèse implique que le partage de ces données n'est plus une possibilité, *il est*. Il nous semble que la *logique d'accès* que nous avons décrite auparavant[2402] pourrait constituer un point de départ dans le sens d'une telle rigidification. Dans ce schéma, un professionnel qui voudrait, pour une raison qui lui appartient, ne pas partager certaines informations, devrait s'abstenir de les entrer dans le système car ce n'est pas lui qui définit les droits d'accès. Actuellement, la gestion de la circulation des données est encore entre les mains de l'homme mais dans l'hypothèse, qui relève pour l'instant de l'anticipation ou de

---

[2398] G. LEWKOWICZ, « Le droit dans les choses, le futur du droit ? », *op. cit.*, à partir de 1 :16 :00 min.
[2399] « *The conclusion must be that lawyers and computer scientists should negotiate mutual transformations in the legal and technological infrastructure to sustain and reinvent democracy and rule of law in the age of Ambient Intelligence* » (M. HILDEBRANDT, « A vision of ambient law », *op. cit.*, p. 176 et p. 189). A la suite de ses propos que nous avons reproduit plus avant, Monsieur Frydman complète : « *Si nous voulons, en tant que juristes, continuer à remplir les missions qui sont les nôtres, en particulier celle de veiller sur les principes de l'État de droit et de protéger les droits fondamentaux des personnes, alors il faut sans attendre nous atteler à la compréhension et à la maîtrise de cet univers et de ces techniques si étrangers à nos pratiques. Telle est en tout cas la leçon que je retire personnellement de cette réflexion sur le droit naturel* » (B. FRYDMAN, « Les métamorphoses d'Antigone », *op. cit.*, p. 167).
[2400] G. LEWKOWICZ, « Le droit dans les choses, le futur du droit ? », *op. cit.*, à partir de 1 :06 :00.
[2401] F. ALT-MAES, « Un exemple de dépénalisation : la liberté de conscience accordée aux personnes tenues au secret professionnel », *RSC* 1998, p. 301.
[2402] V. *supra*, n°373 et svt.

la science-fiction, d'un système de santé dans lequel la rencontre entre le patient et le soignant serait supplantée par la machine et d'où le lien social serait exclu, ce circuit pourrait être entièrement défini par le code. De manière plus générale, Monsieur Lewkovicz explique qu'une généralisation du *droit dans les choses* conduirait à un « *passage du modèle herméneutique au modèle techno-managérial* »[2403] et à un « *déplacement du droit depuis les sciences sociales vers les sciences de l'ingénieur* »[2404].

477. Normalisation. Il est alors tentant d'abandonner la conception du droit au regard de laquelle il pourrait exister un *droit dans les choses*, c'est-à-dire de ne pas admettre que le droit se définit uniquement par rapport à des finalités de justice[2405], de raison[2406] ou par rapport à des intérêts collectifs[2407]. Et de considérer alors que le phénomène décrit n'est plus du droit. Il pourrait s'agir d'un processus de normalisation. Pour expliciter ce processus, nous avons choisi de nous appuyer sur la pensée de Monsieur Ost parce qu'elle offre une vision d'ensemble, enrichie, de la littérature relative à cette question. Nous avons conscience que ces développements sont extrêmement contextualisés, qu'ils appartiennent à une théorie dont la construction va d'un seul tenant et sont donc enserrés dans la démarche dialectique adoptée par l'auteur. Nous souhaitons tout de même les évoquer, afin qu'ils apportent une lumière différente sur ce que nous avons exposé jusqu'ici[2408].

Au moment d'envisager l'opposition entre droit et normalisation, Monsieur Ost distingue plusieurs formes de *régulations normalisatrices*, dont « *la normalisation par les dispositifs techniques inscrits dans les choses elles-mêmes* (*sur le modèle* […] *des procédures obligées inscrites dans les logiciels d'ordinateurs*) »[2409]. Il explique que ces formes de

---

[2403] G. LEWKOWICZ, « Le droit dans les choses, le futur du droit ? », *op. cit.*, à partir de 1 :06 :00.
[2404] *Ibid.*
[2405] Comme l'enseignait le jusnaturalisme classique dont Michel Villey était un des plus illustres défenseurs contemporains (M. VILLEY, *Philosophie du droit. Définitions et fins du droit. Les moyens du droit*, coll. Bibliothèque Dalloz, Dalloz, 2001).
[2406] Comme l'enseignait l'Ecole moderne du droit naturel. Pour un résumé, v. B. FRYDMAN, *Le sens des lois*, 2ème éd., coll. Penser le droit, Bruylant-LGDJ, 2007, p. 236 et svt.
[2407] V. notamment J. HABERMAS, *Droit et démocratie*, Gallimard, 1997.
[2408] Pour une présentation de l'ouvrage v. F. GEA, « François Ost, *À quoi sert le droit ? Usages, fonctions, finalités* », Bruylant, coll. Penser le droit, 2016 », *Rev. trav.* 2016, p. 649.
[2409] F. OST, *A quoi sert le droit ? Usages, fonctions, finalités*, *op. cit.*, p. 300.

régulation par les normes[2410] ont des traits communs, qu'il considère à l'opposé des « *présupposés anthropologiques de la normativité juridique* »[2411], c'est-à-dire à l'opposé d'une certaine conception de l'humain[2412]. Il ne nous est pas possible de formuler de manière satisfaisante cette conception de l'humain développée par l'auteur tant elle est riche de nuances, d'autant plus qu'elle est déterminante dans l'identification des finalités intrinsèques que l'auteur assigne au droit, puisque c'est par ce « *détour anthropologique* »[2413] qu'il « *réfléchit au type d'humanité qu'il* [paraît] *souhaitable de garantir* »[2414]. En résumé, le trait saillant qui permet de souligner l'opposition entre normalisation et régulation juridique au regard de cette nature, consiste dans son *indétermination*. Pour Monsieur Ost, l'humain est *digne*. L'auteur trouve dans la pensée de Kant matière à construire une conception de l'homme dont la dignité repose sur son indétermination et « *corrélativement, sa capacité d'autoconstitution* »[2415], « *l'effort constant qu'il déploit pour donner sens à son existence* »[2416]. Partant, il s'emploie à exposer en quoi la normalisation est à l'opposé de la nature humaine et de la normativité juridique telle qu'il les conçoit. Pour ce faire, il en relève les traits caractéristiques, parfois mis en exergue par d'autres théoriciens et qu'il envisage dans une perspective critique. Ces dispositifs normatifs agissent comme des « *forces invisibles* »[2417]. La norme, selon les mots de Monsieur Supiot « *opère de l'intérieur, comme un programme biologique ou un logiciel d'ordinateur* »[2418], ces dispositifs procèdent donc comme des programmes, évacuant le libre-arbitre des individus[2419]. L'auteur se réfère ensuite aux travaux de Michel Foucault, qui, envisageant les dispositifs de sécurité, notamment comme mode de régulation, écrit : « *la loi interdit, la discipline prescrit, et la sécurité, sans interdire ou sans prescrire* […], *a*

[2410] Egalement : « *la normalisation par objectifs chiffrés : indicateurs, standards, nombres* ; […] ; *la normalisation opérant par les méthodes* béhaviourises *(*nudges, big datas*, et, à la limite,* moral machines*) ; et enfin la normalisation psychique par les récits (*storytelling) *et les images* (vidéosphère). » (*Ibid.*).
[2411] *Ibid.*
[2412] Conception que l'auteur expose au travers de six « polarités paradoxales » mais solidaires en ce qu'elles révèlent, selon lui, les paradoxes même de la nature humaine : « Vivants, et pourtant mortels », « Corps, et pourtant esprits », « Libres, et pourtant déterminés », « Rationnels, et pourtant faillibles ; moraux et pourtant virtuellement coupables », « Egaux et pourtant singulier », « Individus, et pourtant être sociaux » (*Ibid.*, Pp. 273-294).
[2413] *Ibid.*
[2414] *Ibid.*, p. 329.
[2415] *Ibid.* p. 296.
[2416] *Ibid.*
[2417] *Ibid.* p. 300.
[2418] A. SUPIOT, *La gouvernance par les nombres*, *Cours au collège de France (2012-2014)*, coll. Poids et mesures du monde, Fayard, 2015, p. 174
[2419] F. OST, *A quoi sert le droit ? Usages, fonctions et finalités*, *op. cit.*, p. 300-301.

essentiellement pour fonction de répondre à une réalité de manière à ce que cette réponse annule cette réalité à laquelle elle répond – l'annule, ou la limite ou la freine ou la règle. C'est cette régulation dans l'élément de la réalité qui est […] *fondamentale dans les dispositifs de sécurité* »[2420].

Monsieur Ost n'envisage pas de manière spécifique la normalisation inscrite dans les dispositifs techniques et n'évoque pas la régulation des *Big data*. Il nous semble, toutefois, que ces traits s'observent dans la régulation du traitement des données et, plus encore, dans l'approche *by design*. Evoquant une des scènes de fin du roman *Big Brother* de George Orwell, il explique que l'on peut observer le passage « *de l'interdit (qui ménage la liberté : « tu ne dois pas »), à l'impératif (qui la contraint déjà plus fortement : « tu dois »), et finalement à l'estompement du normatif au profit de la prédiction, ou mieux : de la détermination qui réduit à rien cette liberté (« tu es »)* ». Il ajoute : « *Plutôt que d'interdire un comportement et de le sanctionner éventuellement a posteriori, on anticipe les dispositions du sujet, on les oriente, les formate, les conditionne dans le sens souhaité* »[2421]. Si les dispositifs techniques, tels que nous les avons décrits jusqu'alors, peuvent être prédéfinis de sorte à préserver le secret des données à caractère personnel dans le domaine de la santé, alors les règles juridiques organisant la protection des informations relatives à cette part de leur intimité pourraient se révéler redondantes et donc inutiles. Les discours sur la disparition du « secret médical » et les dangers qui le guêtent sont, sous cet angle encore, frappés de cécité, dans la mesure où ce n'est pas cet aspect intime de la vie privée des personnes qui est en danger *mais les règles juridiques qui régulent le jeu de la parole et du silence*. Le secret est la technique. Il ne s'agit là que d'une potentialité, il faudrait, pour qu'elle se réalise qu'il n'y ait plus *d'information*, c'est-à-dire plus de sens à former pour l'esprit humain, plus de *parole* à *opposer* au *silence*. Que se réalise « *la médecine sans patient et sans médecin* »[2422] ébauchée par Gilles Deleuze, ou que se réalise

---

[2420] M. FOUCAULT, *Sécurité, territoire, population. Cours au Collège de France, 1978*, Seuil/Gallimard, 2004, pp. 48-49 ; *Adde* F. OST, *A quoi sert le droit ? Usages, fonctions et finalités*, *op. cit.*, p. 304 ; A propos de la gouvernementalité algorithmique, v. A. ROUVROY et T. BERNS, « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », *Réseaux* 2013/1, n° 177, p. 174.
[2421] Ibid. p. 298.
[2422] G. DELEUZE, « Post-scriptum sur les sociétés de contrôle », *in Pourparlers 1972-1990*, Editions de Minuit, 1990.

totalement la médecine dite des « 4 P » (personnalisée, préventive, prédictive et participative) et les projets de l'intelligence artificielle[2423]. Il n'y aurait, alors, plus besoin de préserver la confiance dans les professions historiquement soumises au secret, consubstantielle à l'institution du secret professionnel, la machine permettrait la certitude du déterminisme. Il peut paraître évident que la régulation juridique du secret des données à caractère personnel dans le domaine de la santé serait vouée à disparaître avec la relation interpersonnelle qui en est la base, mais cette mise en contexte éclaire mieux, nous l'espéons, les enjeux. Il ne s'agit pas de verser dans le discours prophétique mais il nous fallait, à ce stade, examiner le phénomène en cours en prenant le recul le plus important possible.

478. Conclusion du second chapitre. Les secrets professionnels, dont nous avions expliqué qu'ils n'étaient pas tous de même ordre, sont hierarchisés au regard du risque de réidentification des personnes concernées par les données. L'utilisation des techniques de pseudonymisation n'est pas nouvelle. Dès les débuts de la loi information et libertés la CNIL admettait cette technique comme moyen d'assurer le secret. Elle a ainsi autorisé la transmission des données issues de la relation de soin à des acteurs ne participant pas à la prise en charge, à condition que soient prises des mesures qui, dans les années 1980, garantissant l'anonymat. La mise en relief des techniques de pseudonymisation laisse voir que s'opère une hiérarchisation des secrets professionnels facilitant le partage des utilités des données et visant à graduer l'accès a celles-ci.

Cette hierarchisation n'est pas explicite, elle sout de l'utilisation des techniques de pseudonymisation. L'influence de la diversification des dispositifs normatifs est encore visible dans les instruments de l'Union européenne et les normes de droit souple nationales. La référence aux normes techniques et managériales se fait plus visible puisque certains instruments européens y font explicitement référence. Au niveau national, les instruments de l'ASIP-santé et de la CNIL, dans le domaine de la santé, sont établies sur la base de normes techniques nationales, européennes et internationnales. Par ailleurs, ce que nous avons identifié comme un phénomène d'enchevêtrement normatif s'observe encore en sens inverse, les normes techniques sont spécifiquement conçues pour *appliquer* les dispositions du RGPD. En dernière analyse, le couple formé par les dispositifs techniques de l'information et de la communication

[2423] « *La relation de soin et la prise en charge de la personne dans le cadre de la médecine reposent classiquement sur un rapport humain fondé sur la confiance, l'écoute, l'observation, l'utilisation d'indicateurs physiologiques et l'expérience ; ce rapport ne peut qu'être profondément modifié par la place que prendra dans cette démarche une aide à la décision fondée sur l'exploitation algorithmique des données* » (CCNE, Avis n° 130, *Données massives et santé : une nouvelle approche des enjeux éthiques*, p. 13).

et les normes technico-managériales facilite une migration du « droit », si tant est que l'on considère qu'il s'agit encore de droit, dans la structure même des choses. Cette migration n'implique pas la disparition du droit. C'est encore une représentation que de penser que les techniques normalisantes peuvent remplacer la normativité, mais l'on ne peut que prendre acte de l'actractivité que présente la normalisation par les dispositifs techniques.

479. Conclusion du second titre. Certains moyens de préserver les données et, dans le cadre de notre étude, les données issues de la prise en charge des personnes dans le système de santé, ne sont pas des normes juridiques. Les normes techniques et managériales occupent une place de plus en plus importante dans la mise en œuvre de la confidentialité et apparaissent mieux adaptées aux enjeux des technologies de l'information que ne l'est le secret professionnel. Ce que nous laissait d'ailleurs entrevoir l'étude de la doctrine de la CNIL au regard de laquelle le secret professionnel n'était qu'un instrument de réservation des données parmi d'autres. La cybersécurité et la *Privacy by design* telle qu'elle est entendue dans le RGPD, entretiennent un lien de filiation certains avec ces normes. Tant le maintien de la sécurité informatique que la protection de la vie privée dès la conception des dispositifs techniques appellent ces normes. Elles sont les plus à même de réaliser les conditions de sécurité et de confidentialité nécessaire à la mise en œuvre des Règlements européens. La normalisation technico-manégériale répond en effet à un projet politique européen, elles ont vocation à permettre la création d'un marché unique numérique en santé. Ce qui laisse entrevoir que les utilités des données issues de la relation de soin sont déstinées à être partagé en dehors du territoire national. La hierarchisation des secrets professionnels et la graduation des accès, permises par les techniques de pseudonymisation seraient, à cet égard, un moyen adéquat de préservation des données. En dernier lieu, la migration du secret dans les objets pose une question anthropologique essentielle.

480. Rien n'est sans doute rien de plus banal que de clore nos propos sur une idée mille fois répétée. Il s'agira de notre seule prise de position, elle ne consiste pas en une quelconque invitation a protéger la vie privée, mais sur un plan plus général : Tant que la relation entre les professionnels du soin, du social et du médico-social et les patients demeurera, tant qu'elle ne sera pas remplacée par un autre type d'interaction, hors du réel, c'est-à-dire tant que se formera une rencontre entre des individus, les règles juridiques, dont le secret professionnel, continueront à produire du sens. Quant à l'influence des dispositifs techniques de l'information et de la communication sur le « secret médical », il convient de prendre acte que le secret

compris comme un moyen de préservation des données est, au moins partiellement, *transféré* dans l'architecture des objets pour empêcher l'accès des tiers, mais également les mésusages – c'est-à-dire les révélation involontaires – et, dans une certaine mesure, les révélations volontaires.

CONCLUSION DE LA SECONDE PARTIE.

481. Le secret professionnel comme « moyen » privilégié de protection du secret « objet » est affaibli. Cet affaiblissement procède moins d'une véritable généralisation au regard de laquelle la nature de l'information ou des données dicterait les désignations des personnes qui y sont astreintes que d'une diversification des secrets professionnels au sein du système de santé. Les intervenants techniques grâce auxquels les traitements de données remplissent leurs finalités ne disposent pas toujours des options de conscience offertes aux professionnels dont la soumission au secret tient à leur rôle social et qui, en général, prennent part à la prise en charge des personnes. Cela est particulièrement visible dans la loi informatique et libertés puisque toutes les personnes réutilisant les données issues de la relation de soin sont désormais soumises au secret professionnel. Le critère central de ces désignations se trouve dans la source des données plus que dans leur nature. Car, si la nature des données fondait le secret professionnel, il importerait de soumettre au secret professionnel tous les acteurs privés qui traitent les données avec le consentement de la personne.

482. Il est également remarquable que chaque nouveau texte de désignation entraîne une nouvelle obligation ou permission de révéler. Etudier les traitements de données issues des soins sous le prisme étatique permet de comprendre comment s'opère l'équilibre entre l'efficacité des traitements, instruments de l'Etat et des personnes publiques, et le secret professionnel. Sous ce même angle, il apparaît que le consentement de la personne concernée n'est pas au centre des dispositifs de réutilisation des données. Ni la personne, ni le professionnel n'en a la maîtrise complète. Le discours de la doctrine décrit un glissement de la « maîtrise du secret », du professionnel vers le patient, il nous semble pourtant que les choses soient bien plus complexes qu'elles n'y paraissent. Le patient maîtrise les informations contenues dans ses dossiers médicaux, le professionnel n'en perd pas pour autant toute maîtrise dès lors qu'il n'est pas possible de le contraindre à parler. Néanmoins, plus on s'éloigne de ce centre plus l'on observe que les données issues de la relation de soin sont réutilisées et partagées. Elles seraient désormais des *communs*, produites par le système de santé, le partage de leurs utilités est plébiscité. Bien que la portée du secret professionnel soit affaiblie, le secret de la vie privée des personnes n'en est pas moins renforcé, la confiance qu'elles portent dans le système de santé est construit par ailleurs, sur d'autres bases. C'est que d'autres mécanismes viennent réguler la communication des données. Les normes techniques et managériales

occupent une place de choix dans la régulation du secret des données issues de la relation de soin. Qu'elles soient issues d'organismes nationaux, européens ou internationaux elles présentent une flexibilité et une adaptabilité sans commune mesure avec les règles juridiques. Elles constituent en outre un outil efficace pour la mise en œuvre d'un marché unique des données de santé. Moins couteuses, elles permettent également de passer outre les complexités d'une législation européenne trop précise ou dans des domaines où les Etats sont encore souverains. Enfin, c'est un dernier mouvement qui s'observe, celui d'un enchevêtrement normatif. Il est fait référence aux normes techniques dans les instruments juridiques de l'Union européenne et dans les instruments de droit souple produits par les agences de l'Etat en charge de la sécurité des systèmes d'information. Dans le domaine de la santé, les référentiels et guides de l'ASIP-santé constituent un bon point d'observation de ce phénomène. Enfin, le secret dans les choses, s'il n'est plus tout à fait à l'état de potentialité ne signifie par une disparition du secret professionnel. Il partage la tâche l'un étant un « moyen » de régulation dans le monde physique, l'autre, agissant comme régulation normalisatrice.

CONCLUSION GENERALE

483. Mener une étude relative à l'influence des technologies de l'information et de la communication sur le « secret médical » nous a conduit à adopter la distinction la plus ouverte possible : le secret « objet » et le secret « moyen ». L'étude du droit commun et la mise au jour des fonctions – que l'on peut qualifier de « primaires » – des techniques de l'information et de la communication, a d'abord permis de souligner les rapports entre l'information et son support. En prenant de la distance avec la conception traditionnellement admise du « secret médical », nous avons considéré le secret « objet » de la manière la plus extensive possible en retenant qu'il s'agit du « secret des informations relatives aux personnes prises en charge par un professionnel intervenant dans le système de santé ». Il a ensuite été possible de déterminer que l'*instrumentum* – incorporant l'information secrète représentée – bénéficiait également d'une protection, assurée aussi bien par des mécanismes classiquement rattachés à la protection des biens que par ceux classés dans la catégorie du droit au respect de la vie privée. L'appréhension de l'information indépendamment de son support, notamment rendue possible par l'évolution des dispositifs techniques, a occasionné certaines adaptations jurisprudentielles et légales des infractions sanctionnant les atteintes aux biens. La fonction de communication des dispositifs est également saisie par le droit afin d'assurer la réservation du secret « objet » d'une protection. Cette analyse retraçant l'état du droit positif permet d'affirmer que le droit commun offre une protection du secret des informations issues de la relation de soin, quel que soit le mode d'existence de ce secret.

484. Concernant plus spécifiquement les fonctions de communication et de captation ou fixation à distance, il a été expliqué qu'elles pouvaient être employées pour percer le secret. Ici encore le droit commun s'applique, certaines règles nécessitant une adaptation, d'autre non. Dans cette dernière hypothèse, la neutralité technologique des textes remplit son office. En tant que moyen de communication les dispositifs techniques sont également des moyens de révélation du secret « objet » par le professionnel soumis au secret professionnel. Le caractère compréhensif du texte d'incrimination permet de sanctionner la violation du secret

professionnel indépendamment du moyen employé. Néanmoins, l'infraction ne sera constituée que lorsque la révélation a un caractère volontaire. Il apparaît, à l'étude du droit commun applicable aux usages des dispositifs techniques de l'information et de la communication, que le secret « objet » bénéficie d'une protection multipolaire adaptée tant aux évolutions des moyens d'appréhender le secret qu'aux moyens de le révéler.

485. Toutefois, cette analyse est insuffisante pour mesurer les ressources déployées afin de protéger juridiquement le secret relatif aux personnes prises en charge par un professionnel intervenant dans le système de santé dans les contextes d'usage des dispositifs techniques de l'information et de la communication. Elle exclut une partie des fonctions que les dispositifs techniques de l'information et de la communication ont acquis par l'effet de la convergence technologique : le traitement des données. Les potentialités de la puissance de l'informatique ont conduit à la création d'une législation – ayant fait l'objet de multiples adaptations depuis sa création – spécifiquement applicable à cet emploi. Ces dispositions ont pour objet le traitement des données à caractère personnel. L'étude du champ d'application de ces dispositions nous apprend que « *les informations couvertes par le secret professionnel dans le domaine de la santé* », lorsqu'elles sont traitées, sont également des données à caractère personnel sensibles. Le traitement emporte donc la coexistence de deux qualifications pour ce même objet. Par ailleurs, les opérations caractérisant le traitement révèlent la nature dynamique de la protection des données à caractère personnel. En comparaison l'infraction sanctionnant la violation du secret professionnel n'a pas pour fonction d'organiser la circulation des informations. Il apparaît encore que l'assujettissement au secret professionnel constitue une *condition du traitement* des données issues d'informations couvertes par le secret et une *conséquence de la réutilisation* des données. Le jeu des mécanismes s'opère de manière récursive.

486. L'articulation des dispositions relatives à la protection des données à caractère personnel et de l'infraction sanctionnant la violation du secret professionnel met, de plus, en lumière la complémentarité entre l'obligation de confidentialité – dont le non-respect est pénalement sanctionné – et l'infraction sanctionnant la violation du secret professionnel. La confidentialité constitue un moyen supplémentaire de protection du secret « objet » et la CNIL appréhende le secret professionnel comme un moyen parmi d'autres de garantir la confidentialité. Ainsi, d'autres moyens sont mobilisés pour assurer le secret des données issues de la prise en charge des personnes dans le système de santé. Ces moyens sont parfois mis en œuvre pour contourner la rigidité du secret professionnel et autoriser la communication des données hors des situations prévues par le législateur. L'articulation des dispositions relatives

à la protection des données à caractère personnel et de l'infraction sanctionnant la violation du secret professionnel révèle, enfin, l'influence centrale de la CNIL quant aux aménagements successifs dont le secret professionnel a fait l'objet.

487. La première conséquence du traitement des données issues de la relation de soin consiste ainsi dans une généralisation du secret professionnel. Rien ne permet, pour autant, d'affirmer, comme le font certains commentateurs, que la nature de l'information ou des données serait le critère de désignation. L'examen des textes de désignation inscrits dans l'ensemble du Code de la santé publique à la lumière de la doctrine de la CNIL incline à envisager un autre critère. Les acteurs techniques de tous ordres sont soumis au secret professionnel car, sans eux, les traitements de données ne peuvent être mis en œuvre et répondre à leur finalité. Ensuite, toutes les personnes réutilisant les données issues de la prise en charge – et donc couvertes par le secret professionnel – sont à leur tour astreintes au secret professionnel. Sous cet angle, il est formé une « chaîne de secrets » dont le critère central consiste dans la source des données. Il semble toutefois possible de différencier le régime du secret des professionnels originellement soumis au secret et celui des acteurs qui ne sont pas en relation avec le malade. Il faudrait considérer qu'il existe des secrets de « premier rang » et des secrets de « second rang », ces derniers ne bénéficiant pas des options de conscience propres aux premiers.

488. L'extension du champ d'application de l'infraction sanctionnant la violation du secret professionnel s'accompagne d'un affaiblissement considérable de la portée des secrets professionnels de « premier rang ». Une conciliation s'effectue entre la restriction de la circulation de l'information induite par le secret professionnel et les intérêts poursuivis par les traitements étatiques des données de santé. Des exceptions sont, ainsi, successivement admises à des fins d'évaluation de l'activité des établissements de santé, de maîtrise des dépenses de santé, de recherche d'intérêt public dans le domaine de la santé et des statistiques, mais également pour la défense de l'ordre public. Alors que l'on pouvait penser, au regard du discours dominant, que le consentement de la personne concernée était une condition essentielle de la réutilisation des données, il est apparu que la personne concernée n'a, au mieux, qu'un droit d'opposition. La représentation selon laquelle « le patient maîtrise le secret » est, à ce titre, fortement remise en cause. Il n'a que la maîtrise des données les plus évidentes à identifier : celles formalisées dans ses dossiers médicaux et désormais réunies sur son espace numérique de santé. Le professionnel de santé n'a pas plus la maîtrise de ces données, puisque la mise en réseau des données a conduit à restreindre le pouvoir d'opposition des professionnels intervenant, principalement, dans les établissements publics. Elle se manifeste encore par la

multiplication des autorisations d'accès aux données non anonymisées au profit des démembrements de l'Etat. S'agissant des données pseudonymisées, leur réutilisation est rendue de plus en plus évidente en dépit du risque de réidentification. Ce mouvement s'accompagne d'un discours politique préconisant le partage des utilités de ces données, qui seraient désormais des biens communs. C'est, dès lors, une maîtrise partagée des données qui se dessine.

489. Il ne peut, pour autant, en être déduit un affaiblissement de la protection du secret « objet ». Dans les rapports où la protection juridique du secret professionnel ne joue plus, d'autres moyens visent à assurer la protection du secret des données. Les normes technico-managériales et les moyens techniques mis en œuvre pour assurer la *Privacy by Design* répondent idéalement au contexte technologique des *Big data*. Ces nouveaux instruments favorisent également la mise en œuvre des politiques nationales et européennes visant à créer un marché unique numérique au sein duquel les données produites à l'occasion des soins occupent une place centrale.

490. L'on remarque, en outre, qu'est à l'œuvre un phénomène d'enchevêtrement normatif. Il se traduit, sur le plan juridique, par une hiérarchisation des secrets professionnels et une graduation des accès aux données produites à l'occasion des soins. La « chaîne des secrets » dépend autant de la soumission au secret professionnel que du risque de réidentification des données, lequel s'apprécie notamment au regard des méthodes de pseudonymisation. Cet enchevêtrement nous semble également perceptible au travers de la multiplication des références aux normes technico-managériales dans les instruments de droit souple produits par la CNIL et l'Asip-santé, tout comme dans les instuments de l'Union européenne. Au dernier stade de l'analyse, il apparaît que le secret des données produites par le système de santé est désormais assuré par des moyens de gestion collective – management – et des moyens techniques. Se dessine alors une forme de migration des normes juridiques dans les dispositifs techniques, qui oriente, très probablement, l'avenir du « secret médical » vers un « secret dans les choses ».

491. Le mouvement que nous avons décrit n'est pas celui d'une marche inéluctable vers la transparence des individus, du moins pas au sens dans lequel l'emploie la doctrine lorsqu'elle

l'oppose au « secret médical »[2424]. En ce qui concerne notre objet d'étude, le « *respect de la vie privée et le secret des informations* » semble renforcé. La seule disparition possible du secret serait celle de son essence : le lien social et l'interaction humaine au fondement de la confiance. Au-delà de la question relative à la disparition du tiers de confiance, des études déjà entreprises dans d'autres disciplines interrogent les formes de confiance dans les dispositifs techniques[2425], la réflexion mériterait peut-être d'être également engagée par les juristes. Par ailleurs, la normalisation technique, encore largement ignorée des juristes, notamment dans le champ de la santé, est, de toute évidence, digne d'intérêt.

[2424] Quelques exemples parmi tant d'autres : D. SICARD, « Quelles limites au secret médical partagé ? », *D.* 2009, p. 2634 ; M. BENEJAT-GUERLIN, « Que reste-t-il de la protection pénale du secret médical ? », *AJ pénal* 2017, p. 368 ; D. TABUTEAU, « Le secret médical et l'évolution du système de santé », *D.* 2009, p. 2629 ; J. LAGREE, « Éthique et partage du secret professionnel », *RDSS* 2015, p. 465 ; P. SARGOS, « Les principes d'immunité et de légitimité en matière de secret professionnel médical », *JCP G* 2004, n° 50, doctr. 187.

[2425] C. LEVALLOIS-BARTH (coord.), *Signes de confiance l'impact des labels sur la gestion des données personnelles*, Institut Mines-Télécom, janv. 2018.

BIBLIOGRAPHIE

§ 1 - Manuels, traités et ouvrages généraux

A

ALLAND D., RIALS S., *Dictionnaire de culture juridique*, coll. Quadrige, Lamy-PUF, 2003.

ARNAUD A.J. (dir.), *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2ème éd., LGDJ 1993.

B

BAILLY A., *Dictionnaire Grec – Français*, Hachette, 1935.

BATTEUR A., *Droit des personnes*, *des familles et des majeurs protégés*, 10ème éd., coll., LGDJ, 2019.

BENTHAM J., *Traité de législation civile et pénale*, coll. Bibliothèque Dalloz, Dalloz, 2010.

BERGEL J.-L., *Méthodologie juridique*, 5ème éd., coll. Méthodes du droit, PUF, 2005.

BERGOIGNAN-ESPER C., DUPONT M., *Droit hospitalier*, 10ème éd., coll. Cours, Dalloz, 2017.

BRAS P.- L., DE POURVILLE G., TABUTEAU D. (dir.), *Traité d'économie et de gestion de la santé*, Presses de Sciences Po – Éditions de santé, 2009.

C

CARBONNIER J., *Sociologie juridique*, coll. Quadrige manuels, PUF, 2004.

CHAMPEIL-DESPLATS V., *Méthodologies du droit et des sciences du droit*, 2ème éd., coll. Méthodes du droit, Dalloz, 2016.

CHAPUS R., *Droit administratif général*, t. II, 10ème éd., Montchrestien, 1997.

CONTE Ph., *Droit pénal spécial*,6ème éd., coll. Manuel, LexisNexis, 2019.

CORNU G.,

- *Linguistique juridique*, 3ème éd., coll. Domat droit privé, Montchrestien, 2005.
- *Vocabulaire juridique*, 12ème éd., coll. Quadrige, PUF, 2018.

CORNU G., *Droit civil*. *Les personnes*, 13ème éd., coll. Précis Domat, Montchrestien, 2007.

D

DELMAS-MARTY M., GUIDICELLI-DELAGE G., *Droit pénal des affaires*, 4ème éd., coll. Thémis, PUF, 2000.

DEMOGUE R., *Traité des obligations en général*, t. V, Rousseau, 1925.

DEUMIER P., *Introduction générale au droit*, 5ème éd., coll. Manuels, LGDJ, 2019.

DE SAUSSURE F., *Cours de linguistique générale*, 3ème éd., Payot, 1931.

DREYER E.,

- *Droit pénal général*, 5ème éd., coll. Manuels, LexisNexis, 2019.
- *Droit pénal spécial*, 3ème éd., coll. Cours magistral, Ellipses, 2016.

DROSS W., *Droit civil*. *Les choses*, LGDJ, 2012.

F

FRYDMAN B., *Petit manuel pratique de droit global*. *L'économie de marché est-elle juste ?* t. 4, coll. L'Académie en poche, Académie Royale de Belgique, 2014.

G

GAUDEMET Y., *Traité de droit administratif*, 16ème éd., LGDJ t. I, 2001.

GUINCHARD S., BUISSON J., *Procédure pénale*, 12ème éd., coll. Manuel, LexisNexis, 2018.

GUINCHARD S., MONTAGNIER G., *Lexique des termes juridiques*, 17ème éd., Dalloz, 2009.

J

JEANDIDIER W., *Droit pénal des affaires*, 5ème éd., coll. Précis, Dalloz, 2003.

L

LALANDE A., *Vocabulaire technique et critique de la philosophie*, coll. Quadrige, PUF, 2010.

LARGUIER J., CONTE P.-H., *Droit pénal des affaires*, 11ème éd., Armand Colin, 2004.

LEPAGE A., MATSOPOULOU H., *Droit pénal spécial*, coll. Thémis, PUF, 2015.

LUCAS A., *Le droit de l'informatique*, 2ème éd., coll. Thémis, PUF, 2001.

M

MALAURIE P., AYNES L., *Droit des biens*, 8ème éd., LGDJ, 2019.

MEMETEAU G., GIRER M., *Cours de droit médical*, 5ème éd., LEH, 2016.

MERLE R., VITU A., *Traité de droit criminel*. *Droit pénal spécial*, t. 2, Cujas, 1982.

MISTRETTA P., *Droit pénal médical*, Cujas, 2013.

N

NAY O., *Lexique de science Politique*, 3ème éd., coll. Lexiques, Dalloz, 2017.

P

PIN X., *Droit pénal général*, 11ème éd., coll. Cours, Dalloz, 2019.

PRADEL J., DANTI-JUAN M., *Droit pénal spécial*, 7ème éd., coll. Référence, Cujas, 2017.

R

RASSAT M.-L.,

- *Droit pénal spécial*, *infractions des et contre les particuliers*, 5ème éd., coll. Précis, Dalloz, 2006.
- *Droit pénal spécial*. *Infractions du Code pénal*, 8ème éd., coll. Précis, Dalloz, 2018.

REY A. (dir.), *Dictionnaire historique et étymologique de la langue française Robert*, t. 2, 3ème éd., 2000.

ROBERT J.-H., *Droit pénal général*, 6ème éd., coll. Thémis, PUF, 2005.

ROCHFELD J., *Les grandes notions du droit privé*, 2ème éd., coll. Thémis, PUF, 2013.

ROUJOU DE BOUBEE G., FRANCILLON J., BOULOC B., MAYAUD Y., *Code pénal commenté*, coll. Dalloz Référence, Dalloz, 1996.

S

SAINT-PAU J.-C., *Traité de droit de la personnalité*, 1ère éd., coll. Traités, LexisNexis, 2013.

SEVE R., *Philosophie et théorie du droit*, 2ème éd., coll. Cours, Dalloz, 2017.

T

TERRE F., FENOUILLET D., *Droit civil*. *Les personnes*. Personnalité – Incapacité – Protection, 8ème éd., coll. Précis, Dalloz, 2012.

TRUCHET D., *Droit de la santé publique*, 9ème éd., coll. Mémentos, Dalloz, 2016.

V

VERON M.,

- *Droit pénal des affaires*, 6ème éd., coll. Compact Droit, Armand Colin, 2005.
- *Droit pénal spécial*, 17ème éd., coll. Université, Sirey, 2019.

VILLEY M., *Philosophie du droit. Définitions et fins du droit. Les moyens du droit*, coll. Bibl. Dalloz, Dalloz, 2001.

Z

ZENATI-CASTAING F., REVET Th.,

- *Les biens*, 3ème éd., coll. Droit Fondamental, PUF, 2008
- *Manuel de droit des personnes*, 1ère éd., coll. Droit fondamental, PUF, 2006.

§ 2 - Thèses, monographies, essais et ouvrages spéciaux

A - Thèses et mémoires (tous domaines)

A

ABDOU A.-F., *Le consentement de la victime*, préf. VOUIN R., coll. Bibl. sc. crim., t. 11, LGDJ, 1971.

ANCEL P., *L'indisponibilité des droits de la personnalité. Une approche critique de la théorie des droits de la personnalité*, th. dact., ss. la dir. de COUTURIER G., soutenue en 1978, Université de Lyon.

ANTIPPAS J., *Les droits de la personnalité*, préf. HUET J., coll. Laboratoire de droit privé & de sciences criminelles, PUAM, 2012.

B

BARDEAU M.-O., *La notion de contrat unilatéral : analyse fonctionnelle*, coll. Bibl. dr. privé, t. 552, LGDJ, 2014.

BAUDOUIN J.-L., *Secret professionnel et droit au secret dans le droit de la preuve*, coll. Bibl. de dr. privé canadien, t. 3 ; LGDJ 1965.

BEAUSSONIE G., *La prise en compte de la dématérialisation des biens par le droit pénal. Contribution à l'étude de la protection pénale de la propriété*, préf. DE LAMY B., coll. Bibl. de dr. privé, t. 532, LGDJ, 2012.

BEIGNIER B., *L'honneur et le droit*, préf. FOYER J., coll. Bibl. dr. privé, t. 234, LGDJ, 1995.

BENEJAT M., *La responsabilité pénale professionnelle*, préf. SAINT-PAU J.-Ch., coll. Nouv. Bibl. th., t. 111, Dalloz, 2012.

BINET J.-R., *Droit et progrès scientifique. Science du droit, valeurs et biomédecine*, coll. Partage du savoir, Le Monde-PUF, 2002.

BONNE-HARBIL A., *Les droits de la personne détenue en matière de santé*, th. dact., ss. la dir. de PY B., soutenue en 2016, Université de Lorraine.

BOU NASSAR P., *Gestion de la sécurité dans une infrastructure de services dynamique : Une approche par gestion des risques,* th. dact. ss. la dir. de BIENNER F., BADAR Y., BARBART K., soutenue le 21 décembre 2012, en informatique et mathématique, Institut National des sciences appliquées de Lyon.

C

CACHARD O., *La régulation internationale du marché électronique*, Préf. FOUCHARD ph., coll. Bibl dr. privé, t. 365, LGDJ, 2002.

CAUPERT F., *La normalisation*, th. dact., soutenue en 1977, Université Montpellier I.

CHAUVET D., *La vie privée-étude de droit privé*, th. dact., ss la dir. de DREYER D., soutenue en 2014, Université Paris-Sud.

CAVALIER M., *La propriété des données de santé*, th. dact. ss. la dir. de GIRER M., soutenue en 2016, Université Lyon III Jean Moulin.

CLUZEL-METAYER L., *Le service public et l'exigence de qualité*, préf. CHEVALLIER J., coll. Nouv. bibl. th., t. 52, Dalloz, 2006.

COCHE A., *La détermination de la dangerosité des délinquants en droit pénal*. *Etude de droit français*, préf. PRADEL J., coll. Institut de Sciences Pénales et de Criminologie, PUAM, 2005.

CONTIS M., *Secret médical et évolutions du système de santé*, préf. NEIRINCK C., Coll. Thèses, Les Etudes Hospitalières, 2010.

COULIBALY I., *La protection des données à caractère personnel dans le domaine de la recherche scientifique*, th. dact., ss. la dir. de VERGES E., DE LAMBERTRIE I., soutenue en 2011, Université de Grenoble.

COUTURIER M., *Pour une approche fonctionnelle du secret professionnel*, th. dact., ss. la dir. de PROTHAIS A., soutenue en 2004, Université Lille II.

D

DANA A.-C., *Essai sur la notion d'infraction pénale*, coll. Bibl. sc. crim., LGDJ, 1982.

DARTIGUELONGUE J.-P., *Le secret dans les relations juridiques*, th. dact., soutenue le 21 décembre 1968, Université de Bordeaux.

DECOCQ A., *Essai d'une théorie générale des droits sur la personne*, préf. LEVASSEUR G., coll. Anthologie du droit, LGDJ, 1960.

DELAUNAY B., *L'amélioration des rapports entre l'administration et les administrés – Contribution à l'étude des réformes administratives entreprises depuis 1945*, préf. DEBOUY Ch., coll. Bibl. dr. public, t. 172, LGDJ, 1993.

DENIZOT A., *L'universalité de fait*, coll. Thèses, t. 23, Institut universitaire Varenne-LGDJ, 2008.

F

FABRE-MAGNAN M., *De l'obligation d'information dans les contrats*. *Essai d'une théorie*, préf. GHESTIN J., coll. Anthologie du droit, LGDJ, 1992.

FERRIE S.-M., *Le droit à l'autodétermination de la personne humaine : essai en faveur du renouvellement des pouvoirs de la personne sur son corps*, préf. LOISEAU G., coll. Bibliothèque de l'Institut de Recherche Juridique de la Sorbonne-André Tunc, Vol. 92, IRJS, 2018.

FERY B., *Gouverner par les données ? : Pour une analyse des processus de traduction dans l'usage des systèmes d'information : Déploiement et utilisations de Cassiopée dans l'Institution pénale*, th. dact., ss. la dir. de DE MAILLARD J., soutenue en 2015, Université de Versailles-Saint-Quentin-en-Yvelines.

G

GERRY-VERNIERES S., *Les « petites » sources du droit*. *A propos des sources étatiques non contraignantes*, préf. MOLFESSIS N., coll. Recherches juridiques, Economica, 2012.

GIRER M., *Contribution à une analyse rénovée de la relation de soins : Essai de remise en cause du contrat médical*, coll. Thèses, LEH, 2010.

GUINCHARD S., *L'affectation des biens en droit privé français*, coll. Bibl. dr. privé, t. 145, LGDJ, 1976.

GUTMANN D., *Le sentiment d'identité – étude de droit des personnes et de la famille*, préf. TERRE F., coll. Bibl. dr. privé, t. 327, LGDJ, 2000.

H

HELLENBRAND L., *Secret et justice pénale*, th. dact., ss. la dir. de VITU A., soutenue en 1997, Université Nancy II.

J

JAY C., *Le risque santé et la souscription d'assurance du crédit*, th. dact., ss. la dir. de PY B., soutenue en 2017, Université de Lorraine.

JOLY-PASSANT E., *L'écrit confronté aux nouvelles technologies*, coll. Bibliothèque de droit privé, t. 465, LGDJ, 2006

L

LANGARD S., *Approche juridique de la télémédecine : entre droit commun et règles spécifiques*, th. dact., ss. la dir. de PY B., THIERRY J.-B., soutenue en 2012, Université de Lorraine.

LAROUER M., *Les codes de conduite, sources du droit*, préf. DEUMIER P., coll. Nouv. Bibl. th., t. 176, Dalloz, 2018.

LAVERGNE B., *Recherche sur la soft law en droit public français*, préf. JACQUINOT N., coll. Thèses de l'IFR, LGDJ, 2013.

LASZLO-FENOUILLET D., *La conscience*, préf. CORNU G., Bibl. Dr. privé, t. 235, LGDJ, 1993.

LEONHARD J., *Etude sur la pornographie pénalement prohibée*, th. dact., ss. la dir. de PY B., soutenue en 2011, Université de Lorraine.

LESAULNIER F., *L'information nominative*, th. dact. ss. la dir. de CATALA P., soutenue en 2005, Université Paris II.

LI X., *Evaluation et amélioration des méthodes de chaînage de données*, th. dact. ss. la dir. de BOIRE J.-Y., OUCHCHANE L., soutenue le 29 janv. 2015, Université d'Auvergne.

LIVET P., *Autorisation administrative préalable et les libertés publiques*, LGDJ, 1974.

LOLIES I., *La protection pénale de la vie privée*, préf. GASSIN R., coll. « Institut de Sciences Pénales et de Criminologie », PUAM, 1999.

LOUHIBI-BENATEK F., *Le secret professionnel*, th. dact., ss. la dir. de BERNARDINI R., 1997 Université de Nice.

LOUIS-CAPORAL D., *La distinction du fait et du droit en droit judiciaire privé*, th. dact., ss. la dir. de MATHIEU M.-L., soutenue le 21 novembre 2014, Université Montpellier I.

M

MANGEMATIN C., *La faute de fonction en droit privé*, préf. MALABAT V., coll. Nouv. bibl. th., vol. 135, Dalloz, 2014.

MARLIAC-NEGRIER C., *La protection des données nominatives informatiques en matière de recherche médicale*, préf. GENIOT M., PUAM, 2001.

MORON-PUECH B., *Contrat ou acte juridique ? Étude à partir de la relation médicale*, th. dact., ss. la dir. de FENOUILLET D., 2016, Université de Panthéon-Assas.

MOUCHETTE J., *La magistrature d'influence des autorités administratives indépendantes*, préf. WACHSMANN P., LGDJ, coll. Bibl dr. public, t. 303, 2019.

N

NERSON R., *Les droits extrapatrimoniaux*, préf. ROUBIER P., Bosc frères, 1939.

NETTER E., *Numérique et grandes notions du droit privé*, mémoire présenté pour l'obtention de l'HDR ss. la dir. de ROCHFELD J., soutenu le 20 novembre 2017.

O

OCHOA N., *Le droit des données personnelles*, *une police administrative spéciale*, th. dact., ss. la dir. de TEITGEN-COLLY C., 2014, Université Paris I-Panthéon-Sorbonne.

P

PELTIER V., *Le secret des correspondances*, préf. CONTE Ph., coll. Institut de droit des affaires, PUAM, 1999.

PERELMAN Ch., *Logique juridique. Nouvelle rhétorique*, 2ème éd., coll. Méthodes du droit, Dalloz, 1979.

PIAZZON Th., *La sécurité juridique*, préf. LEVENEUR L., coll. Doctorat & Notariat, t. 35, Defrénois, 2009.

PIC E., *Caractérisation de l'anglais des droits de l'Homme en tant que langue de spécialité. Un essai de méthodologie terminologique*, th. dact. de linguistique théorique, descriptive et automatique, ss. la dir. de HYMBLEY J., 2007, Université Paris Diderot.

PICARD E., *La notion de police administrative*, préf. DRAGO R., coll. Bibl. dr. public, t. 146, LGDJ 1984.

PIN X., *Le consentement en matière pénale*. *Contribution à une étude juridique*, préf. MAISTRE DU CHAMBON P., Bibl. sc. crim., t. 36, LGDJ, 2002.

PY B., *Recherches sur les justifications pénales de l'activité médicale*, th. dact., ss. la dir. de SEUVIC J.-F., soutenue en 1993, Université de Nancy II.

R

RAHALI C., *Le secret professionnel et l'action médico-sociale*, th. dact., ss. la dir. de PY B., 2014, Université de Lorraine.

RASCHEL E., *La pénalisation des atteintes au consentement dans le champ contractuel*, th. dact. ss. la dir. de DANTI-JUAN M., SCHÜTZ R.-N., soutenue en 2013, Université de Poitiers.

RENAUD L., *Dix ans de discours sur le téléphone mobile*. *Contribution à l'analyse des discours accompagnant l'insertion sociale des objets techniques contemporains*, th. dact. ss. la dir. de TETU J.-F., soutenue en 2007, Université de Lyon II.

RENOUF M., *Contribution à l'analyse juridique de la notion de valeur : essai sur les biens à valeur négative*, th. dact., ss. la dir. de AUDIT M., soutenue en 2012, Université de Caen.

ROCAYAURA C., *Réflexions sur la dématérialisation de la procédure pénale*, th. dact., ss. la dir. de THOMAS D., soutenue en 2013, Université de Montpellier 1.

ROUSVOAL L., *L'infraction composite- essai sur la complexité en droit pénal*, th. dact., ss. la dir. de MORVAN P., soutenue en 2011, Université de Rennes.

S

SAINT-PAU J., *L'anonymat et le droit*, th. dact., ss. la dir. de CONTE P., 1998, Université de Bordeaux IV.

SONTAG-KOENIG S., *Les droits de la défense face aux technologies de l'information et de la communication*, th. dact., ss. la dir. de JEAN J.-P., soutenue en 2013, Université de Poitiers.

SUPIOT E., *Les tests génétiques*. *Contribution à une étude juridique*, préf. WATT H., NOIVILLE Ch., coll. dr. de la Santé, PUAM, 2014.

SZTULMAN M., *La biométrie saisie par le droit public*. *Etude sur l'identification et la localisation des personnes physiques*, préf. BIOY X., coll. Bibl. dr. public, t. 305, LGDJ, 2019.

T

TILMAN L., *L'utilisation des technologies de l'information et de la communication à l'hôpital face au droit*, coll. Thèses numériques de la BNDS, LEH, 2019.

THELLIER DE PONCHEVILLE B., *La condition préalable de l'infraction*, préf. VARINARD A., PUAM, coll. Institut de Sciences Pénales et de Criminologie, 2010.

THUILLIER B., *L'autorisation*, *étude de droit privé*, préf. BENABENT A., coll. Bibl. de droit privé, t. 252, LGDJ, 1996.

TURINETTI A., *La normalisation*. *Étude en droit économique*, préf. PENNEAU A., coll. Droit civil et procédures, Connaissances et Savoirs, 2018.

TOURE A., *L'influence des nouvelles technologies dans l'administration de la justice pénale*, th. dact. ss. la dir de CIMAMONTI S., soutenue en 2015, Université d'Aix-Marseille.

V

VAN MEERBEECK J., *De la certitude à la confiance*. *Le principe de sécurité juridique dans la jurisprudence de la Cour de justice de l'Union européenne*, FUSL, 2014.

VAUTHIER J.-P., *Le psychiatre et la sanction pénale*, th. dact., ss. la dir. de PY B., soutenue en 2013, Université de Lorraine.

VERON P., *La décision médicale*, th. dact., ss. la dir. de VIALLA F., soutenue en 2015, Université de Montpellier.

W

WATRIN L., *Les données scientifiques saisies par le droit*, th. dact., ss. la dir. de PANCRAZI M.-E., soutenue en 2016, Université d'Aix-Marseille.

Z

ZAGURY V., *Regards sur le droit d'opposition extrapatrimonial : contribution à l'étude de la volonté en droit prive*, th. dact., ss. la dir. de BELLIVIER F., soutenue le 1er juillet 2009, Université Paris X.

B - Monographies et recueils

1 - Monographies et recueils extra-juridiques

A

ANIS J., *Texte et Ordinateur*. *L'écriture réinventée ?*, coll. « Méthodes en sciences humaines », De Boeck Université, 1998.

ARPAGIAN N., *La cybersécurité*, coll. Que sais-je ?, PUF, 2018.

B

BECK U., *La société du risque*. *Sur la voie d'une autre modernité*, Flammarion, coll. Champs essais, 2008.

BENTHAM J., *La déontologie ou la science de la morale*, ouvrage posthume, revu, mis en ordre et publié par BOWRING J., Charpentier, 1934.

BOULLIER D., *Sociologie du numérique*, coll. « U sociologie », Armand Colin, 2016.

BRETON P., *L'utopie de la communication*, La Découverte, 1992.

C

CANGUILHEM G., *Le normal et le pathologique*, PUF, 1975.

CARDON D., *A quoi rêvent les algorithmes*. *Nos vies à l'heure des big data*, coll. La république des idées, Seuil, 2015.

CARMILLE R., *La Mécanographie dans les administrations*, Recueil Sirey, 1936.

CHAVAND F., *Des données à l'information*. *De l'invention de l'écriture à l'explosion numérique*, coll. Histoire des sciences et des techniques, ISTE éditions, 2017.

CHEVALIER Y., *Système d'information et gouvernance*, coll. Echanges, EME, 2008.

CHEVALLIER J., *Science administrative*, coll. Thémis, 6ème éd., PUF, 2019.

A. COMTE, Cours de philosophie positive : première et deuxième leçon (cours en 72 leçons dispensés en 1926-1927 et publiées en 1830). Le document est accessible en version numérique (et non numérisée) sur <http://classiques.uqac.ca/classiques/Comte_auguste/cours_philo_positive/cours_philo_positive.html> (la citation est issue du document word, p. 64

CROZIER M.et FRIEDBERG E., *L'acteur et le système*, Seuil, 1977.

D

DE FILIPPI P., *Blockchain et cryptomonnaie*, coll. Que sais-je ?, PUF, 2018

DELORT P., *Le Big Data*, coll. Que sais-je ?, PUF, 2015.

DENIS V., *Une histoire de l'identité*. *France 1715-1815*, coll. Epoques, Champ Vallon, 2008.

E

ELLUL J.,

- *Le bluff technologique*, préf. PORQUET J.-L., coll. Pluriel, Hachette, 2012.
- *La technique ou l'enjeu du siècle*, coll. classiques de sciences sociales, Economica, 2008.
- *Le système technicien*, Le cherche midi, 2012.

ESCARPIT R., *Théorie générale de l'information et de la communication*, Hachette Université, 1976.

F

FONTAINE C., *L'empire cybernétique. Des machines à penser à la pensée machine*, Seuil, 2014.

FOUCAULT M.,

- *Archéologie du savoir*, Gallimard, 1969.
- *Il faut défendre la société*. *Cours au collège de France (1975-1976)*, coll. Hautes Études, Seuil-Gallimard, 1997.
- *La volonté de savoir*, Gallimard, 1954.
- *Sécurité, territoire, population. Cours au Collège de France,* 1978, Seuil-Gallimard, 2004.
- *Surveiller et punir*, coll. Tel, Gallimard, 1993.

G

GAUCHET M., *La démocratie contre elle-même*, coll. Tel, Gallimard, 2002.

GERRY-VERNIERES S., *Les « petites » sources du droit*. *A propos des sources étatiques non contraignantes*, préf. MOLFESSIS N., coll. Recherches Juridiques, Economica, 2012.

GRUSON D., *La machine*, *mon médecin et moi*, coll. Editions de l'O, L'Observatoire, 2018.

J

JAMOUS H., GREMION P., *L'ordinateur au pouvoir*. *Essai sur les projets de rationalisation du gouvernement et des hommes*, Seuil, 1978.

JEANNERET Y., *Y-a-t-il (vraiment) des technologies de l'information ?*, coll. Savoirs Mieux, Presses universitaires du Septentrion, 2017.

K

KAHN D., *The Codebreakers : the Story of Secret Writing*, McMillan Pub, 1967.

L

LEOPOLD E., LHOSTE S., *La sécurité informatique*, coll. Que sais-je ? PUF, 2007.

LEGENDRE P., *Sur la question dogmatique en occident*, coll. Sciences humaines, Fayard, 1999.

LEVY-STRAUSS C., *La pensée sauvage*, Plon, 1962.

LOCARD E., *La police : ce qu'elle est*, *ce qu'elle devrait être*, Payot, 1919.

M

MATTELART A., *Histoire de la société de l'information*, 5ème éd., coll. Repères Découverte, La Découverte, 2009.

MCLUHAN M.,

- *Pour comprendre les médias*, coll. points, Seuil, 1968.
- *Understanding Media: The Extensions of Man*, Gingko Press, 2003.

MELESE J., *Approches systémiques des organisations*, *vers l'entreprise à complexité humaine*, Éditions d'organisation, 1990.

M. MERLEAU-PONTY, *Parcours* II, 1951-1961, collection « Philosophie », Éditions Verdier, 2000, p. 13.

MICHAEL ALVAREZ R., *Computional Social Science : Discovery and Prediction*, Cambridge University Press, 2016.

MUMFORD L., *Technique et civilisation*, Parenthèses, coll. eupalinos, 2016.

O

OSTRÖM E., *La gouvernance des biens communs : pour une nouvelle approche des ressources naturelles*, Editions De Boeck, 2010.

P

PARSONS T., *The social system*, Glencoe - Free Press, 1951.

PEDAUQUE R.,

- *Le Document à la lumière du numérique : forme*, *texte*, *médium*. *Comprendre le rôle du document numérique dans l'émergence d'une nouvelle modernité*, C&F éditions, 2006.
- *La Redocumentarisation du Monde*, Éditions Cépadues, 2007.

S

SEGAL J., *Le zéro et le un*, coll. Sciences & philosophie, Éditions Matériologiques, 2011.

SERRES M.,

- *Hermès III*, *la traduction*, coll. Critique, Éditions de Minuit, 1974.
- *Retour au contrat naturel,* coll. Conférences et Etudes, BNF, 2000.

SFEZ L.,

- *Critique de la communication*, coll. Points essai, Points, 1992.
- *Technique et Idéologie. Un enjeu de pouvoir*, coll. La couleur des idées, Seuil, 2002.

SIMMEL G., *Secret et sociétés secrètes*, Circé, 1991.

SOURNIA J.-C., *Histoire de la médecine*, coll. Poche/Sciences humaines et sociales, La Découverte, 2004.

SUPIOT A., *La gouvernance par les nombres*, *Cours au collège de France (2012-2014)*, coll. poids et mesures du monde, Fayard, 2015.

V

VITALIS A.,

- *Informatique*, *Pouvoir et Libertés*, 2ème éd., coll. Politiques comparée, Economica, 1988.

- *L'incertaine révolution numérique*, coll. Systèmes d'information, web et société, Série informatique et société connectées, vol. 1, ISTE éditions, 2016.

W

WIENER N.,

- *Cybernetics : Control and communication in the animal and the machine*, The MIT Press, 1948.
- *Cybernetique et société*, coll. 10/18, Edition des Deux-Rives, 1971.

2 - Monographies et recueils juridiques

A

AMSELEK P., *Cheminements philosophiques dans le monde du droit et des règles en général*, coll. Le temps des idées, Armand Colin, 2012.

ATIAS Ch.,

- *Questions et réponses en droit*, coll. L'interrogation philosophique, PUF, 2009.
- *Théorie contre arbitraire*, coll. les voies du droit, PUF, 1987.

B

BECCARIA C., *Des délits et des peines*, coll. La croisée des chemins, ENS,2009.

BENSOUSSAN A., *Informatique et libertés*, Francis Lefebvre, 2008.

BIDAUD H., BIGNON P., CAILLOUX J.-P., *La fonction juridique et l'entreprise*, coll. Gestion Droit, Eska, 1995.

BRAS P.-L., DE POURVILLE G., TABUTEAU D., *Traité d'économie et de gestion de la santé*, Ed. Presses de Sciences Po – Editions de santé, 2009.

BRUGUIERE J.-M., *Les données publiques et le droit*, Litec, 2002.

C

CARBONNIER J.,

- *Flexible Droit*. *Pour une sociologie du droit sans rigueur*, 10ème éd., LGDJ 2001.
- *Droit et passion du droit sous la Ve République*, coll. Champs essais, Flammarion, 2008.

CARDOZO B.-N., *La nature de la décision judiciaire*, coll. Rivages du droit, Dalloz, 2011.

CASTETS-RENARD C., *Le droit de l'internet*, coll. Cours, Montchrestien – Lextenso éditions, 2010.

CHEVALLIER J., *L'État post-moderne*, 4ème éd., coll. Droit et société, LGDJ, 2014.

CLEMENT J.-M., *Question de politiques hospitalières-Organisation médicale*, *technocratie-Droits des malades*, LEH, 2015.

CNIL, *Les données génétiques*, coll. point Cnil, La documentation française, 2017.

COQ V., *Nouvelles recherches sur les fonctions de l'intérêt général dans la jurisprudence administrative*, préf. PLESSIX B., L'Harmattan, coll. Logiques juridiques, 2015.

D

DAMIEN A., *Le secret nécessaire*, Desclée de Brouwer, Paris, 1989.

DEBET A., MASSOT J., METALLINOS N., *Informatique et libertés*. *La protection des données à caractère personnel en droit français et européen*, coll. Les intégrales, Lextenso éditions, 2015.

DELMAS-MARTY M., *Libertés et sûreté dans un monde dangereux*, Seuil, coll. La couleur des idées, 2010.

DERIEUX E., *Droit de la communication*. *Droit européen et international*, 3ème éd., coll. Legipresse, Victoires, 2011.

DEVEJEANS N., *Traité de droit et d'éthique de la robotique civile*, coll. Science, éthique et société, LEH, 2017.

DUPUY O., *Le dossier médical*, 2ème éd., LEH, coll. essentiel, 2005.

E

EYNARD J., *Les données personnelles*. *Quelles définitions pour un régime de protection efficace ?* Michalon, 2013.

F

FABRE-MAGNAN M., *L'institution de la liberté*, PUF, 2018.

FERAL-SCHUHL C., *Cyberdroit*. *Le droit à l'épreuve d'internet*, coll. Praxis, Dalloz, 2018-2019.

FERRAUD-CIANDET N., *Droit de la télésanté et de la télémédecine*, Editions Heures de France, 2011.

FRAYSSINET J., *Informatique*, *fichiers et libertés*, Litec, 1992.

FRISON-ROCHE M.-A.,

- *Les 100 mots de la régulation*, coll. Que sais-je ?, PUF, 2011.
- *Secrets professionnels*, coll. Essai, Editions Autrement, 1999.

FRYDMAN B., *Le sens des lois*, 2ème éd., coll. penser le droit, Bruylant-LGDJ, 2007.

G

GARÇON E., *Code pénal annoté*, t. 2, éd. refondue et mise à jour par ROUSSELET M., PATIN M., ANCEL M., Sirey, 1956.

GARIN A., *Le droit d'accès aux documents : en quête d'un nouveau droit fondamental dans l'Union européenne*, Pedone, 2017.

GASSIN R., *Le droit criminel face aux technologies nouvelles de la communication*, Economica, 1986.

GENY F., *Science et technique en droit privé positif : nouvelle contribution à la critique de la méthode juridique*, Sirey, 1913.

GLEIZAL J.-J., *Figures du secret*, Presses universitaires de Grenoble, 1986.

GROS J., *Santé et nouvelles technologies de l'information*, Conseil économique et social, 2002.

GROS F., *Le principe sécurité*, coll. NRF Essais, Gallimard, 2012.

GUERY C., CHAMBON P., *Droit et pratique de l'instruction préparatoire*. *Juge d'instruction*, *chambre de l'instruction*, coll. Dalloz Action, Dalloz, 2018-2019.

GURVITCH G., *L'expérience juridique et la philosophie pluraliste du droit*, Pedone, 1935.

H

HABERMAS J., *Droit et démocratie*, Gallimard, 1997.

HERVE C., STANTON-JEAN M., MARTINANT E., C, *Les systèmes informatisés complexes en santé*, coll. Thèmes et commentaires, Dalloz, 2013.

HOQUET-BERG S., PY B., *La responsabilité du médecin*, coll. Droit professionnel, HDF, 2006.

J

JEULAND E., *Théorie relationiste du droit. De la* French Theory *à une pensée européene des rapports de droit*, LGDJ, 2016.

K

KAYSER P., *La protection de la vie privée par le droit*. *Protection du secret de la vie privée*, 3ème éd., Economica - PUAM, 1995.

KELSEN H., *Théorie pure du droit*, 2ème éd., Dalloz, 1962.

KULLMAN J., « Assurance de personne : vie-prévoyance-Exécution du contrat d'assurance », *Rep. civ.*, Janvier 2013, (act. Juillet 2019).

L

LAFFAIRE M.-L., *Protection des données à caractère personnel*, Éditions d'Organisation, 2005.

LARGUIER A.-M., *Certificats médicaux et secret professionnel*, Dalloz, 1963.

LASSERRE V., *Le nouvel ordre juridique*. *Le droit de la gouvernance*, LexisNexis, 2015.

LESSIG L., *Code and Other Laws of Cyberspace*, Basic Books éditeur, 1999.

LUCAS A., *Droit de l'informatique et de l'Internet*, coll. Thémis, PUF, 2001.

LUCAS H.-J., DE LAMBERTERIE I., *Informatique, libertés et recherche médicale*, coll. CNRS Droit, CNRS éditions, 2001

M

MAILLARD DESGREES DU LOU D., *Droit des relations de l'administration avec les usagers*, PUF, 2000.

MAISL H., *Le droit des données publiques*, LGDJ 1996.

MATTATIA F., *Le droit des données personnelles*, 2ème éd., EYROLLES, 2016

MIE A.-L., *L'administration et le droit à l'information : Le secret en question*, coll. L'administration nouvelle, Berger-Levrault, 1985.

MOOR P., *Pour une théorie micropolitique du droit*, PUF, 2005.

N

NOIVILLE C., *Du bon gouvernement des risques*. *Le droit et la question du "risque acceptable"*, coll. Les voies du droit, PUF, 2003.

O

OST F., *A quoi sert le droit ? Usages*, *fonctions*, *finalités*, coll. Penser le droit, Bruylant, 2016.

P

POULLET Y., *La vie privée à l'heure de la société du numérique*, coll. Essai, Larcier, 2019.

PRADEL J., *Histoire des doctrines pénales*, coll. Que sais-je ?, PUF, 1991.

PY B., *Le secret professionnel*, coll. La Justice au quotidien, L'Harmattan, 2005.

R

RIBEYRE C., *La communication du dossier pénal*, PUAM, 2007.

RIPERT G., *Les forces créatrices du droit*, 2ème éd., LGDJ 1955.

ROCHEFELD J., *Les grandes notions du droit privé*, 2ème éd., PUF, 2013.

ROMANO S., *L'ordre juridique*, 2ème éd., 1946, traduction française par FRANÇOIS L., GOTHOT P., Dalloz, 1975.

ROUBIER P., *Droits subjectifs et situations juridiques*, Dalloz, 2005.

S

SALEILLES R., *De la déclaration de volonté : Contribution à l'étude de l'acte juridique dans le Code civil allemand*, Pichon, 1901.

SAVATIER R., *Les métamorphoses économiques et sociales du droit privé d'aujourd'hui*, 3ème série, Dalloz, 1959.

SUPIOT A., *Homo juridicus*. *Essai sur la fonction anthropologique du Droit*, coll. Essais, Points, 2005.

T

THOUVENIN D., *Le secret médical et l'information du malade*, Presses Universitaire de Lyon, 1982.

TROPER M., *La philosophie du droit*, coll. Que sais-je ?, PUF, 2015.

V

VANDERLINDEN J., *Les pluralismes juridiques*, coll. penser le droit, Bruylant, 2013.

VILLEY M., *Les biens et les choses en droit*, coll. Archives de philosophie du droit, t. 24, Sirey, 1979.

VILLEY R., *Histoire du secret médical*, Seghers, coll. Médecine et Histoire, 1986.

VON JHERING R.,

- *L'évolution du droit*, Librairie A. Marescq, 1901.
- *La lutte pour le droit*, présentation d'JOUANJAN O., coll. Dalloz bibliothèque, Dalloz, 2006.

Z

ZORN C., *Données de santé et secret partagé*. *Pour un droit de la personne à la protection de la ses données de santé partagées*, coll. santé qualité de vie et handicap, PUN, 2010.

C - Ouvrages collectifs, mélanges, actes de colloques

1 - Ouvrages collectifs extra-juridiques

A

ABOUT I., DENIS V., *Histoire de l'identification des personnes*, coll. Repères-Histoire, La Découverte, 2010.

B

BRETON P., PROULX S., *L'explosion de la communication*, coll. Sciences humaines et sociales, La Découverte, 1996.

C

CASELLI G., VALLIN J., WUNCH G. (dir.), *Démographie : Histoire des idées et politiques de population*, t. VII, INED, 2006.

CHEVALLIER J., LOCHAK D., *Science administrative*, t. II, L'administration comme organisation et système d'action, LGDJ, 1978.

D

DE LAMBERTERIE I., LUCAS H.-J., *Informatique*, *libertés et recherche médicale,* coll. CNRS droit, CNRS, 2002.

DUBAR C., TRIPIER P., BOUSSARD V., *Sociologie des professions*, 4ème éd., coll. U, Armand Colin, 2015.

G

GODARD O., HENRY C., LAGADEC P., MICHEL-KERJAN E., *Traité des nouveaux risques*, coll. Folio actuel, Gallimard, 2002.

J

JAUREGUIBERRY F., PROULX S., *Usages et enjeux des technologies de communication*, coll. Poche-société, ERES, 2011.

M

MATTELART A., MATTELART M., *Histoire des théories de la communication*, coll. Repères, La découverte, 2010.

MATTELART A., VITALIS A., *Le profilage des populations – Du livret ouvrier au cybercontrôle*, *coll. Cahiers libres,* La Découverte, 2014.

MERIC J., PESQUEUX Y, SOLE A., *La "société du risque" : analyse et critique,* coll. Gestion, Economica, 2009.

P

PARANCE B., DE SAINT VICTOR J. (dir.), *Repenser les biens communs*, coll. CNRS Economie, CNRS Éditions, 2014.

PEDAUQUE R., SALAUN J.-M., *Le document à la lumière du numérique*, C&F Éditions, 2006.

T

TRICOT A., SAHUT G., LEMARIE J., *Le document : communication et mémoire*, coll. Information et stratégie, De Boeck, 2016.

V

VON JHERING R., *L'évolution du droit (Zweck im Recht)*, trad. DE MEULENAERE O., Chevalier-Marescq et cie, 1901.

2 - Ouvrages collectifs juridiques

A

ARNAUD A.-J. (dir.), *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2ème éd., coll. Anthologie du droit, LGDJ, 1993.

ASSOCIATION H. CAPITANT, *Le contrat électronique*, t. 5, coll. Colloques, éd. Panthéon-Assas, 2003.

B

BALLE F. (dir.), *Lexique d'information communication*, coll. Lexique, Dalloz, 2006.

BEIGNIER B., DE LAMY B., DREYER E., *Traité de droit de la presse et des médias*, coll. Traités, LexisNexis, 2009.

BELLIVIER F., NOIVILLE C., *Les biobanques*, coll. Que sais-je ?, PUF, 2009.

BENSAMOUN A., LOISEAU G. (dir.), *Droit de l'intelligence artificielle*, coll. Les intégrales, LGDJ, 2019.

BERGOIGNAN-ESPER C., DUPONT M., *Droit hospitalier*, 10ème éd., coll. Cours, Dalloz, 2017.

BOULOC B., FRANCILLON J., MAYAUD Y., ROUJOU DE BOUBEE G., *Code pénal commenté – Article par article Livres I à IV*, coll. Dalloz référence, Dalloz, 1996.

BOURCIER D., DE FILIPPI P. (dir.), *Open Data et Big Data – Nouveaux défis pour la vie privée*, coll. Droit et Sciences Politique, Éditions Mare et Martin, 2016.

BRICTEUX C., FRYDMAN B. (dir.), *Les défis du droit global*, coll. Penser le droit, Bruylant, 2018.

BROSSET E., GAMBARDELLA S., NICOLAS G. (dir.), *La santé connectée et « son » droit : approches de droit européen et de droit français*, coll. Droit de la santé, PUAM, 2017.

C

CALLU M.-F., GIRER M., ROUSSET G., Dictionnaire de droit de la santé – Secteur sanitaire, médico-social et social, LexisNexis, 2017.

CAPRON M., QUAIREL-LANOUZELEE F., TURCOTTE M.-F. (dir.), *ISO 26000 : une norme « hors norme » ? – Vers une conception mondiale de la responsabilité sociétale*, Economica, 2011.

CHEROT J.-Y., FRYDMAN B. (dir.), *La science du droit dans la globalisation*, Bruylant, 2012.

D

DAVID C., FOUQUET O., PLAGNET P., RACINE P.-F., *Les grands arrêts de la jurisprudence fiscale*, 4ème éd. Dalloz, 2003.

DEBET A., MASSOT J., METTALINOS N., *Informatique et libertés*, coll. Les intégrales, LGDJ, 2015.

DE LAMBERTERIE I. (dir.), *Les actes authentiques électroniques – Réflexion juridique prospective*, Mission de recherche « droit et justice », La Documentation française, 2002.

DE LAMBERTERIE I., LUCAS H.-J. (dir), *Informatique, libertés et recherche médicale*, CNRS Editions, 2002.

DONIER V., LAPEROU-SCHENEIDER B. (dir.), *Accès au juge : quelles évolutions ? – Recherche sur l'effectivité du droit*, Bruylant, 2013.

DUFFAR J., ROBERT J., *Droits de l'homme et libertés fondamentales*, 8ème éd., coll. Précis Domat, sous coll. Public, LGDJ, 2009.

F

FLORIOT R., COMBALDIEU R., *Le secret professionnel*, Flammarion, 1973.

FORRAY V., PIMONT S., *Décrire le droit...et le transformer – Essai sur la décriture du droit*, coll. Méthode du droit, Dalloz, 2017.

FRYDMAN B., VAN WAEYENBERGE A. (dir.), *Gouverner par les standards et les indicateurs : De Hume au rankings*, coll. Penser le droit, Bruylant, 2013.

G

GARAPON A., LASSEGUE J., *Justice Digitale*, PUF, 2018.

H

HAUTEREAU-BOUTONNET M., KHOURY L., SAINT-PAU J.-C., *L'influence du principe de précaution en droit de la responsabilité civile et pénale – Regards franco-québécois*, coll. Mission de recherche Droit & Justice, Éditions Revue de Droit de l'Université de Sherbrooke, 2015.

HILDEBRANDT M., DE VRIES K. (ss. la dir.), *Privacy, Due Process and the Computational Turn – The Philosophy of Law Meets the Philosophy of Technology*, Oxford, Routledge, 2013

J

JESTAZ P., JAMIN C., *La doctrine*, coll. Méthodes du droit, Dalloz, 2004.

K

KOUCHNER C., LAUDE A., TABUTEAU D. (dir.), *Rapport sur le droit des malades*, Presses de L'EHESP, 2009.

L

LALONDE L., BERNATCHEZ S. (dir.), *La norme juridique « reformatée » - Perspectives québécoises des notions de force normative et de sources revisitées*, Les Éditions Revue de Droit Université de Sherbrooke, 2016.

LAUDE A., MATHIEU B., TABUTEAU D., *Droit de la santé*, 3ème éd., coll. Thémis, sous coll. Droit, PUF, 2012.

LECA A. (dir.), *Le secret médical*, Les cahiers de droit de la santé du Sud-Est n°15, LEH, 2012.

LEPAGE A., MATSOPOULOU H., *Droit pénal spécial*, coll. Thémis, PUF, 2015.

LUCAS A., DEVEZE J., FRAYSSINET J., *Droit de l'informatique et de l'Internet*, coll. Thémis Droit privé, PUF, 2001.

M

MARTIAL-BRAZ N. (dir.), *La proposition de règlement européen relatif aux données à caractère personnel : propositions du réseau Trans Europe Experts*, coll. Trans Europe Experts, Société de législation comparée, 2014.

MATTEI J.-F., ETIENNE J.-C., CHABOT J.-M., *De la médecine à la santé, pour une réforme des études médicales et la création d'universités de la santé*, Flammarion, 1997.

MESTRE J. (dir.), *Le droit face à l'exigence contemporaine de sécurité*, PUAM, 2000.

MORELLE A., TABUTEAU D., *La santé publique,* coll. Que sais-je ?, PUF, 2017.

N

NICOD M. (dir.), *Qu'en est-il de la sécurité des personnes et des biens*, Actes du colloque des 19 et 20 octobre 2006, coll. Travaux de l'IRF n° 7, Presses de l'Université Toulouse 1 Capitole, L.G.D.J - Lextenso Editions, 2008.

O

OST F., VAN DE KERCHOVE M., *De la pyramide au réseau ? – pour une théorie dialectique du droit*, coll. Droit, FUSL, 2002.

P

PEDROT P. (dir.), *Dictionnaire de droit de la santé et de la biomédecine,* Ellipses, 2006.

PRADEL J., VARINARD A., *Les grands arrêts du droit pénal général*, 9ème éd., coll. Grands arrêts, Dalloz, 2016.

Q

QUEMENER M., CHARPENEL Y., *Cybercriminalité – Droit pénal appliqué*, coll. Pratique du droit, Economica, 2010.

S

SAINT-PAU J.-C. (dir.), *Traité de droit de la personnalité*, coll. Traités, LexisNexis, 2013.

T

THIBIERGE C.,

- (dir.), *La force normative – Naissance d'un concept*, L.G.D.J - Bruylant, 2009.
- *et alii*, *La densification normative – Découverte d'un processus*, Mare&Martin, 2013.

TÜRK P., VALLAR C., *La souveraineté numérique – Le concept, les enjeux,* coll. Droit public, Mare & Martin, 2018.

V

VERDIER J., *Essai sur la jurisprudence de la médecine en France*, *ou Abregé historique et juridique des établissemens*, *réglemens*, *police*, *devoirs*, *fonctions*, *récompenses*, *honneurs*, *droits*, *& privilèges des trois corps de médecine ; avec les devoirs*, *fonctions & autorité des juges à leur égard*, Malassis le jeune - Prault père, 1763.

Etudes à la mémoire du professeur XAVIER LINANT de Bellefond – Droit et technique, Litec, 2007

§ 3 - Articles, interventions, encyclopédies

A - Articles extra-juridiques

A

ABOUT I., « Identifier les étrangers dans la France de l'entre-deux-guerres », *in* NOIRIEL G., *L'identification*, *Genèse d'un travail d'Etat*, Belin, 2007, p. 152.

B

BABOU I., « Des discours d'accompagnement aux langages : les nouveaux médias », *Études de linguistique appliquée*, n°114, 1998, p. 407-420.

BAQUE M.-H., BIEWENER C., « L'empowerment, un nouveau vocabulaire pour parler de participation ? », *Idées économiques et sociales* 2013/3, n°173.

BARREAU C., « Le marché unique numérique et la régulation des données personnelles », *in L'Union numérique européenne*, Série Réalités industrielles 2016/3, *Annales des Mines*, p. 37-41.

BERTHIER T., KEMPF O., « Vers une géopolitique de la donnée », *in L'Union numérique européenne*, série Réalités industrielles, 2016/3, *Annales des Mines*, p. 13-18.

BERTHOD-WURMSER M., BOUSQUET F., LEGAL R, « Patients et usagers du système de santé : l'émergence progressive de voix qui commencent à compter », *Revue française des affaires sociales* 2017/1, p. 5.

BEVIERE-BOYER B., « Bioéthique : la creation du health data hub national peut-elle contribuer à renforcer la protection des donnees sensibles de sante ? », avril 2019, disponible sur : <https://managersante.com/2019/04/15/les-potentialites-demultipliees-des-donnees-sensibles-de-sante-necessitant-une-protection-renforcee/>).

BRETON Ph., « Que faut-il entendre par discours d'accompagnement des nouvelles technologies ? », *Les dossiers de l'audiovisuel*, 2002, n°3.

BLOCKCHAIN PARTNER, Etude *Blockchain et Santé*, p. 9, disponible sur <https://blockchainpartner.fr/wp-content/uploads/2017/06/Sant%C3%A9-Industrie-Pharmaceutique-Blockchain.pdf>, dernière consultation le 12 octobre 2019.

BOSSI J., « Technologies de l'information et de la communication et données de santé : pour un cadre juridique en phase avec les évolutions technologiques et les besoins du système de santé », *Statistique et société*, mai 2014, vol. 2, n° 2, p. 37.

BOURQUARD K., « Norme numérique et e-Santé », *in Normaliser le numérique*, série Enjeux numériques, 5 mars 2019, *Annales des Mines*, p. 68.

BURGUN A., JANNOT A.-S., RANCE B., MAMZER M.-F, « Partage des données patients pour la recherche : aspects organisationnels et éthiques », *Ethics*, *Médecine and Public Health* 2016, n° 2, p. 435.

BUTERIN V., « Privacy on the blockchain », 15 janv. 2016, <https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/>, dernière consultation le 12 octobre 2019.

C

CASTETS-RENARD C., « Traitement algorithmique des activités humaines : le sempiternel face-à-face homme/machine », *Cahiers Droit Sciences & Technologies* 2016, n°6, Regards croisés sur les objets et les pratiques scientifiques et techniques, p. 239-255.

COHEN J.-E., « Turning Privacy Inside Out », *Theoretical Inquiries in Law*, 2018, vol. 20.1, p. 22.

COTTE D., « Système, information, média, Le SI comme objet des Sciences de l'information et de la communication », *Communication & languages* 2009/2, n° 160, p. 39.

D

DELEUZE G., « Post-scriptum sur les sociétés de contrôle » *in* DELEUZE G., *Pourparlers 1972-1990*, Éditions de Minuit, 1990, p. 244.

DE POURVILLE G.,

- « L'économie de la santé : périmètre et question de recherche », *in* Bras P.-L., DE POURVILLE G., TABUTEAU D., *Traité d'économie et de gestion de la santé*, Ed. Presses de Sciences Po – Editions de santé, 2009, p. 22.
- « La crise d'identité des médecins face au nouveau management de l'hôpital », *Le journal de l'école de Paris du management* 2010/6, n° 86, p. 22.

DUCATILLON J., « Le serment d'Hippocrate, problèmes et interprétations », *Bulletin de l'association Guillaume Budé*, 2001, p. 34-61.

E

ERTZSCHEID O., « L'homme est un document comme les autres : du World Wide Web au World Life Web », *Revue Hermès*, 2009, p. 33.

G

GUERIN S., « Les aidants, cœur du système social », *Revue Projet* 2012/1 (n° 326), p. 47.

GUIBET-LAFAYE C., RAPIN A.-J., « La "radicalisation", Individualisation et dépolitisation d'une notion », *Politiques de communication* 2017/1, n°8, p. 127-154.

H

HOFFSAES C., « Le système gamin : Erreur technocratique ou premier pas vers un fichage généralisé ? », *Esprit*, Mai 1982, n°65, p. 22-42.

J

JEANNERET Y.,

- « Autre chose qu'un discours, davantage qu'un accompagnement, mieux qu'une résistance », *Revue Terminal*, 2001, n°85.
- « "Nouvelles technologies de l'information" : une expression mal formée » *In Y-a-t-il (vraiment) des technologies de l'information ?* Nouvelle édition revue et corrigée [en ligne], Presses universitaires du Septentrion, 2011 (dernière consultation le 08 oct. 2019).

K

KING G., « Big Data Is Not About The Data ! », *in* MICHAEL ALVAREZ R., *Computional Social Science: Discovery and Prediction*, Cambridge University Press, 2016, p. VII.

L

LAVAL Ch., « Surveiller et prévenir. La nouvelle société panoptique », *Revue du MAUSS* 2012/2, n° 40, p. 47.

LAVILLE J.-L., « Politique de l'informatique et intérêt général », *in Variations autour de l'idéologie de l'intérêt général*, CURAPP, vol. 1, 1978.

LECLERCQ-VANDELANOITTE A., ISSAC H., « Technologies de l'information, contrôle et panoptique : Pour une approche deleuzienne », *Système d'information et management* 2013/2, vol. 18, n° 18.

LE DEUF O., « Utopies documentaires : de l'indexation des connaissances à l'indexation des existences », *Communication & Organisation*, 2015, n°48, p. 93.

LESSIG L., « Privacy as property », *Social Research : An International Quarterly*, 69(1), 2002, p. 247.

M

MERLIN X., WEILL M., Quel avenir numérique pour l'Europe ? », Série Réalités industrielles 2018/1, *Annales des* Mines, p. 42-45.

MEUNIER D., LAMBOTTE F., CHOUKAH S., « Du bricolage au rhizome : comment rendre compte de l'hétérogénéité de la pratique de recherche scientifique en sciences sociales ? », *Questions de communication*, 2013, n°23, p. 345-366.

MOLES A., « La fonction des mythes dynamiques dans la construction de l'imaginaire social », *Cahiers de l'imaginaire*, 1990, n°5/6, p. 9-33.

MUCCHIELLI A., « introdution », *Les sciences de l'information et de la communication*, 4e éd., coll. Les Fondamentaux ; sous-coll. Sciences Humaines, Hachette Supérieur, 2006.

MUMFORD L., « Technique autoritaire et technique démocratique », *in* MUMFORD L. *Technology and Culture*, John Hopkins University Press, 1963.

MUSSO P., « Usages et imaginaires des TIC », *in* LICOPEE C. (ss. la dir.), *L'évolution des cultures numériques. De la mutation du lien social à l'organisation du travail*, coll. innovation, éditions Fyp, 2009, Pp. 201-210.

P

PEUGEOT V., « Données de santé : contours d'une controverse », *L'Économie politique* 2018/4, n° 80, p. 40.

PEYRAT O., LEGENDRE J.-F., « Quel est l'apport d'une norme volontaire dans le domaine du numérique ? Pourquoi les acteurs s'y intéressent-ils ? », *in Normaliser le numérique ?* série Enjeux numériques, *Annales des Mines*, 5 mars 2019, p. 9.

R

RONAI M., « L'État comme machine informationnelle », *in Les données publiques*, *RFDP*, octobre-décembre 1994, n° 72, p. 571.

S

SCARDIGLI V., « Nouvelles technologies : l'imaginaire du progrès », *in* GRAS A., POIROT-DELPECH S. (dir.), *L'imaginaire des techniques de pointe. Au doigt et à l'œil*, L'Harmattan, 1989, Pp. 31-34.

SERRIS L., TOUTAIN L., « Introduction », *in Normaliser le numérique ?*, série Enjeux Numériques, mars 2019, *Annales des Mines*, n° 5.

SHANNON C., « A Mathematical Theory of Communication », *Bell System Technical Journal*, 1948, vol. 27.

SWEENEY L., « k-anonymity : a model for protecting privacy », *Int. J. Uncertain. Fuzziness Knowl. - Based Syst.*, vol. 10, n° 5, oct. 2002, p. 557.

T

TEAGUE V., CULNANE C., RUBINSTEIN B., « Research reveals de-identified patient data can be re-identified », Université de Melbourne (disponible en ligne sur <https://phys.org/news/2017-12-reveals-de-identified-patient-re-identified.html>, dernière consultation le 12 octobre 2019).

W

WORLD ECONOMIC FORUM, « *Unlocking the Value of Personal Data : From Collection to Usage* », 2013.

B - Articles juridiques

A

ABRAVANEL-JOLLY S., « Le secret médical en assurance de personnes », *RGDA* 2005, n°4, p. 887.

ALT-MAES F.,

- « Une évolution vers l'abstraction : de nouvelles applications de la détention », *RTD civ.* 1987, p. 21.
- « Les deux faces de l'information médicale : vers un nouvel équilibre des relations médecin-malade après la loi du 4 mars 2002 », *Gaz. Pal.*, 14-16 décembre 2003, p. 3.
- « Un exemple de dépénalisation : la liberté de conscience accordée aux personnes tenues au secret professionnel », *RSC* 1998, p. 301.

AMBROISE-CASTEROT C., « Consommation d'assurances et choix des textes applicables : code de la consommation ou code des assurances ? », *RSC* 2018, p. 95.

AMSELEK P.,

- « Normes et loi », *Arch. ph. droit* 1980.
- « L'évolution générale de la technique juridique dans les sociétés occidentales », *RDP* 1982, p. 287.
- « Le droit, technique de direction publique des conduites humaines, *Droits* 1989, n° 10, p.7.

ANCEL M., « Les principes de la Révolution française et le droit répressif moderne », *in La République française*, 1948, p. 79.

ANCEL P., « La protection des données personnelles. Aspects de droit privé français », *RIDC* 1987, n°3, p. 614.

ANCIAUX A., FARCHY J., « Données personnelles et droit de propriété : quatre chantiers et un enterrement », *Rev. int. dr. écon.* 2015, n°29-3, p. 307.

ANDRE C., « La cohérence de la notion de produit », *RRJ* 2003, n°2, p. 751.

APOLLIS B., « L'accès aux soins et la loi du 26 janvier 2016 », *RDSS* 2016, p. 673.

AUGAGNEUR L.- M., « Le management juridique de la cybersécurité en matière d'« e-santé », *RLDI*, janvier 2017, n° 133.

AZEMA J., « Modernisation et adaptation du droit des brevets en Europe », *RTD com.* 2000, p. 79.

B

BADINTER R., « Le droit au respect de la vie privée », *JCP* 1968, I, p. 2136.

BAHR A., BULACH C., FABER S., « Comment appliquer la loi Informatique et Libertés à la recherche médicale ? », *RGDM* 2012, n°45, Pp. 47-70.

BEATRIX O., « Open data et secteur de l'énergie : le début de l'histoire », *RFDA* 2018, p.49.

BEAUD O., LIBCHABER R., « Où va l'Université ? Les chemins de la liberté », *JCP G*, 2014, I 1264, n° 7, p. 2227.

BEAUSSONIE G.,

- *Jcl. comm.*, Fasc. 3403 : « Secret des correspondances », 2014 (mise à jour le 1er août 2017).
- « La dématérialisation de l'abus de confiance », *AJ pénal*, 2017, p. 215.
- « À propos d'une controverse contemporaine et persistante : le vol d'informations », *Revue de droit d'Assas* 2018, n°17, p. 99.

BENEAT A.-L., BALLET P., « Dématérialisation des données de santé : quels référentiels ? », *Gaz. Pal.*, 2011, n°351, p. 22.

BENEJAT M., « Les droits sur l'identité – Les droits sur les données personnelles », *in* SAINT-PAU J.-C. (dir.), *Traité de droit de la personnalité*, LexisNexis, coll. Traités, 2013, n°958.

BENEJAT-GUERLIN M., « Que reste-t-il de la protection pénale du secret médical ? », *AJ pénal* 2017, p. 368.

BENEZECH D., « La norme : une convention structurant les interrelations technologiques et industrielles », *Revue d'économie industrielle* 1996, n° 75, p. 27.

BENGHOZI P.-J., « Blockchain - Blockchain : objet à réguler ou outil pour réguler ? », *JCP E*, sept. 2017, n° 36, 1470.

BENICHOU D., « Dossier, Cybercriminalité, Jouer d'un nouvel espace sans frontière », *AJ pénal*, 2005, p. 224.

BENILLOUCHE M., « Les incertitudes juridiques entourant la contamination volontaire par le VIH », *AJ pénal* 2012, p. 388.

BENSAMOUN A.,

- « Création et données : différence de notions = différence de régime ? », *Dalloz IP/IT* 2018, p. 85.
- « Des robots et du droit... », *Dalloz IP/IT* 2016, p. 281.
- « Intelligence artificielle et santé : l'intégration en droit de l'IA médicale », *Journal de droit de la santé et de l'assurance maladie* (*JDSAM*) 2017, n° 17, Pp. 30-33.
- « La personne robot », *D.* 2017, p. 2044
- « Stratégie européenne sur l'intelligence artificielle : toujours à la mode éthique... », *D*. 2018, p. 1022.

BENSAMOUN A., LOISEAU G., « L'intégration de l'intelligence artificielle dans certains droits spéciaux », *Dalloz IP/IT* 2017, p. 295.

- « La gestion des risques de l'intelligence artificielle. De l'éthique à la responsabilité », *JCP G* 2017, doctr. 1203.
- « L'intelligence artificielle à la mode éthique », *D*. 2017, p. 1371.
- « L'intelligence artificielle : faut-il légiférer ? », *D*. 2017, p. 581.

BENSAMOUN A., ZOLYNSKI C.,

- « Big data et privacy : comment concilier nouveaux modèles d'affaires et droits des utilisateurs ? », *LPA*, 18 août 2014, p. 8.
- « Cloud computing et big data. Quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux* 2015/1, n° 189, p. 103-121.

BERGOIGNAN-ESPER C.,

- « Fasc. 14 : Secret Médical – Particularités en établissements publics de santé », *Feuillets mobiles Litec Droit médical et hospitalier*, 17 janv. 2012 (dernière modif. Le 3 mars 2016).
- « La confidentialité des informations de santé peut-elle tenir face à la protection d'autres intérêts légitimes ? », *D*. 2008, p. 1918.
- « L'hôpital public au sein du plan « Ma santé 2022 » », *RDSS* 2019, p. 15.

BERLIOZ P., « Consécration du vol de données informatiques. Peut-on encore douter de la propriété de l'information ? », *RDC* 2015, n°04, p. 951.

BERTIER-LESTRADE B., « Acte électronique et métamorphoses en droit des contrats », *in* NICOD M., *Métamorphoses de l'acte juridique*, coll. Travaux de l'IFR, Presses de l'Université Toulouse 1 Capitole, LGDJ, 2011, p. 50.

BEVIERE-BOYER B.,

- « Médecine personnalisée : de la délimitation entre le soin et la recherche », *in* HERVE C. et STANTON-JEAN M. (dir.), *Les nouveaux paradigmes de la médecine personnalisée ou médecine de précision*, coll. Thèmes & Commentaires, Dalloz, 2014.
- « Le proche du patient, un statut complexe, des améliorations possibles », *RDS* 2011, n° 41, p. 230.

BICHOT P., « Le secret médical : un outil redoutable à la disposition des assurés de mauvaise foi », *RLDC*, janvier 2005, n° 12.

BLOUD-REY C., « Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? », *D*. 2013, p. 2795.

BOISSON DE CHAZOURNES L., « Standards, régulation internationale et organisations », *in* FRYDMAN B., VAN WAEYENBERGE A. (dir.), *Gouverner par les standards et les indicateurs : De Hume aux rankings*, coll. Penser le droit, Bruylant, 2014, p. 73 et svt.

BONFILS P., GALLARDO E., « Secret des correspondances », *Rep. pén*., 2009.

BORDE J.-M., VAUCELLE A., HUDRISIER H., « La normalisation : dynamique opaque ou bonne gouvernance », *Pensée plurielle* 2014, n° 36, p. 9.

BORGES R.-M., LASSALAS C., « Personnalisation des soins et risques liés aux données de santé », *in* CASTAING C. (dir.), *Technologies médicales innovantes et protection des droits fondamentaux des patients*, Mare & Martin, coll. Droit public, 2018.

BORGETTO M., « La stratégie nationale de santé », *RDSS* 2018, p. 387.

BORGETTO M., BERGOIGNAN-ESPER C., « La loi "Hôpital, patients, santé et territoires" », *RDSS* 2009, p. 789.

BOSSAN J., « La dématérialisation de la procédure pénale », *D*. 2012, p. 627.

BOSSI J., « Comment organiser aujourd'hui en France la protection des données de santé », *RDSS* 2010, p. 208.

BOSSI-MALAFOSSE J.,

- « Les nouvelles règles d'accès aux bases médico-administratives : quel effet sur l'ouverture des données ? », *I2D Information*, *données & documents* 2016, Vol. 53, n°3, p. 84.
- « Le règlement européen et la protection des données de santé », *Dalloz IP/IT* 2017, p. 260.

BOTTHEGI D., LALLET A., « Les vicissitudes du fichage », *AJDA* 2010, p. 1930.

BOULOC B.,

- « Les limites du secret bancaire », *in Mélanges AEDBF*, Revue Banque Edition, 1997, p. 71.
- « Le secret professionnel de l'avocat », *in Mélanges offerts à Raymond Gassin*, PUAM, 2007 p. 121.

BOURCIER D., « Le bien commun ou le nouvel intérêt général », *in Mélanges en l'honneur du professeur CHEVALLIER J. - Penser la science administrative dans la post-modernité*, LGDJ, 2013, p. 92.

BOURCIER D., DE FILIPPI P., « L'Open Data : universalité du principe et diversité des expériences ? », *JCP A*, 2013, n°38.

- « Vers un droit collectif sur les données de santé », *RDSS* 2018, p. 444-456.
- « Transparence des algorithmes face à l'open data : quel statut pour les données d'apprentissage ? », *RFAP* 2018/3, n° 167, p. 525.

BOURDAIRE-MIGNOT C., « Téléconsultation : quelles exigences ? Quelles pratiques ? », *RDSS* 2011, p. 100.

BOURGEOIS M., MOINE M., « La nouvelle loi informatique et libertés. Une transposition du RGPD ? », *JCP E* 2018, n°30, p. 1417.

BOY L.,

- « Réflexions sur "le droit de la régulation" », *D*. 2001, p. 303.

- « Liens entre la norme technique et la norme juridique en droit communautaire et international », *in* BROSSET E., TRUILHE-MARENGO E. (dir.), *Les enjeux de la normalisation technique internationale*. *Entre environnement*, *santé et commerce international*, La documentation française, 2006, p. 337.
- « Normes techniques et normes juridiques », *in La normativité, Cahiers du Conseil* Constitutionnel, Janvier 2007, n°21.

BRAIBANT G.,

- « Droit d'accès et droit à l'information », *in Service public et libertés*. *Mélanges offerts au professeur Robert-Edouard Charlier*, Éd. de l'Université et de l'enseignement moderne, 1981, p. 703.
- « Données personnelles et société de l'informations », *La Documentation française*, 1998, p. 77.

BREDIN J.-D., « Secret, transparence et démocratie », *Pouvoirs*, 2001, n°97, p. 5.

BREEN E., « La "compliance" une privatisation de la régulation ? », *RSC* 2019, p. 327.

BROCAS A.- M., « La convention médicale de 1993 », *Droit social* 1994, p. 422.

BROSSET E., « Brèves observations sur un secret de Polichinelle : l'influence du droit européen sur le droit médical à travers l'exemple du secret médical », *in* LECA E. (dir.), *Le secret médical*, LEH, 2012, p. 51-66.

BRUGUIERE J.-M., MALLET-POUJOL N., VIVANT M., « Droit de l'informatique », *JCP E*, 2002, n°23, p. 888.

BRUNAUX G., « Cloud computing, protection des données : et si la solution résidait dans le droit des contrats spéciaux ? », *D*. 2013. p. 1158.

BUCKI E., CASANOVAS G., LANGARD S., « Les règles d'échange et de partage d'informations : aux limites de la démarche empirique », *RDS*, n° 79, 2017, p. 658-663.

BUI-XIAN O., « Les secrets de l'administration », *RDP* 2012, p. 1119.

BYK C., « Chapitre 4. La jurisprudence française relative à la contamination des produits sanguins : une clarification de la perception juridique du sang humain », *Journal International de bioéthique*, n°2, vol. 12, 2001, p. 49-58.

C

CADIET L., « Les conditions de diffusion des décisions de justice représentent un enjeu essentiel de la mise en œuvre du projet de leur mise à disposition du public », *JCP G* 2018, n°7, p. 170.

CANIVET G., « Blockchain et régulation », *JCP E*, 7 Septembre 2017, n° 36, 1469.

CAPRIOLI E., CHARPENTIER B., CHAVANNE V., DE LABRIFFE J., O'KANE D., ROQUILLY C., TOUATI A., VIGUIER E., « Blockchain et smart contracts : enjeux technologiques, juridiques et business », *Cah. dr. entr.*, Mars 2017, n° 2, entretien 2.

CARBONNIER J., « Les phénomènes d'internormativité », *in* Essais *sur les lois*, Defrénois 1979, Pp. 253-270.

CARON C., « Brèves observations sur l'abus des droits de la personnalité », *Gaz*. *Pal*. 2007, p. 47.

CASEAU-ROCHE C., « La clause de confidentialité », *AJCA*, 2014, p. 119.

CASTAING C., « Psychiatrie et soins ambulatoires », *RDSS* 2016, p. 77.

CASTETS-RENARD C.,

- « La spécificité des communications en ligne », *in* BEIGNIER B., DE LAMY B., DREYER E. (dir.), *Traité de droit de la presse et des médias*, coll. Traités, LexisNexis, 2009, n°1898.
- « Marché unique numérique » : la Commission européenne présente les premières mesures en droit d'auteur », *D*. 2016, p. 388.
- « Santé connectée et politique française de l'open data », *in* BROSSET E., GAMBARDELLA S., NICOLAS G. (dir.), *La santé connectée et « son » droit : approches de droit européen et de droit français*, coll. Droit de la santé, PUAM, 2017, p. 191.
- « La protection des données personnelles dans les relations internes à l'Union européenne – La protection des données personnelles en matière civile et commerciale », *Rep. dr. eur.*, oct. 2018 (act. mai 2019), n°109.

CASTETS-RENARD C., NDIOR V., RASS-MASSON L., « Le marché unique numérique : quelles réalités matérielles et conceptuelles ? », *D.* 2019., p. 956.

CATALA P.,

- « Ebauche d'une théorie juridique de l'information », *D*. 1984, chron., p. 97.
- « La « propriété » de l'information », *Mélanges offerts à PIERRE RAYNAUD*, Dalloz-Sirey, 1985, p. 97.
- « Le formalisme et les nouvelles technologies », *Rép. Defrénois* 2000, n° 18, p. 897

CATALA P., DE LAMBERTERIE I., GAUTIER P.-Y., « L'introduction de la preuve électronique dans le code civil », *JCP G* 1999, n° 47, doctr. 182

CAUCHY M., DIONISI-PEYRUSSE A., « Le droit au secret médical et son application en matière d'assurances », *D*. 2005, p. 1313.

CAVERS D.-F., « Law and Sciences : Some Points of Confrontation »*, in* JONES H.-W. (dir.), *Law and the social role of science*, The Rockefeller Universtity Press, 1966, p. 6.

CAVOUKIAN A., *Privacy by Design : The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, 2009, disponible sur : <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> (dernière consultation le 9 juillet 2019).

CEDILLE G., « Le signalement par le psychologue est-il compatible avec le respect du secret professionnel ? », *AJ pénal* 2011, p. 579.

CERVEAU B, « Assurance et secret médical : un cadre juridique précis, une jurisprudence bien établie », *Gaz. Pal.* 2010, n° 43-44, p. 15.

CHAPEAU P.-Y., MIJUSKOVIC V., « Le recul des libertés en psychiatrie sous couvert de prévention de la radicalisation », *RDS* 2018, n° 85, p. 832.

CHASSANG G., « E-santé, droit de l'union européenne et protection de la vie privée des personnes : vers l'émergence d'un « technodroit » spécifique au travers de la proposition de règlement général sur la protection des données personnelles ? », *RLDI*, 1er octobre 2014, n° 108.

CHAVANNE A., « Les atteintes à l'intimité de la vie privée au sens de l'article 368 du Code pénal », *in Actes du 8e Congrès de l'Association de droit pénal*, Economica, 1985, p. 24.

CHENEDE F., « Le contrat d'adhésion de l'article 1110 du Code civil », *JCP G* 2016, n° 27, p. 1334.

CHERON A., « La réutilisation des données publiques : bases de données et open data », *AJCT* 2011, p. 391.

CHEVALLIER J.,

- « Ficher, c'est encore administrer », in EDDAZI F., MAUCLAIR S. (dir.), *Le fichier*, LGDJ, coll. Grands colloques, 2017, p. 204.
- « L'État régulateur », *RFAP* 2004, n°111, p. 473-482.
- « Les agences : effet de mode ou révolution administrative ? », *in Etudes en l'honneur de GEORGES DUPUIS*, LGDJ, 1997, p. 47
- « Les fichiers administratifs instruments de l'action publique », *in* EDDAZI F., MAUCLAIR S. (dir.), *Le fichier*, Actes du colloque organisé les 26 et 27 novembre 2015 par le Centre de recherche juridique Pothier de l'Université d'Orléans, LGDJ coll. Grands Colloques, 2017, p. 125.
- « Juriste engagé(e) ? », *in* CHAMPEIL-DESPLATS V., FERRE N. (dir.), *Frontière du droit, critique des droits*, Coll. Droit et Société, LGDJ, 2007, Pp. 305-310.
- « Vers un droit post-moderne ? Les transformations de la régulation juridique », *RDP* 1998, p. 659-714.
- « Réflexions sur l'idéologie de l'intérêt général », *in Variations autour de l'idéologie de l'intérêt général*, coll. CURAP, PUF, 1978, vol. 1, p. 11.

CHILSTEIN D., « Les biens à valeur vénale négative », *RTD civ*., 2006, p. 663.

CHOPIN F., « Cybercriminalité », *Rep*. *Pén*. 2013, n°3.

CLEMENT E., « Concours et cumul des infractions contre les biens », *AJ pénal*, 2017, p. 219.

CLEMENT G., « Le secret de la preuve pénale », *in Mélanges dédiés à BERNARD BOULOC*, *Les droits et le droit*, Dalloz, 2007, p. 183.

CLUZEL-METAYER L.,

- « Les téléservices publics face au droit à la confidentialité des données », *RFAP* 2013/2, n° 146, p. 405-418.
- « Les limites de l'open data », *AJDA* 2016, p. 102.
- « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », *AJDA* 2017, p. 340.

CLUZEL-METAYER L., DEBAETS E., « Le droit de la protection des données personnelles : la loi du 18 juin 2018 », *RFDA* 2018, p. 1101.

COHEN-HADRIA Y., « *Blockchain* : révolution ou évolution ? », *Dalloz IP/IT* 2016, p. 537.

COLLIARD C.-A., « La machine et le droit privé français contemporain », *in Le droit privé français au milieu du XX*e *siècle. Études offertes à GEORGES RIPERT*, t. 1, LGDJ, 1950, p. 115.

CONTE P.-H.,

- « "Effectivité", "inefficacité", "sous-effectivité", "surefficacité"…variations pour un droit pénal », *in Etudes offertes à PIERRE CATALA – Le droit privé français à la fin du XX*ème *siècle*, Litec, 2001, p. 125.
- « Algorithme idéologique », *Dr*. *pén*., novembre 2017, repère 10.

CONROY F., CYTERMAN L., « L'encadrement du "big data" et la protection des droits fondamentaux », *Revues des Juristes de Sciences Po*, n° 10, mars 2015, p. 118.

CONTIS M., « La télémédecine : nouveaux enjeux, nouvelles perspectives juridiques », *RDSS* 2010, p. 235.

CORGAS-BERNARD C., « Responsabilité civile médicale et nouvelles pratiques numériques : l'exemple de la télémédecine », *LPA* 2014, n°164, p. 27.

COTTET M., « Le secret de la personne protégé par le médecin : le secret médical », *LPA* 2016, n°226-227, p. 36.

COUTURIER M., « Que reste-t-il du secret médical ? », in *Mélanges en l'honneur de Gérard Mémeteau*. *Droit médical et éthique médicale : regards contemporains*, coll. Mélanges, LEH, 2015, p. 351.

CNIL, communiqué, 24 sept. 2018, *JCP E* 2018, act. 738

CREDEVILLE A.-E., « Le secret médical et la preuve judiciaire ou le secret médical mis en perspective », *D*. 2009, p. 2645.

CRISTOL D.,

- « Le droit à la protection de la santé face aux exigences de maîtrise des dépenses de santé », *in Mélanges en l'honneur de JEAN-HENRI SOUTOUL*, LEH, 2000, p. 103.
- « L'usager dans la stratégie nationale de santé : la démocratie en santé en quête d'un nouveau souffle », *RDSS* 2018, p. 413

CROZE H., « L'apport du droit pénal à la théorie générale du droit de l'informatique », *JCP G* 1988, I, n°7, p. 3333.

CULIOLI M., « Le recel commis par le passager connaissant la provenance du véhicule utilisé », *RSC* 1973, p. 81.

D

DARAGON E., « Etude sur le statut juridique de l'information », *D*. 1998, chron. n°3, p. 63.

DANET J., « La dangerosité, une notion criminologique, séculaire et mutante », *Champ pénal* Vol. V, 2008.

DANIS-FATOME A., « Biens publics et choses communes ou biens communs ? Environnement et domanialité », *in Mélanges en l'honneur d'ETIENNE FATOME*, Dalloz, 2011, p. 99.

DAUBIGNEY M.-C., « La marche vers la dématérialisation de la procédure pénale », *AJ Pénal* 2007, p. 460.

DAURY-FAUVEAU M., *Jcl Pénal Code*, Fasc. 20 : « Recel », 2012 (mise à jour 2018).

DAVER C., « La télémédecine entre progrès techniques et responsabilités », *D*. 2000, p. 527.

DEBET A.,

- « Intelligence artificielle et données à caractère personnel », *in* Bensamoun A., Loiseau G. (dir.), *Droit de l'intelligence artificielle*, coll. Les intégrales, Vol. 15, LGDJ, 2019.
- « L'exclusion des hommes homosexuels du don de sang examinée sous l'angle de la protection des données », *Com*. *comm*. *électr*., 2015, n°1.
- « Le responsable de traitement est tenu d'une obligation de résultat s'agissant de l'exactitude des données », *Com*. *comm*. *électr*., 2016, n°5.
- « À la veille de l'entrée en vigueur du RGPD, la CNIL publie son rapport annuel 2017 », *JCP G* 2018, n° 19-20, 537, p. 916.

DEBIES E., « L'incertitude de l'anonymisation face à l'ouverture des données de santé », *in* BOURCIER D., DE FILIPPI P., (dir.), *Open data et Big data*. *Nouveaux défis pour la vie privée*, coll. Droit & Science politique, 2016, p. 86.

DECOCQ A., *«* Rapport sur le secret de la vie privé en droit français », *in* Association CAPITANT H. (dir.), *Le Secret et le Droit*, Dalloz, 1974.

DECOOPMAN N., « A propos des autorités administratives indépendantes et de la déréglementation », *in* CLAM J., MARTIN G. (dir.), *Les transformations de la régulation juridique*, coll. Droit et Société, Recherches et Travaux du RED&S à la maison des Sciences de l'Homme, n°5, LGDJ, 1998, p. 252.

DE FALLOIS M., « Assurance et ''droit à l'oubli'' en matière de santé », *RDSS* 2017, p. 132.

DEFFAINS B., « Le défi de l'analyse économique du droit : le point de vue de l'économiste », *LPA* 2005, n° 99, p. 6.

DE GROVE-VALDEYRON N., « Politique de santé de l'Union européenne et transformation numérique des soins : quels enjeux pour quelle compétence ? », *Rev. UE* 2019, p. 39.

DELAGE P.-J., « La dangerosité comme éclipse de l'imputabilité et de la dignité », *RSC* 2007, p. 797.

DE LAMBERTERIE I.,

- « Qu'est-ce qu'une donnée de santé ? », *RGDM* 2004, n°4, Pp. 11-26.
- « L'adaptation du droit au progrès technologique : l'exemple de la protection des logiciels », *Arch. phil. dr.*, t. 36, 1991, Pp. 155 et svt.

DE LAUDABERE A., « Relations entre l'administration et le public », *AJDA* 1978, p. 495.

DELMAS-MARTY M.,

- « A propos du secret professionnel », *D*. 1982, chron. p. 267.
- « Face au terrorisme global, la distinction entre guerre et paix a-t-elle encore un sens ? », *Constitutions* 2018, n° 3, p. 353.
- « Le droit au silence en procédure pénale », *in Mélanges en l'honneur de Jacques Teneur*, Université du droit et de la santé de Lille, 1977, p. 273.

DELPECH X., « Vers un droit civil des robots », *AJ contrat* 2017, p.148.

DEL REY M.-J., « L'ISO 26000, une démarche « développement durable » à portée des collectivités », *AJCT* 2012, p. 370.

DELTORN J.-M., « La protection des données personnelles face aux algorithmes prédictifs », *RDLF* 2017, chron. n° 12, p. 7.

DE MAISON ROUGE O., « Décryptage sur la protection juridique des informations sensibles », *Dalloz IP/IT* 2017, p. 273.

DE MAISON ROUGE O., « La donnée, enjeu cardinal de la cybersécurité », *Dalloz IP/IT* 2018, p. 170.

DENIZOT A., « Droit de la santé : les avalanches de l'hiver 2017 », *RTD civ*. 2017, p. 500.

DE POURVILLE G., « L'économie de la santé : périmètre et questions de recherche » *in* BRAS P.-L., DE POURVILLE G., TABUTEAU D. (dir.), *Traité d'économie et de gestion de la santé*, Presses de Sciences Po – Éditions de santé, 2009.

DEROUDILLE A., « Le secret professionnel dans le règlement général à la protection des données », *RFDA* 2018, p. 1112.

DEROULEZ J., « Blockchain et données personnelles. Quelle protection de la vie privée ? », *JCP G*, 18 sept. 2017, n° 38, 973, spéc. n° 9.

DESGENS-PASANAU G., « Le Conseil d'État censure la CNIL sur la question des contrôles sur place et des fichiers d'exclusion », *Dalloz IP/IT* 2016, p. 615.

DE SOTO J., « La responsabilité pénale et la Révolution française », *in La responsabilité pénale*, Travaux du colloque de philosophie pénale (12 au 21 janvier 1959) présentés par LEAUTE J., travaux de l'Institut de Sciences Criminelles et pénitentiaires, *Annales de la faculté de droit et des sciences politiques et économiques de Strasbourg*, t. VIII, Dalloz 1961, p. 137.

DETRAZ S., « Vol du contenu informationnel de fichiers informatiques », *Rev. pén*. 2008, p. 880.

DEULEUZE G., « Post-scriptum sur les sociétés de contrôle », *in Pourparlers 1972-1990*, Editions de Minuit, 1990.

DEUMIER P., « Le principe "appliquer ou expliquer", appliquer la norme autrement ? », *RTD civ*. 2013, p. 79.

DEVEZE J., « Les vols de « biens informatiques », *JCP* 1985, I., n°20, p. 3210.

DIBOUT P., « La liberté d'accès aux documents administratifs », *Rev. adm*. 1979, p. 23.

DIEU F.,

- « Divulguer le secret médical au médecin-conseil d'une compagnie d'assurance est une faute pour un hôpital », *AJDA* 2007, p. 1089.
- « Hospitalisation sous contrainte et encadrement thérapeutique de l'information délivrée au malade », *RDSS* 2009, p. 688.

DOBKINE M., « L'ordre repressif administratif », *D*. 1993, p. 157.

DONDERO B., « Justice prédictive : la fin de l'aléa judiciaire ? », *D*. 2017, p. 532.

DOUVILLE T.,

- « Blockchain et protection des données à caractère personnel », *AJ contrat* 2019, p. 316.
- « Cybersécurité : transposition de la directive NIS, ses limites et ses conséquences », *JCP E*, n° 15-16, 12 Avril 2018, act. 284.
- « L'émergence d'un droit commun de la cybersécurité », *D*. 2017, p. 2255.
- « Le règlement européen sur la cybersécurité », *JCP E*, 20 juin 2019, n° 25, act. 408.

DREIFUSS-NETTER F., « Feue la responsabilité civile contractuelle du médecin ? », *RCA* 2002, chron. 17, p. 6.

DREYER E., « Droit de la presse et droits de la personnalité », *D*. 2012, p. 765.

DREYER E., « Consécration –provisoire- du vol de données informatiques », *AJ pén*. 2015, p. 413.

DUBOUIS L.,

- « Convention nationale. Dossier de suivi médical », *RDSS* 1994, p. 433.
- « Feu le secret médical ? », *in Mélanges en l'honneur du Professeur Gustave Peiser*, coll. Droit public, Presses Universitaire de Grenoble, 1995, p. 201.
- « La directive n° 2011/24/UE relative à l'application des droits des patients en matière de soins de santé transfrontaliers », *RDSS* 2011, p. 1068, n° 6
- « La sixième convention nationale médicale : la mise en chantier de la maîtrise médicalisée des dépenses médicales », *RDSS* 1994, p. 40.
- « Secret médical et liberté de la presse », *RDSS* 2004, p. 841.

DUBREUIL C.-A., « La démocratie et la transparence », *RFDA* 2016, n°655.

DUCLERCQ J.-B.,

- « Big data - Les effets de la multiplication des algorithmes informatiques sur l'ordonnancement juridique », *CCC*, novembre 2015, étude 20.
- « Les algorithmes en procès », *RFDA* 2018, p.131.

DUFOUR J.-B., « Le dossier pharmaceutique : du DP patient au DP rupture, un formidable outil de santé publique créé par les pharmaciens », *RGDM* 2018, n°67, p. 19-28.

DUPONT B., « L'évolution du piratage informatique : de la curiosité technique au crime par sous-traitance », in Association sur l'Accès et la Protection de l'Information (dir.), *Le respons@ble 2.0 : Acteur clé en AIPRP*, Cowansville : Yvon Blais, 2010, p. 63-81.

DUPONT M., « Dossier médical. – Dossier en établissement de santé. Dossier dématérialisé », *Feuill. Mob. Litec Droit médical et hospitalier* 2016, Fasc. 9-30.

DUPRES DE BOULOIS X., « Existe-t-il un droit fondamental à la sécurité ? », *RDLF* 2018, chron. n° 13.

DURAN P., « Piloter l'action publique avec ou sans le droit ? », *Politique et management public* 1993, n°4, Pp. 1-45.

DUTOIT M., « Entre injonction et impératif de coopération, les nouveaux modes d'organisation des personnes " usagers " », *in* JAEGER M. (dir.), *Usagers ou citoyens ? De l'usage des catégories en action sociale et médico-sociale*, Dunod, 2011, p. 162.

DUVAL-ARNOULD D., « Le juge civil face au secret médical », *D.* 2004, p. 2682.

E

EDDAZI F., « Prolégomènes », *in* EDDAZI F., MAUCLAIR S. (dir.) *Le fichier*, Actes du colloque organisé les 26 et 27 novembre 2015 par le Centre de recherche juridique Pothier de l'Université d'Orléans, coll. Grands Colloques, LGDJ, 2017, p. 3.

EISENMANN Ch., « Quelques problèmes de méthodologie des définitions et des classifications en science juridique », *Arch. ph. dr.*, n° 11, 1966, Pp. 25-43.

EON F.,

- « Hôpital public et données personnelles des patients », *RDSS* 2015, p. 85.
- « Objets connectés : comment protéger les données de santé ? », *RLDI* 2016, nº 125.
- « La donnée au cœur de l'e-santé », *Expertises des systèmes d'information*, 2016, n°419, p. 405.
- « L'accélération du numérique en santé : enjeux et conditions de son succès », *RDSS* 2019, p. 55.

EVEN B., « La notion de document administratif », *AJDA* 1985, p. 521.

EVIN C, « Les nouveaux outils d'une politique territoriale de santé : un mille-feuille qui a besoin d'une mise en cohérence », *RDSS* 2017, p. 107.

EYMARD O., « Questions de cryptologie », *Délibérée*, *Revue de réflexion critique animée par le Syndicat de la magistrature* 2018/1, n° 3, p. 60.

F

FAUVARQUE-COSSON B., MAXWELL W., « Protection des données personnelles », *D.* 2018, p. 1033.

FAVRO K., « La CNIL, une autorité à "l'âge de la maturité" », *Dalloz IP/IT* 2018, p. 464.

FAVRO K., « La démarche de compliance ou la mise en œuvre d'une approche inversée », *Légicom* 2017, n°59, Pp. 21-28.

FEREY S., *Une histoire de l'analyse économique du droit*, Bruylant, 2008.

FEUILLET B., « L'accès aux soins, entre promesse et réalité », *RDSS* 2008, p. 713.

FEUILLET- LE MINTIER B., « Les fondements du secret médical », *Revue juridique de* l'Ouest 2000, *in Les médecins libéraux face au secret médical*, Pp. 1-9.

FIESHI M., « Vers un dossier médical personnel », *Dr. soc.* 2005, p. 80.

FOEGEL J.-P., « *Le Conseil d'Etat*, *héraut de la révolution numérique ? Protection des données personnelles (Conseil d'Etat)* », *La revue des droits de l'Homme*, *Actualité Droits-Libertés*, décembre 2014.

FOMBEUR P., « Un décret d'application ne peut renvoyer à un arrêté ultérieur la mise en œuvre des principes de la loi », *AJDA* 2000, p. 831.

FOREST D.,

- « 3 questions Le "Big data" », *JCP E* 2014, n° 8, 138.
- « 3 questions Open data et données publiques », *JCP E*, 28 juillet 2016, n° 30-34, 638.
- « 3 questions La gouvernementalité algorithmique », *JCP E*, 24 novembre 2016, n° 47, 932.

FORGERON J., « Les application de télémédecine : des responsabilités médicales traditionnelles aux responsabilités techniques *nouvelles* », *Gaz. Pal*. 2001, n°289, p. 20.

FORGERON J., SEGUINOT F., « Le dossier médical personnel : l'activité d'hébergeur de données de santé (2ème partie) », *Gaz. Pal*. 2006, n°26, p. 10.

FOUCAULT M., « Le sujet et le pouvoir », *in* FOUCAULT M., *Dits et écrits*, t. II, Gallimard, coll. Quarto, 1982, p. 1041-1062.

FOUGERE L., « Les secrets de l'administration », *Bull*. II AP, 1967, p. 21.

FRANCILLON J., « Infractions relevant du droit de l'information et de la communication », *RSC* 1996, n°3, p. 676.

FRAYSSINET J., PEDROT P., « La loi du 1er juillet 1994 relative au traitement des données nominatives ayant pour fin la recherche dans le domaine de la santé », *JCP G* 1994, n° 51, doctr. 3810.

FRAYSSINET J.,

- « Contre l'excessive distinction entre fichier et dossier, le pas en avant du Tribunal de grande instance de Paris », *Cah. dr. entr.* 1989, p. 3.
- « Données nominatives et recherche biomédicale », *Médecine et Droit*, septembre-octobre 1995, n° 8, p. 111.
- « Un concurrent associé du secret professionnel : le droit de la confidentialité du traitement des données personnelles », *Revue juridique de l'ouest* 2000, p. 23-46.
- « La confidentialité sur l'Internet : du secret professionnel à la protection des données personnelles », *Gaz. Pal*. 2002, n°85, p. 17.
- « La régulation du respect de la loi informatique, fichiers et libertés par le droit pénal : une épée en bois », *Légicom* 2009, n°42, p. 23.

FRICERO N., « Collecte, diffusion et exploitation des décisions de justice : quelles limites, quels contrôles ? À propos du rapport sur l'open data des décisions de justice », *JCP G* 2018, n°7, p. 168.

FRISON-ROCHE M.-A.,

- « Compliance et personnalité », *D.* 2019, p. 604.
- « L'immatériel à travers la virtualité », *in* TERRE F. (dir.), *Le droit et l'immatériel*, coll. Archives de philosophie du droit, Sirey, t. 43, 1999, p. 139-148.
- « Critère des intérêts et secret professionnel », *in Les entretiens du Palais*, *Gaz. Pal*., 18 février 2005, p. 78-81.
- « Repenser le monde à partir de la notion de données », *in* FRISON-ROCHE M.-A, (dir.), *Internet*, *espace d'interrégulation*, coll. Thèmes & commentaires, Dalloz, 2016, p. 9.
- « La rhétorique juridique », *in Argumentation et rhétorique (II)*, *Hermès, La Revue*, 1995, n° 16, p. 80.
- « Les droits des personnes, Internet et la CNIL », *Dalloz - Etudiants*, 2016.

- « Gouvernance d'internet : "Nous sommes face à un enjeu de civilisation" », *LPA*, 18 juillet 2019.
- « Un droit substantiel de la compliance, appuyé sur la tradition européenne humaniste », *Pour une Europe de la compliance*, coll. Thèmes et commentaires, Dalloz, 2019, p. 13.

FRYDMAN B.,

- « Comment penser le droit global ? » *in* CHEROT J.-Y., FRYDMAN B., *La science du droit dans la globalisation*, Bruylant, 2012, p. 20.
- « Le droit comme savoir et comme instrument d'action dans la philosophie pragmatique », *Revue de la recherche juridique* 2017-5, n° 31, coll. Cahier de méthodologie juridique, p. 1805.
- « Les métamorphoses d'Antigone », *Droit & Philosophie* 2016, n° 8, Pp. 111-167.
- « Prendre les standards et les indicateurs au sérieux », *in* FRYDMAN B., VAN WAEYENBERGE A. (dir.), *Gouverner par les standards et les indicateurs : De Hume au rankings*, coll. Penser le droit, Bruylant, 2014, p. 14.

G

GAGNEUX M., « Systèmes d'information et efficience du système de santé » *in* BRAS P.- L., DE POURVILLE G., TABUTEAU D. (dir.), *Traité d'économie et de gestion de la santé*, Presses de Sciences Po – Éditions de santé, 2009.

GALATRYROLIN E., *Jcl*. *Communication*, Fasc. 1000 : « Agence nationale de la sécurité des systèmes d'information (ANSSI) », février 2018.

GALLOUX J.-C., « Ebauche d'une définition juridique de l'information », *D*. 1994, chron. n°10, p. 230.

GASSIN R.,

- « Le droit pénal de l'informatique », *D*. 1986, Chron. 35.
- « La protection pénale d'une nouvelle "universalité de fait" en droit français : les systèmes de traitement automatisé de données », *ALD* 1989, 2ème cahier, p. 5.
- « Commentaire du jugement de Tribunal correctionnel de Paris, du 2 mars 1989 ou de la distinction des fichiers nominatifs et des dossiers individuels », *Cah*. *Jurispr*. Paris, 1989, p. 9.

GAUDEMET A., « Qu'est-ce que la compliance », *Commentaires* 2019/1, n° 165, p. 109.

GAUDEMET Y., « L'administration au grand jour : France », *in Journées de la Société de législation comparée*, 1983, p. 39 et s.

GAUTIER P.-Y.

- « Du contrat de dépôt dématérialisé : l'exemple du cloud computing », *in La communication numérique*, éd. Panthéon-Assas, 2012, p. 157.
- « Le bouleversement du droit de la preuve : vers un mode alternatif de conclusion des conventions », *LPA*, 5 mai 2000, n° 90.
- « Le dépôt : exercice de qualification » *RDC* 2014, n°1, p. 149.
- « L'équivalence entre supports électronique et papier, au regard du contrat », *in Droit et technique. Etudes à la mémoire du Professeur XAVIER LINANT de Bellefonds*, LexisNexis, 2007, p. 195.

GAUTRAIS V., « Différences culturelles en matière de vie privée : point de vue canadien », *Dalloz IP/IT* 2016, p. 128.

GAUTRON V., « Usages et mésusages des fichiers de police : la sécurité contre la sûreté ? », *AJ pénal*, 2010, p. 266.

GEA F. « FRANÇOIS OST, "*À quoi sert le droit ? Usages, fonctions, finalités*", coll. Penser le droit, 2016, Bruylant », *Rev. trav.* 2016, p. 649.

GEFFRAY E., « Quelle protection des données personnelles dans l'univers de la robotique ? », *Dalloz IP/IT* 2016, p. 295.

GENDREAU A., « La dématérialisation du dépôt : l'exemple du contrat de cloud computing », *AJ contrat* 2016, p. 519.

GHICA-LEMARCHAND C.,

- « Une certaine idée du secret bancaire », *in Mélanges offerts à ANDRE DECOCQ*, *Une certaine idée du droit*, Litec, 2004, p. 279.
- « La responsabilité pénale de la violation du secret professionnel », *RDSS* 2015 p. 419.

GIARD V., « La normalisation technique », *Revue française de gestion* 2003/6, n° 147, p. 49.

GIUDICELLI-DELAGE G., « Droit à la protection de la santé et droit pénal en France », *RSC* 1996, p. 13.

GIRER M., « Droits des patients et exercice en société », *RDSS* 2014, p. 434.

GODEFROY L., « Le code algorithmique au service du droit », *D*. 2018, p. 734.

GOLA R., « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *Légicom* 2017/2 n° 59, Pp. 29-38.

GRANET F., « Les fichiers sanitaires automatisés », *D*. 1995, p. 10.

GRASSER M., MANAOUIL C., VERRIER A., JARDE O., « L'équipe médicale à l'hôpital », *RGDM* 2004, n° 14, p. 13.

GRAZ J.-C., « Quand les normes font loi : Topologie intégrée et processus différenciés de la normalisation internationale », *Études internationales* 2004, n° 2, vol. 35, Pp. 233-260.

GREMION P.et JAMOUS H., « Les systèmes d'information dans l'administration publique », *Revue française de science politique* 1974, n° 2, p. 214.

GRIGUER M., « Le point sur le nouveau régime des traitements de données personnelles », *Cahiers de droit de l'entreprise*, juillet 2018, n° 4, prat. 20.

GROUTEL H., « Preuve de la déclaration inexacte du risque et secret médical », *Resp. civ. et assur.* 2004, Étude n° 18.

GRYNBAUM L.,

- « La responsabilité des acteurs de la télémédecine », *RDSS* 2011, p. 996.
- « La preuve littérale et la signature à l'heure de la communication électronique », *Comm. et Com. életr.* 1999-2, p. 9.
- « loi économie numérique : le sacre des égalités formelles », *Rev. des contrats* 2005/2, p. 580.

GROSCLAUDE J., « L'obligation de discrétion professionnelle », *Rev. adm*. 1967, Pp. 127 et svt.

GUEDJ A., « Liberté et responsabilité en droit européen et international », *in* BEIGNIER B., DE LAMY B., DREYER E. (dir.), *Traité de droit de la presse et des médias*, coll. Traités, LexisNexis, 2009, n°218.

GUERRIER C., « La CNI biométrique française : entre préservation de l'identité et protection des libertés individuelles », *RLDI* 2012, n°82, p. 2758.

GULPHE P., « Le secret professionnel en droit français », *in Le secret et le droit*, Travaux de l'association HENRI CAPITANT, t. XXV, Dalloz, 1974, p. 110-111.

GUTMANN D., « Du matériel à l'immatériel dans le domaine des biens », in TERRE F. (dir.), *Le droit et l'immatériel*, coll. Archives de philosophie du droit, Sirey, t. 43, 1999, p. 65-78.

GUYON C., « Le concept d'archives : d'une définition à l'autre », *HAL - archives ouvertes* 2016, p. 1.

H

HAAS G., DUBARRY A., « Confidentialité et protection des données », *Dalloz IP/IT* 2017, p. 322.

HAAS G., DUBARRY A., D'AUVERGNE M., RUIMY R., « Enjeux et réalités juridiques des Objets Connectés », *Dalloz IP/IT* 2016 p. 394.

HABOUZIT, F., « L'usage de la notion de radicalisation dans le champ pénitentiaire (suite) : Existe-t-il un statut *sui generis* des personnes « radicalisées » ? », *RSC* 2018, p. 541.

HALPERIN J.-L., « L'essor de la "privacy" et l'usage des concepts juridiques », *Droit et Société* 2005, n°61, p 765 s., *spéc*. p. 778.

HARDY J., « Les catégories juridiques à l'épreuve de la réforme administrative », *AJDA* 2017, p. 919.

HARICHAUX M., « L'obligation du médecin de respecter les données de la science, À propos du cinquantenaire de l'arrêt Mercier : bilan d'une jurisprudence », *JCP G* 1987, I, p. 3306.

HARICHAUX M., « La télétransmission des feuilles de soins », *RDSS* 1998, p. 496.

HAUSER J., « Les géniteurs anonymes : des donneurs de gamètes et des parturientes inconnues », *RTD civ*. 2012, p. 520.

HENRY A., « Un suicide qui dérange : le suicide en prison », *AJ pénal* 2010, p. 437.

HERMITTE M.-A., « La fondation juridique d'une société des sciences et des techniques par les crises et les risques », *in Pour un droit commun de l'environnement, Mélanges en l'honneur de MICHEL PRIEUR*, Dalloz, 2007, p. 145 et svt.

HERVEG J., VAN GYSEGHEM J.-M., « Titre 16 - L'impact du Règlement général sur la protection des données dans le secteur de la santé » *in* DE TERWANGNE C., ROSIER K. (dir.), *Le règlement général sur la protection des données* (RGPD/GDPR), Larcier, 2018, p. 703.

HERZOG-EVANS M., « Isolement carcéral : un arrêt du Conseil d'État révolutionnant les sources du droit pénitentiaire », *D*. 2009, p. 134.

HIELLE O., « La technologie *blockchain* : une révolution aux nombreux problèmes juridiques », *Dalloz act.*, 31 mai 2016.

HILDEBRANDT M., « A vision of ambiant law », *in* BROWNSWORD R., K. YEUNG (dir.), *Regulating Technologies*, *Legal Futures, Regulatory Frames and Technological Fixes*, Hart Publishing, 2008, Pp. 175 et svt.

HOERNI B., « Principes et pratiques d'un secret : le secret médical », *in* FRISON-ROCHE M.-A. (dir.), *Secrets professionnels*, éd. Autrement, 1999, p. 177.

HOLLEAUX A., « Les lois de la troisième génération des droits de l'homme : ébauche d'étude comparative », *Rev. franç. adm. publ.* 1980, n°15, p. 45.

HOUSSIN D., « Le secret médical dans les nouvelles pratiques et les nouveaux champs de la médecine », *D*. 2009, p. 2619.

I

IDOUX P., « L'argument sociologique et les autorités administratives indépendantes », *in* FENOUILLET D. (dir.), *L'argument sociologique en droit. Pluriel et singularité*, coll. Thèmes, actes et commentaires, Dalloz, 2015, p. 137.

J

JAMIN C., « Services juridiques : la fin des professions ? », *Pouvoirs* 2012, vol. 1, n° 140, p. 33-47.

JAMIN C., XIFARAS M., « Sur la formation des juristes en France. Prolégomènes à une enquête », *Commentaires* 2015/2, n°150, Pp. 385-392.

JESTAZ P., « Rapport de synthèse » *in* REVET Th. (dir.), *L'inflation des avis*, coll. Etudes juridiques, Economica, 1998, p. 113.

JOMNI A., « Le RGPD : un atout ou un frein pour la cybersécurité ? », *Dalloz IP/IT* 2019, p. 352.

JONAS C., « Protéger ou trahir ? Réflexion d'un praticien sur les contradictions entre assistance à autrui et secret professionnel », *in Mélanges en l'honneur de JEAN-HENRI SOUTOUL*, LEH, 2000, p. 133.

JUTRAS D., JAMIN Ch., « À quoi servent les études de droit ? Correspondance outre-Atlantique », *JCP G*, 2014, 639, p. 1098.

JOURDAIN P., « Existe-t-il un droit subjectif à la sécurité ? », *in* NICOD M. (dir.), *Qu'en est-il de la sécurité des personnes et des biens ?* Presses de l'Université Toulouse 1 Capitole, coll. Travaux de l'IFR, LGDJ, 2008, p. 77-83.

JUNG H., « Introduction au droit médical allemand », *RSC* 1996, p. 41.

K

KAHN A., « Le secret médical : d'Hippocrate à internet », *D.* 2009, p. 2623.

KAMINA P., *Jcl. comm.*, Synt. 30 « Régulation de la communication », 2018.

KAYSER P., *Diffamation et atteinte au respect de la vie privée*, *in Etudes ALFRED JAUFFRET*, PUAM, 1974.

KAYSER P., « Les droits de la personnalité, aspects théoriques et pratiques », *RTD civ.* 1971, p. 445.

KENNEDY D., « Une alternative phénoménologique de gauche à la théorie de l'interprétation juridique HART / KELSEN », *Jurisprudence – Revue critique* 2010, p. 24.

KLEINER C., « Les droits de l'homme et le secret bancaire : opposition ou subsomption ? », *Journal du droit international (Clunet)*, n° 4, Octobre 2014, doctr. 15.

KRANZBERG M., «Technology and History: "Kranzberg's Laws" », *Technology and Culture* 1986, Vol. 27, n° 3, Pp. 544-560.

KRIEGEL B., « Chapitre 5. La responsabilité politique et pénale dans l'affaire du sang contaminé », *Journal international de bioéthique*, n°2, vol. 12, 2001, 59-71.

L

LABBE E., « L'efficacité technique comme critère juridique ou la manière dont les lois se technicisent », *Lex-Electonica* 2004, 9-2.

LACOUR S.,

- « Chapitre 3- Nouvelles technologies et patrimonialisation des données personnelles : un changement de paradigme », *in* VIOLET F. (dir.), *Personne et patrimoine en droit – Recherche sur les marqueurs d'une connexion*, Bruylant, 2015, p. 369.
- « Du secret médical aux dossiers de santé électroniques. Réflexions juridiques sur la protection des données de santé », *Médecine & Droit* 2016, n° 138, p.66.

LAFARGE P., « Secret professionnel, confidentialité et nouvelles technologies d'informations », *Gaz. Pal.* 1998, p. 481.

LAGREE J., « Éthique et partage du secret professionnel », *RDSS* 2015, p. 465.

LALLET A., « Documents administratifs : accès et réutilisation », *Rep. cont. admin.*, décembre 2014, act. Décembre 2017.

LAMBERT P., « Le respect du secret professionnel de l'avocat, composante du droit à un procès équitable », *in Mélanges en l'honneur de SERGE GUINCHARD*, *Justice et droit du procès : Du légalisme procédural à l'humanisme processuel*, Dalloz, 2006, p. 291.

LANDREAU I., « Mes Data sont à moi : pour une patrimonialité des données personnelles », *Rapport du think-tank Génération Libre*, 2018 (https://www.generationlibre.eu/data-a-moi).

LANNA M., « L'homme surveillé : les objets connectés », in CASTAING C. (dir.), *Technologies médicales innovantes et protection des droits fondamentaux des patients*, coll. Droit public, Mare & Martin, 2018, Pp. 84-87.

LARGUIER J., « Le secret de l'instruction et l'art. 11 du Code de procédure pénale », *RSC* 1959, p. 313.

LARIVET S., « L'intelligence économique : un concept managérial », *Market Management* 2006/3, vol. 6, p. 23.

LARONZE F., « La norme ISO 26000, une source de droit en matière sociale ? L'apport de la théorie du droit à la réflexion sur les normes de la RSO », *Dr. soc.* 2013. p. 345.

LASSERRE B.,

- « La Commission d'accès aux documents administratifs », *Et. et doc.*, CE, 19811982, p. 33 et svt.
- « Six ans après le vote de la loi du 17 juillet 1978 : une administration plus transparente ? », *Et. et doc.*, CE, 1983, n°35, p. 99 et svt.

LASSERRE V., « Loi et Règlement », *Rép. civ.*, 2015 (act. janvier 2016), n°218.

LASSERRE CAPDEVILLE J.,

- « Les développements récents du droit sanctionnant le vol », *AJ pénal* 2017, p. 208.
- « La détection du délit d'abus de faiblesse par le banquier », *AJ pénal* 2018, p. 223.

LASMOLES O., « La difficile appréhension des blockchains par le droit », *RIDE* 2018/4 (t. XXXII), p. 453.

LAVEISSIERE J.,

- « En marge de la transparence administrative : le statut juridique du secret », *in Etudes offertes à JEAN-MARIE AUBY*, Dalloz 1992, p. 181
- « La communication administration-administrés », *in* COLAS D. (dir.), *L'État et les corporatisme*s, coll. Droit et sciences politiques, PUF, 1988.
- « Le droit à l'information à l'épreuve du contentieux. A propos de l'accès aux documents administratifs », *D.* 1987, p. 275.
- « Le pouvoir, ses archives et ses secrets », *D.* 1984, chron. p. 63.
- « Le statut des archives en France », *Rev. adm.* 1980, n°195, p. 256.

LAZERGES C.,

- « Le déclin du droit pénal : l'émergence d'une politique criminelle de l'ennemi », *RSC* 2016, p. 649.
- « Le choix de la fuite en avant au nom de la dangerosité : les lois 1, 2, 3, 4, 5, etc. sur la prévention et la répression de la récidive », *RSC* 2012, p. 274.

LECAS A., CAREGHI J.-C., « Le secret médical, au crible d'une analyse historique » *in* LECAS A. (dir.), *Le secret médical*, Les cahiers de droit de la santé du Sud-Est, n°15, LEH, 2012, p. 15.

LECLERC H., « La justice et le secret », *in Mélanges en l'honneur de Robert Badinter*, *L'exigence de justice*, Dalloz, 2016, p. 545.

LECLERC O., « Sur la validité des clauses de confidentialité en droit du travail », *Dr. soc*. 2005, p. 173.

LECLERCQ P., « Evolutions législatives sur les signatures électroniques », *RD informatique et télécoms* 1998-3, p. 19 et svt.

LECOURT A., « RGPD : nouvelles contraintes, nouvelles stratégies pour les entreprises », *Dalloz IP/IT* 2019, p. 205.

LEFEBVRE-DUTILLEUL V., « Le conformité, droit vivant », *in* ROQUILLY C., *La contribution des juristes et du droit à la performance de l'entreprise. Management juridique et culture juridique de l'entreprise*, coll. Pratique des affaires, Joly éd. - Lextenso Editions, 2011.

LE GAL C., « Le dossier pharmaceutique : un outil technique de santé publique », *RDSS* 2009, p. 301.

LEGEAIS D.,

- « Blockchain et actifs numériques : le droit français va-t-il devenir réellement attractif ? », *RDBF* Mars 2019, n° 2, repère 2.
- « Blockchain et données personnelles : réponse de la CNIL », *JCP E*, 11 octobre 2018, n° 41, act. 754
- « L'apport de la Blockchain au droit bancaire », *RDBF*, Janvier 2017, n° 1, dossier 5.
- « Le droit d'auteur face aux nouvelles technologies », *RIDC* 1990, n° 42-2, Pp. 677-692.
- « L'utilisation de la blockchain pour les titres de sociétés non cotées », *Droit des sociétés* Février 2019, n° 2, étude 2.
- « Quel avenir pour la blockchain ? », *RDBF* Mars 2018, n° 2, repère 2.

LE GOFFIC C., « Consentement et confidentialité à l'épreuve de la télémédecine », *RDSS* 2011, p. 987.

LEMAIRE S., « Interrogations sur la portée juridique du préambule du règlement Rome I », *D.*, 2018, p. 2157.

LEMASURIER J., « Vers une démocratie administrative : du refus d'informer au droit d'être informé », *RDP* 1980, p. 1239 et svt.

LEPAGE A.,

- « Droits de la personnalité – De certains droits de la personnalité en particulier », *Rép. civ*. 2000 (act. : juillet 2019), n°119.
- « Droit pénal et internet : la part de la tradition, l'œuvre de l'innovation », *AJ pénal* 2005, p. 217.
- « Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *Com. comm. électr*. 2005, n°2, étude 9.

- « Le secret, figure polymorphe du droit pénal », *in Mélanges en l'honneur du Professeur MICHEL GERMAIN*, LexisNexis-LGDJ, 2015, p. 481.
- « Personnalité (Droits de la) », *Rép. civ.*, septembre 2009 (act. : novembre 2017).
- « Un an de droit pénal du numérique », *Dr. pén*. 2017, n°12, chron. 11.
- « Droit à l'oubli : une jurisprudence tâtonnante », *D*. 2001, p. 2079.
- « Droit pénal et conscience », *Dr. pén*. 1999, chron. 1.

LEQUILLERIER C., « L'impact de l'intelligence artificielle sur la relation de soin », *Journal de droit de la santé et de l'assurance maladie* (*JDSAM*) 2017, n° 17, p. 14-20.

LESAULNIER F., « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p. 573.

LESSIG L., « Code Is Law. On Liberty in Cyberspace », *Harvard Magazine*, 1 janv. 2000, disponible sur < https://www.harvardmagazine.com/2000/01/code-is-law-html > (dernière consultation le 27 août 2019)

LEVASSEUR G., « La protection pénale de la vie privée », *in Études offertes à PIERRE KAYSER*, t. 2, PUAM, 1979, p. 107.

LEVENEUR L., « Le fait », *Arch. phil. dr.*, t. 35, *Vocabulaire fondamental du droit*, 1991, p. 143.

LEWKOWICZ G., VAN WAEYENBERGE A., « L'École de Bruxelles : origines, méthodes et chantiers », *in La méthodologie et l'épistémologie juridiques*, Éditions Yvon Blais, 2016, p. 363-372.

LIBCHABER R.,

- « L'autorité des recommandations de la Commission des clauses abusives », *RTD civ*. 1997, p. 791.
- « La recodification du droit des biens », *in Le code civil 1804-2004. Le livre du bicentenaire*, Dalloz-Litec, 2004, p. 348.
- « Biens », *Rép. civ*. 2016.

LINDON R., « La presse et la vie privée », *JCP G* 1965, I, p. 1887.

LINOTTE D., « Chronique des réformes administratives françaises », *RDP* 1978, p. 1417.

LOISEAU G.,

- « De la protection intégrée de la vie privée (*privacy by design*) à l'intégration d'une culture de la vie privée », *Légipresse* 2012/300, p. 712.
- « Le contrat de don d'éléments et produits du corps humain. Un autre regard sur les contrats réels », *D*. 2014, p. 2252.
- « Responsabilité », *Journal de Droit de la Santé et de l'Assurance Maladie* (*JDSAM*) 2017, n° 17, p. 21-24.
- « Typologie des choses hors commerce », *RTD civ*. 2000, p. 47.
- *Rapport de synthèse in Actes du colloque annuel de la Semaine Juridique, Le secret à l'ère de la transparence, JCP G* 2012, suppl. au n° 47, p. 44 et svt.

LOKIEC P., « La décision médicale », *RTD civ*., 2004, p. 641.

LOTH A., « Systèmes d'information et cartes de santé », *Dr. soc.* 1996, p. 829.

LUCAS A., « La réception des nouvelles techniques dans la loi, l'exemple de la propriété intellectuelle », *Juriscom.net* 2001.

LUCAS DE LEYSSAC M.-P., « Une information seule est-elle susceptible de vol ou d'une autre atteinte juridique aux biens ? », *D*. 1985, Chron. 443.

LUCAS-PUGET A.-S., « L'opportunité des clauses de confidentialité aujourd'hui, et demain ? », *LPA* 2016, n°119, v.2, p. 50.

M

MAILLOLS-PERROY A.- C., « Les vigilances », *RDS* 2005, n° 3, p. 81.

MAISNIER-BOCHE L., « Intelligence artificielle et données de santé », Dossier *Intelligence artificielle et santé*, *Journal de Droit de la Santé et de l'Assurance Maladie (JDSAM)*, n° 17, 2017, p. 25.

MAISTRE DU CHAMBON P., « Recel », *Rep. pén*. 2009, n°2 à 13 (mise à jour juillet 2019).

MALAURIE P.,

- « La responsabilité civile médicale », *Defrénois* 2002, n°23, p. 1516.
- « Le secret et le droit. Une petite anthologie littéraire », *in mélanges CHRISTIAN MOULY*, Litec, 1998, p. 106.

MALLET-POUJOL N.,

- « Appropriation de l'information : l'éternelle chimère », *D*. 1997, p. 330.
- « Protection des données personnelles et droit à l'information », *Legicom*, n°59, 2017/2, p. 124.
- « La protection des données personnelles à l'épreuve de l'open data des décisions de justice : l'exemple des données des justiciables », *Revue pratique de la prospective et de l'innovation*, 2018, n°1, dossier 4.

MALAURIE-VIGNAL M., « Blockchain et propriété intellectuelle », *PI*, octobre 2018, n° 10, étude 20.

MANSON S., « La mise à disposition de leurs données publiques par les collectivités territoriales », *AJDA* 2016, p. 97.

MARTIAL-BRAZ N., « L'abus de textes peut-il nuire à l'efficacité du droit ? », *Dalloz IP/IT* 2018, p. 459.

MARTIN L., « Le secret de la vie privée », *RTD civ*. 1959, p. 227.

MASSON A., BOUTHINON-DUMAS H., « L'approche « Law & Management » », *RTD com.* 2011, p. 233.

MATHIEU B., « Les droits des personnes malades », *LPA*, 19 juin 2002, n° 122, p. 13.

MATSOPOULOU H.,

- *Jcl*. *Pénal Code*, Fasc. 20 : « Violation de domicile, Art. 226-4 », 15 septembre 2009 (mise à jour 9 septembre 2016).
- « Abus de confiance : détournement de clientèle », *Rev*. *sociétés* 2018, p. 56.

MATTATIA F., « La loi sur la protection de l'identité est-elle conforme à la Constitution ? », *LPA*, 2012, n°82, p. 6.

MAXWELL W., TAÏEB S., « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP/IT*, 2016, p. 123.

MAYAUD Y.,

- « Des mauvais traitements sur mineurs de quinze ans et de leurs retombées, en termes de secours et de dénonciation, sur les professionnels de la santé et de l'assistance », *RSC* 1998, p. 320.
- « Respect de la vie privée, secret professionnel, et droits de la défense », *RSC* 2007, p. 815.

- « Le secret du délibéré, un secret professionnel absolu », *RSC* 2016, p. 265.
- « La condamnation de l'évêque de Bayeux pour non-dénonciation, ou le tribut payé à César… », *D*. 2001, p. 3454.

MEDJKANE M., « Le partage des informations à caractère secret », *AJ pénal* 2017, p. 371.

MEKKI M.,

- « Blockchain, smart contracts et notariat : servir ou asservir ? », *JCP N*, 6 juillet 2018, n° 27, act. 599.
- « La blockchain : de la technologie à la technique juridique », Dossier, *Dalloz IP/IT* 2019, p. 414.
- « L'influence normative des groupes d'intérêt : force vive ou force subversive ? », *JCP G* 2009, p.47.
- « Le contrat, objet des smart contracts (Partie 1) », *Dalloz IP/IT* 2018, p. 409.
- « Le smart contract, objet du droit (Partie 2) », *Dalloz IP/IT* 2019, p. 27.
- « Le formalisme électronique : la "neutralité technique" n'emporte pas "neutralité axiologique" », *RDC* 2007/3, p. 681.
- « Les mystères de la blockchain », *D.* 2017, p. 2160.

MELLERAY F., « La justice administrative doit-elle craindre la « justice prédictive » ? », *AJDA* 2017, p. 193.

MENDOZA-CAMINADE A., « Big data et données de santé : quelles régulations juridiques ? », *RLDI* 2016, n° 127.

MENNELEC L., « Vers une relativisation du secret médical », *JCP* 1979, I, p. 2936.

Merland G., « L'intérêt général, instrument efficace de protection des droits fondamentaux ? », Cahiers du Conseil constitutionnel, juin 2004.

MESLI V., « Quelles articulations entre le dossier médical personnel et le dossier médical en santé au travail ? », *RDSS*, 2014, p. 266.

MIHAN A., « Vol », *Rep. Pén.* 2016 (mise à jour août 2017).

MISTRETTA P.,

- « La loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé. Réflexions critiques sur un droit en pleine mutation », *JCP G*, 2002, p. 1075.
- « La médecine énergétique traditionnelle chinoise et les piqûres du droit pénal médical », *RSC* 2015, p. 413.
- « Le secret des correspondances, Molière et les tartufferies médicales... », *RSC* 2018, p. 480.

MODERNE F.,

- « Rapport de synthèse », *in La maîtrise du sol*, *Travaux de l'association H. Capitant*, t. XLI, Economica, 1990, p. 36.
- « Conception et élaboration de la loi du 17 juillet 1978 », *in Transparence et secret*, La Documentation française, 2004, p. 19 et svt.

MOIROUX J., « Commande publique et technologie blockchain : un avenir, mais quel avenir ? », *JCP A* 2017, p. 2180.

MOLFESSIS N.,

- « Le renvoi d'un texte à un autre », *in* MOLFESSIS N. (dir.), *Les mots de la loi*, Economica, Paris, 1999, p. 55.

- « Les illusions de la codification à droit constant et la sécurité juridique », *RTD civ*. 2000, p. 186.
- « La sécurité juridique et la jurisprudence vue par elle-même », *RTD civ*. 2000, p. 666.
- « La sécurité juridique et la fonction normative de la loi », *RTD civ*. 2000, p. 670.
- « Les "avancées" de la sécurité juridique », *RTD civ*. 2000 p. 660.

MOREAU Y., DORNBIERER C., « Enjeux de la technologie des *blockchains* », *D.* 2016, p. 1856.

MORET-BAILLY J.,

- « Les rapports entre la loi et les déontologies des professions de santé après la loi du 4 mars 2002 », *RDSS* 2003, p. 581.
- « La déontologie médicale, de la résistance à la contre-offensive (à propos du décret du 7 mai 2012 portant modification du code de déontologie médicale) », *RDSS* 2012, p. 1074.

MORLET-HAIDARA L., « Le système national des données de santé et le nouveau régime d'accès aux données », *RDSS* 2018, p. 91.

MONNIER A., « Le Dossier Médical Personnel : histoire, encadrement juridique et perspectives », *RDSS* 2009, p. 625.

MORLET-HAÏDARA L., « Le nouveau cadre légal de l'équipe de soins et du partage des données du patient », *RDSS* 2016, p. 110.

MOUSSERON J.-M., « Valeurs, biens, droits », *in Mélanges en hommage à ANDRE BRETON et FERNAND DERRIDA*, Dalloz, 1991, p. 277.

N

NETTER E., « Blockchain et professions réglementées », *Cah. dr. entr.,* mai 2018, n° 3, dossier 21.

NICOLAS E., « Chapitre 10. De la norme aux flux normatifs », *in* LE GOFF J., ONNEE S. (dir.), *Puissance de la norme. Défis juridiques et managériaux des systèmes normatifs contemporains*, coll. Gestion en liberté, EMS Editions, 2017, p. 187.

O

OBERDORFF H., « Quelle intervention du droit ? » *in* CERCRID, *Le droit au contact de l'innovation technologique*, Université Jean Monnet-Saint Étienne, 1989, p. 13.

OCHAO N., « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA* 2015, p. 1157.

OHM P., « Broken promises of privacy : responding to the surprising failure of anonymization », *57 UCLA Law Review*, 2010, p.1704.

OLECH V., « Soins médicaux en milieu carcéral : confusion des rôles et partage des secrets », *RDS* 2015, n° 63, p. 96.

OPPETTIT B., « L'omnipotence technocratique et eurocratique », *in* OPPETTI B., *Droit et modernité*, PUF, 1998, p. 31 et s.

P

PADOVA Y., « Entre patrimonialité et injonction au partage : la donnée écartelée ? (Partie I) », *RLDI* 2019, nº 155.

PANFILI J.-M., « Dossier « Hospitalisation sans consentement » - Publicité des débats et secret médical : deux principes antagonistes à concilier » *AJ Famille* 2016, p. 27.

PANSIER F.-J., CHARBONNEAU C., « La dématérialisation des données médicales et les enjeux de leur hébergement », *Gaz. Pal.* 2002, n°321, p. 23.

PASSA J., « La propriété de l'information : un malentendu ? », *Dr. et patr.*, 2001, p. 64 et svt.

PATIN M., « La répression des délits de presse », *RSC* 1954, p. 449.

PECHILLON S., « L'adaptation du secret médical à l'hôpital : du silence à l'information médicale », *in* MOQUET-ANGER M.-L. (dir.), *De l'hôpital à l'établissement public de santé*, l'Harmattan, 1998, p. 317.

PECHILLON E., « La responsabilité administrative des établissements intervenant dans l'action sociale et médico-sociale : protection du secret et nécessité du partage d'informations », *RDSS* 2015, p. 440.

PEDROT P.,

- « Le dossier de suivi médical et le carnet médical », *RDSS* 1995, p. 610.
- « Carte d'assurance maladie. Carte électronique individuelle interrégime », *RDSS* 1998, p. 911.

PELTIER V.,

- *Jcl. Pénal Code*, Fasc. 20 : « Atteinte au secret des correspondances commises par des personnes dépositaires de l'autorité publique », 2019 (mise à jour 22 mai 2019).
- *Jcl. Pénal Code*, Fasc. 20 : « Révélation d'une information à caractère secret – Conditions d'existence de l'infraction. - Pénalités », 28 mai 2015 (mise à jour 9 septembre 2016).

PENNEAU A.,

- « Contrat électronique et protection du cybercontractant, Du Code de la consommation au Code civil », *LPA* 13 mai 2004, p. 3.
- « Rapport de droit français », *in La preuve des actes juridiques électroniques privés : mosaïque de droits européens ou trait d'union ? RLDI* 2009, supp. n°52.

PENNEAU A., VOINOT D., *Jcl Concurrence – Consommation*, : « Normalisation », octobre 2010.

PENNEAU J.,

- « Le secret médical et la preuve (ou l'introuvable solution) », in Mélanges dédiés à DOMINIQUE HOLLEAUX, Litec, 1990 p. 345.
- « De quelques incidences du secret médical sur l'expertise judiciaire », *AJ Pénal* 2009, p. 169.

PENNEAU M., « Saisie du dossier médical », *D.* 1996, p. 296.

PERNAZZA F., « Les lois techniciennes », *LPA*, 5 juillet. 2007, n° 134.

PERRAY R.,

- *Jcl Comm.*, Fasc. 930 : « Données à caractère personnel. – Introduction générale et champ d'application de la loi "Informatique et libertés" ».
- « Traitement de données personnelles dans le cadre de recherches médicales : vers un allégement des formalités », *PLDI* 2007, p. 64.

PERREAU E.-H., « Des droits de la personnalité », *RTD civ.* 1909, p. 501.

PIDOUX E., « La responsabilité médicale au regard de la télétransmission et de la télémédecine », *LPA* 2000, n°149, p. 5.

PIGNARRE G., « Le contrat de dépôt éclairé par le prisme de l'opération de qualification », *AJ contrat* 2016, p. 508.

PIN X., « La théorie du consentement de la victime en droit pénal allemand – Eléments pour une comparaison », *RSC* 2003, p. 259.

PLESSIX B., « L'interconnexion des fichiers entre administrations », *in* DEFFAINS N., PLESSIX B. (dir.), *Fichiers informatiques et sécurité publique*, coll. « droit, politique, société », PUF-EUL, 2013, Pp. 109-124.

PONTHOREAU M.-C., « La protection des personnes contre les abus de l'informatique », *RFDA* 1996, p. 796.

PORTES L., « Du secret médical », communication à l'Académie des Sciences Morales et Politiques, *in A la recherche d'une éthique médicale*, Masson-PUF, 1954.

POULLET Y.et ROUVROY A., « Le droit à l'autodétermination informationnelle et la valeur du le développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie » *in* K. BENYEKHELF et P. TRUDEL (dir.), *Etat de droit et virtualité*, Thémis, 2009, p. 157.

PRADEL J.,

- Les dispositions de la loi du 17 juillet 1970 sur la protection de la vie privée », *D*. 1971, p. 3.
- « L'incidence du secret médical sur le cours de la justice pénale », *JCP* 1969, p. 2234.

PUCHERAL Ph., ANCIAUX N., BEHAR-TOUCHAIS M., BENABOU V.-L., MARTIAL-BRAZ N., *et al*., « Directive Contenu numérique Données », *CCC* 2017, dossier 4, n° 5.

PUCHERAL Ph., RALLET A., ROCHELANDET F., ZOLYNSKI C., « La privacy by design : une fausse bonne solution aux problèmes de protection des données personnelles soulevés par l'open data et les objets connectés ? », *Légicom* 2016/1, n° 56, p. 89.

PY B.,

- « De la violation du secret professionnel : essai de légistique progressiste », *in* MALABAT V., DE LAMY B., GIACOPELLI M., coll. Thèmes et commentaires, Dalloz, 2009, p. 89
- « Secret professionnel », *Rép. pen*., fév. 2003 (mise à jour février 2017).
- « Secret professionnel : le syndrome des assignats ? », *AJ pénal* 2004, p.133.
- « Le secret professionnel : une obligation de se taire », *JA* 2008, n°386, p. 12.
- « Le secret professionnel : une obligation de parler », *JA* 2008, n°386, p. 15.
- « Réquisitoire contre l'expression de secret médical : plaidoyer pour l'expression de secret professionnel », *RDS* 2013, p. 161.
- « Signalement des infractions sexuelles commises en institution », *JA* 2015, p. 29.
- « Ficher les fous. Au sujet du traitement automatisé de données à caractère personnel dénommé "Redex" (répertoire des expertises) », *RDS* 2018, p. 611.
- « Secret professionnel : le syndrome des assignats ? », *AJ pénal* 2004, p. 133.
- « Quand la sûrêté nucléaire atomise un peu plus la notion de secret », *RDS* 2017, p. 396.

R

RADE C., « Nouvelles technologies de l'information et de la communication et nouvelles formes de subordination », *Dr. soc.* 2002, p.26.

RALLET A., ROCHELANDET F., ZOLYNSKI C., « De la *privacy by design* à la *Privacy by Using* », *Réseaux* 2015/1, n° 189, p. 15.

RAYNARD J., « Domaines et thèmes des avis », *in* REVET T. (dir.), *L'inflation des avis*, coll. Etudes juridiques, Economica, 1998, p. 11.

REBOUL-MAUPIN N., « Responsabilités des médecins et internet », *Gaz. Pal.*, 2002, n°85, p. 28.

REDON M., « Extorsion », *Rép. Pén.* 2016.

RENARD I., « Régulation de la *blockchain*, il est urgent d'attendre », *Expertise* juin 2016, p. 215.

RENAUDIE O., « Télémédecine et téléservice public », *RFAP* 2013/2, p. 262.

REPIQUET Y., « Le secret professionnel de l'avocat et la lutte contre le blanchiment d'argent » *in Mélanges offerts à ANDRE DECOCQ*, *Une certaine idée du droit*, Litec, 2004, p. 433.

RESTREPO AMARILES D.,

- « Conclusion », *in* FRYDMAN B., BRICTEUX C. (dir.), *Le droit global*, coll. Penser le droit, Bruylant, 2017, p. 253.
- « *The matematical turn* : l'indicateur Rule of Law dans la politique de développement de la Banque Mondiale », *in* B. FRYDMAN et A. VAN WAEYENBERGE (dir.), *Gouverner par les standards et les indicateurs : De Hume aux rankings*, coll. Penser le droit, Bruylant, 2014, p. 193.

RIAL-SEBBAG E., « Chapitre 4. La gouvernance des Big data utilisées en santé, un enjeu national et international », *Données de masse, gouvernance et droit*, *Journal international de bioéthique et d'éthique des sciences* 2017/3, vol. 28, p. 39.

RIGAUX F., « La protection de la vie privée et des autres biens de la personnalité », *in* TABATONI P. (dir.), *La protection de la vie privée dans la société de l'information*, t. 6, 7 et 8, coll. Cahier des sciences morales et politiques, PUF, 2002, n°647, p. 724.

RIOU C., FRESSON J., MADELON G. (*et alii*), « Information médicale et pilotage des établissements de santé », *Journal de gestion et d'économie médicale*s 2016/1, Vol. 34, p. 45.

RIVERO J., « À propos des métamorphoses de l'Administration d'aujourd'hui : démocratie et administration », *in Mélanfes offerts à RENE SAVATIER*, Dalloz, 1965, p. 821.

ROBACZEWSKI C., *Jcl. Pén.*, n°5, Fasc. 20 : « Atteinte aux systèmes de traitement automatisé de données ».

ROBERT J.-H., « Secrets professionnels », *JCP G*, n° 47 hors-série, 19 novembre 2012.

ROCHFELD J.,

- « La loi n° 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique », *RTD civ.* 2004, p. 574.
- « Le "contrat de fourniture de contenus numériques" : la reconnaissance de l'économie spécifique « contenus contre données », *Dalloz IP/IT*, 2017, p. 15.
- « Des données personnelles : Quels nouveaux droits ? », *Statistiques et Société*, 2017, Vol. 5, n°1, p. 49.
- « Accès (enjeux théoriques) », *in* CORNU M., ORSI F. et ROCHFELD J. (dir.) *Dictionnaires des biens communs*, coll. Quadridge, PUF, 2017.
- « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT* 2018, p. 474.

ROMAN D., « Le respect de la volonté du malade : une obligation limitée ? », *RDSS* 2005, p. 423.

ROQUET C., « Le secret médical à l'épreuve du contentieux social des relations collectives, *RDSS*, 2018, p. 658.

ROQUILLY C. (dir.), *Blockchain* et *smart contracts : enjeux technologiques, juridiques et business*, *Cah. dr. entr.,* 2017

ROUAST A., « Les droits discrétionnaires et les droits contrôlés », *RTD civ*. 1944, p. 1.

ROUVIERE F.,

- « La justice prédictive, version moderne de la boule de cristal », *RTD civ*. 2017, p. 527.
- « Le raisonnement par algorithmes : le fantasme du juge-robot », *RTD civ*. 2018, p. 530.

ROUVROY A., BERNS T., « Gouvernementalité algorithmique et perspectives d'émancipation », *Réseaux* 2013/1, n° 177, p. 163.

ROUX A., « La transparence administrative en France », *in Ann. eur. Actes du colloque pour le XXVe anniversaire de la loi du 17 juillet 1978 sur l'accès aux documents administratifs adm. publ.*, Ed. CNRS, 1989, p. 57.

S

SABLIERE P., « Une nouvelle source de droit ? Les "documents référents" », *AJDA* 2007, p. 66.

SADRAN P., « Le miroir sans tain. Réflexions sur la communication entre l'administration et les administrés », *in Religion, société et politique : mélanges en hommage à JACQUES ELLUL*, PUF, 1983, p. 802.

SAENKO L., « Abus de confiance, remise précaire et dématérialisation », *RTD com*. 2017, p. 447.

SAINT-PAU J.-C., « Le droit au respect de la vie privée - Définition conceptuelle du droit au respect de la vie privée », *in* SAINT-PAU J.-C., *Droits de la personnalité*, coll. Traités, LexisNexis, 2013.

SAISON J., « Service public hospitalier ou service public de santé ? À la recherche d'unité pour le système de santé... », *RDSS* 2017, p.634.

SALAIS R.,

- « Du bon (et du mauvais) emploi des indicateurs dans l'action publique », *Semaine sociale Lamy*, 2006, n°1272, p. 73.
- « La donnée n'est pas un donné. Pour une analyse critique de l'évaluation chiffrée de la performance », *RFAP*, 2010/3, p. 497-515.

SARCELET J.-D., « La confidentialité des informations de santé peut-elle tenir face à la protection d'autres intérêts légitimes ? », *D*. 2008, p. 1921.

SARGOS P., « Les principes d'immunité et de légitimité en matière de secret professionnel médical », *JCP G*, 8 décembre 2004, n° 50, doctr. 187.

SAUER F., « Europe et télésanté », *RDSS* 2011, p. 1029.

SAVATIER R., « Contribution à une étude juridique de la profession », *in Dix ans de conférences d'agrégation, Etudes de droit commercial offertes à Mélanges JOSEPH HAMEL*, Dalloz, 1961, p. 1.

SEGUR P., « La confidentialité des données médicales », *AJDA* 2004, p. 858.

SENECHAL J., « La fourniture de données personnelles par le client via Internet, un objet contractuel ? », *AJCA* 2015, p. 212.

SIMMONS & SIMMONS LLP, « Le droit et la technologie blockchain : une approche sectorielle », *CCC*, octobre. 2017, étude 10.

SONTAG-KOENIG S.,

- « La dématérialisation des procédures », *AJ pénal* 2014, p. 154.
- « L'accès de l'avocat aux procédures dématérialisées », *AJ pénal*, 2011, p. 455.

- « La signature électronique en procédure pénale : une évolution amorcée », *AJ pénal*, 2014, p. 123.

STEFANI F., « Le secret médical à l'épreuve des nouvelles technologies », *D*. 2009, p. 2636.

SUPIOT A., « Travail, droit et technique », *Dr. soc.* 2002, p. 13.

T

TABUTEAU D., « La sécurité sanitaire, réforme institutionnelle ou résurgence des politiques de santé publique ? », *Les tribunes de la santé*, 2007/3, p. 87.

TABUTEAU D., « Le secret médical et l'évolution du système de santé », *D*. 2009, p. 2629.

TAMBOU O., « L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ? », *RLDI*,1er avril 2016, n° 126.

TANGHE H., GIBERT O., « L'enjeu de l'anonymisation à l'heure du big data », *Revue française des affaires sociales 2017*, n°4, p. 79-93.

TCHEN V., « L'informatisation des documents d'identité numérisés », *Dr. adm.*, 2012, comm. 48.

TERRE F., « Présentation », *Arch. phil. dr.* 1991, *Droit et science*, p. 5.

THIBIERGE C.,

- « Au coeur de la norme : le tracé et la mesure. Pour une distinction entre normes et règles de droit », *Arch. phil. droit* 2008, p. 341.
- « Le concept de "force normative" », *in* THIBIERGE C.(dir.), *La force normative. Naissance d'un concept*, Mare&Martin, 2013, p. 813.
- « Les "normes sensorielles" », *RTD civ.* 2018, p. 567.

THOMAS J., « Le fichier et l'inclusion de l'individu au sein de la collectivité », *in* EDDAZI F., MAUCLAIR S. (dir.), *Le fichier*, coll. Grands colloques, LGDJ, 2017, p. 204.

THOMAS Y., « Le sujet de droit, la personne et la nature », *Le débat* mai-août 1998, n° 100, p. 104.

THONNET M. « Santé, numérique, droit-s et Europe : interactions et conséquences », *in* POIROT-MAZERES I. (ss. la dir.) , *Santé, numérique et droit-s*, Actes du colloque des 7 et 8 septembre 2017, Université Toulouse 1 Capitole, coll. IFR actes de colloques, Presses de l'Université Toulouse I Capitole, 2018, p. 61 et svt.

THOLOZAN O., « Sécurité et droit : la nécessité au feu de l'imprévisibilité », *in* NGAMPIO-OBELE-BELE U. (dir.), *La sécurité en droit public*, coll. Colloques & Essais, Institut Universitaire Varenne 2018.

THOUVENIN D.,

- « La recherche translationnelle. Présentation de la Journée d'étude « Les frontières entre recherche et soin : Diagnostic et pronostics juridiques » », *in* BERNELIN M., SUPIOT E. (dir.), *Les frontières entre recherche et soin : Diagnostics et pronostics juridiques*, Cahiers Droit, Sciences & Technologies, PUAM, 2015, p. 25-38.
- « Le secret médical : droit ou devoir du professionnel ? », *RD sanit.*, 1982, p. 601.
- « Le secret médical – Droit pénal », *Droit médical et hospitalier*, 1998, Fasc. 11, n°6.
- « Lettre ministérielle DH/9 C n° 2711 du 15 février 1990 relative au secret médical. Relations entre médecins hospitaliers et médecins-conseils d'organismes mutualistes », *RDSS* 1990, p. 721.

- « L'obtention des organes : le don comme finalité et le prélèvement comme modalité », *in* B. FEUILLET-LE MINTIER (dir.), *Les lois « bioéthique » à l'épreuve des fait*s. *Réalités et perspectives*, PUF, 1999, pp. 77-131.
- *Jcl. Pénal*, Art. 226-13 et 226-14, Fasc. 10 : « Révélation d'une information à caractère secret. Conditions d'existence de l'infraction », 1998.
- « Secret médical et loi du 4 mars 2002 : quels changements ? », *Laennec*, 2007, n°1, p. 64.

TILLET E., « Histoire des doctrines pénales », *Rep. pén.*, juin 2002 (mise à jour octobre 2010).

TILMAN L., « Recherche et utilisation des données médicales : un cadre inadéquat ? », *in* BERNELIN M., SUPIOT E. (dir.)*, Les frontières entre recherche et soin : Diagnostics et pronostics juridiques*, Cahiers Droit, Sciences & Technologies, PUAM, 2015, Pp. 89-98.

TREBULLE F.-G., « La propriété à l'épreuve du patrimoine commun : le renouveau du domaine universel », *in Etudes offertes au professeur PHILIPPE MALINVAUD*, Litec, 2007, p. 659.

TRUCHET D., « La genèse de la construction des droits sanitaire et médico-social », *RDSS* 2014, p. 495.

TRUDEL P., « Quel droit et quelle régulation dans le cyberespace ? », *in Les promesses du cyberespace. Médiations, pratiques et pouvoirs à l'heure de la communication électronique*, *Sociologie et sociétés*, 2000, vol. 32, n° 2, Pp. 190–210.

TUNC R., « Le secret professionnel et les relations administratives », *La Revue administrative* 1948/3, p. 18.

TÜRK P.,

- « Les droits émergents dans le monde numérique : l'exemple du droit à l'autodétermination informationnelle », *Politéia*, 2017, p. 251.
- « La citoyenneté à l'ère numérique », *RDP* 2018, p. 623.

TUSSEAU G., « Critique d'une métanotion fonctionnelle », *RFDA* 2009, p. 641.

V

VACARI I., « L'hébergement des données de santé : entre contrat et statut », *RDSS* 2002, p. 695.

VALETTE D., « De l'automatisation à l'intelligence artificielle dans le domaine de la santé. Le Droit humain doit-il se saisir de l'intelligence artificielle ? », *Journal de Droit de la Santé et de l'Assurance Maladie* (*JDSAM*) 2017, n° 17, p. 8-13.

VAN DE MOORTEL B., « Confidentialité et secret professionnel – Pour en finir avec la confusion », *Gaz. Pal.*, 2003, n°126, p. 6.

VAN WAEYENBERGE A., « Les normes ISO, CEN et celles issues des consortiums privés : bric à brac ou système pour l'Union européenne ? », *in* FRYDMAN B., VAN WAEYENBERGE A. (dir.), *Gouverner par les standards et les indicateurs : De Hume au rankings*, coll. Penser le droit, Bruylant, 2014, p. 93.

VARAUT J.-M., RUET L., « Secret professionnel et confidentialité dans les professions juridiques et judiciaires », *Gaz. Pal.*, 1997, p. 1054.

VARNIER F., TREPEAU M., « La coopération hospitalière au service de la modernisation de notre système de santé », *RDSS* 2016, p. 620.

VERDIER H., VERGNOLLE S., « L'Etat et la politique d'ouverture en France », *AJDA* 2016, p. 92.

VERNY E., « La notion de secret professionnel », *RDSS* 2015, p. 395.

VIALLA F., « Perspectives pour une culture commune du secret et de l'information partagée », *JA* 2013, n°474, p.30.

VIALLA F., TERRIER E.,

- « Existe-t-il des notes personnelles ? Points de divergents », *RDS* 2005, n°5, p. 201.
- « Le secret partagé », *RDS*, n° 2, 2016 (v. numérique 2018), Pp. 52-64.
- « Perspectives pour une culture commune du secret et de l'information partagée », *Juris associations* 2013, n°474, p. 30.
- « Les restrictions à l'accès au dossier médical », *RDS*, 2009, n°30, Pp. 341-344.

VIGNAL N., « L'accès au dossier médical », *LPA*, 2002, n°122, p. 19.

VILLEY M., « le droit dans les choses », *in* AMSELEK P., GRZEGORCZYK C. (dir.), *Controverses autour de l'ontologie du droit*, PUF, 1989.

VINCENT J.-Y., *Jcl. Adm*, 2010, Fasc. 109-20 : « Accès aux documents administratifs – Régime spéciaux – Fichiers – Archives ».

VIOUJAS V., « Les soins psychiatriques aux détenus : des modifications mineures pour une problématique de santé publique majeure », *RDSS* 2011, p. 1071.

VIRIOT-BARRIAL D., « Secret médical et terrorisme », *RDSS* 2019, p. 236.

VITU A., « De l'illicéité en droit criminel français », *Bull. de la société de législation comparé*, 1984, p. 127.

VIVANT M.,

- « L'informatique dans la théorie générale du contrat », *D.* 1994, p. 117.
- « La privatisation de l'information par la propriété intellectuelle », *Revue internationale du droit économique*, 2006/4, t. XX, p. 361-388.

W

WAREMBOURG-AUQUE F., « Réflexions sur le secret professionnel », *RSC* 1978, p. 237.

WILSON C., « Personnel des collectivités territoriales : obligations relatives aux informations détenues par les agents », *Enc. des collec. loc. Dalloz*, 2015, Pp. 110-126.

WRIGHT A., DE FILIPPI P., « Decentralized Blockchain Technology and the Rise of Lex Cryptographia », abstract, Social Science Research Network (SSRN), 10 mars 2015 (papers.ssrn.com/sol3/ papers.cfm?abstract_id=2580664)

Y

YOLKA P., « Open data : « L'ouverture, c'est l'aventure », *AJDA* 2016, p. 79.

Z

ZENATI F., « L'immatériel est les choses », *in* TERRE F. (dir.), *Le droit et l'immatériel*, coll. *Arch. ph. droit*, t. 43, Sirey, 1999, p. 79.

ZOLYNSKI C.,

- « Big data : pour une éthique des données », *I2D – Information, données & documents* 2015/2, vol. 52, Pp. 25-26.
- « Blockchain et smart contracts : premiers regards sur une technologie disruptive », *RD banc. fin.* 2017, Dossier 4.
- « La *Privacy by Design* appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel », *Dalloz IP/IT* 2016, p. 404.

- « Les nouveaux contours de l'action de groupe et de l'action collective au lendemain de la loi pour la protection des données : un *empowerment* renforcé », *Dalloz IP/IT* 2018, p. 470.
- « Quelle approche légale de la *blockchain ?* », *Banque et stratégie* 2016, p. 16.

ZOLINSKY C., BENSAMOUN A., « Cloud computing et big data. Quel encadrement pour ces nouveaux usages des données personnelles ? », Réseaux 2015/1 n° 189, p. 103.

ZOLINSKY C., LATREILLE A.,

- « Nouvelle pratiques : faut-il de nouvelles protections ? », *in* MARTIAL-BRAZ N. (dir.), *La proposition de règlement européen relatif aux données à caractère personnel : propositions du réseau Trans Europe Experts*, coll. Trans Europe Experts, Société de législation comparée, 2014, p. 265.
- « Big data et protection des données à caractère personnel », *in* MARTIAL-BRAZ N. (dir.), *La proposition de règlement européen relatif aux données à caractère personnel : propositions du réseau Trans Europe Experts*, coll. Trans Europe Experts, Société de législation comparée, 2014, p. 262.

ZOLYNSKI C., MAXWELL W., « Protection des données personnelles », *D*. 2019, p. 1673.

ZORN-MACREZ C., « L'hébergement des données de santé sur support informatique », *Droit médical et hospitalier*, Litec, Fasc. 10, 2013.

ZORN C., « Libre circulation des données et RGPD : le cas des données composites », intervention au colloque *La libre circulation des données non personnelles* (dir. F. MACREZ), 24 mai 2019, Strasbourg, vidéos des interventions disponibles sur <http://www.canalc2.tv/video/15380>, consulté le 16 octobre 2019.

ZYENEP O., « Pourquoi et comment évaluer la performance des systèmes de santé ? » *in* BRAS P.- L., DE POURVILLE G. et TABUTEAU D. (dir.), *Traité d'économie et de gestion de la santé*, Presses de Sciences Po – Éditions de santé, 2009, pp. 75-82.

C - Articles de presse

B

BERTHIER T., « Convergence technologique : l'homme, la machine et la société », *The Conversation*, 28 mai 2017.

BIENVAULT P., « Faut-il lever le secret médical face à un pilote de ligne dépressif ? », *La croix*, 14 mars 2016.

BOUCHER P., « Safari ou la chasse aux français », *Le Monde*, 21 mars 1974.

C

CAILLARD J.-F., « Le RGPD, et si c'était aussi une opportunité de business ? », *Forbes Magazine*, 13 avril 2018.

F

FAURE S., « Les médecins doivent-ils renoncer au secret professionnel pour sauver des vies ? », *Libération*, 4 avril 2015.

G

GOURION D., « Terrorisme : "les psychiatres n'ont pas vocation à collaborer avec le ministère de l'intérieur", *Le Monde*, 21 août 2017.

J

JACOT M., « Faire de l'expérience de la maladie son métier », *Le Monde*, 22 avr. 2018.

L

LANI F.-P., « Vers un droit de propriété sur nos données personnelles », *Les Échos*, 5 juill. 2018.

LEMAIRE A., « Le secret professionnel, une conception périmée », *Le Monde*, 31 juillet 1953.

M

MARTIN-FORISSIER C., « Blockchain et RGPD, une union impossible », 24 août 2017, Laboratoire d'innovation numérique de la CNIL, disponible sur : <https://linc.cnil.fr/fr/blockchain-et-rgpd-une-union-impossible-0>, dernière consultation le 12 octobre 2019.

MODOUX F., « Pilote inapte, le secret médical en procès », *Tribune de Genève*, 29 mars 2015.

R

ROLLAND S., « Protection des données : le chaotique business de la conformité RGPD », *La tribune*, 25 mai 2018.

T

THIERRY G., « La Cour de cassation et le Conseil d'État s'emparent de l'intelligence artificielle », *Dalloz act.* 23 juillet 2019.

§ 4 - Rapports et communications

CNIL, *Rapport* « bilan et perspective », 1978-1980.

NORA S., MINC A., *L'informatisation de la société*. *Rapport au Président de la République*, La documentation française, 1978.

NORA S., MINC A., *Rapport au président de la République – L'informatisation de la société*, La documentation française, 1978.

CNIL, *Dix ans d'Informatique et libertés*, Economica 1988, p. 30.

THIERRY J.-P., *La télémédecine, enjeux médicaux et industriels, Rapport, Ministère de l'industrie des postes et des télécommunications et du commerce extérieur*, Ministère de l'enseignement supérieur et de la recherche, Ministère des affaires sociales de la santé et de la ville, 1993.

CONSEIL D'ETAT, *Les autorités administratives indépendantes*, 2001, p. 270

THOUVENIN D*., Consentement présumé ou droit d'opposition au prélèvement d'organes sur personne décédée : un exemple de conflit entre représentations communes et règles juridiques*, Rapport ronéotypé à l'Établissement français des greffes, 2004.

DIONIS DU SEJOUR J., ETIENNE J.-C., *Les télécommunications à haut débit au service du système de santé*, Office parlementaire d'évaluation des choix scientifiques et technologiques, Assemblée nationale – Sénat, 2004.

COUR DE CASSATION, *L'innovation technologique*, 2005, disponible sur < https://www.courdecassation.fr/IMG/pdf/cour_cassation-rapport_2005-3.pdf> (dernière consultation le 9 oct. 2019)

VELICOGNA M., *Utilisation des technologies de l'information et de la communication (TIC) dans les systèmes judiciaires européens*, Les études de la CEPEJ, n°7, 2007.

COMITE EUROPEEN DE LA PROTECTION DES DONNEES, Avis n°4/2007, 20 juin 2007, WP 136.19.

Communication de la Commission au Conseil, au Parlement européen et au Comité économique et social européen vers une contribution accrue de la normalisation à l'innovation en Europe, *Vers une contribution accrue de la normalisation à l'innovation en Europe*, COM (2008) 133 final, 11 mars 2008, p.7

DUMOULIN L., LICOPPE C., *Justice et visioconférence : les audiences à distance. Genèse et institutionnalisation d'une innovation*, contrat GIP Mission de recherche Droit et Justice / ISP / Télécoms Paris-Tech, Rapport final, 2009.

FIESCHI M., *La gouvernance de l'interopérabilité sémantique est au cœur du développement des systèmes d'information en santé*, Rapport à la ministre de la santé et des sports, 9 juin 2009.

« Stratégie numérique pour l'Europe » adoptée le 10 mai 2010 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions, COM (2010) 245 final.

CNIL, *Guide professionnel de santé*, 2011.

CNOM, « Prisons : Menace sur le secret médical », *Bulletin d'information de l'ordre national des médecins*, n° 18, juillet-août 2011.

COMITE EUROPEEN DE LA PROTECTION DES DONNEES, Avis n°15/2011, 13 juillet 2011, WP 187.28-29.

CNIL, « Vie privée à l'horizon 2020. Paroles d'experts », *Cahiers IP Innovation et prospective*, 30 novembre 2012, n°1.

CONTROLEUR GENERAL DES LIEUX DE PRIVATION DE LIBERTE, *Rapport d'activité*, 2013.

CONSEIL D'ETAT, *Le droit souple*, 2013, p. 32 et svt.

BRAS P.-L., LOTH A., *Rapport sur la gouvernance et l'utilisation des données de santé*, 2013.

ASIP-SANTE, *Principes fondateurs Politique Générale de Sécurité des Systèmes d'Information de Santé* (PGSSI-S), V1.0., juillet 2013.

ASIP-SANTE, *Guide Pratique Règles pour les dispositifs connectés d'un Système d'Information de Santé*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) - Novembre 2013 - V1.0.

CONSEIL D'ETAT, Étude annuelle 2014 : *le numérique et les droits fondamentaux*, La Documentation française, 2014.

BOUCHOUX C., *Refonder le droit à l'information publique à l'heure du numérique : un enjeu citoyen*, *une opportunité stratégique*, Rapport d'information n°589, 2014, t. 1.

COMITE EUROPEEN DE LA PROTECTION DES DONNEES, Avis n°05/2014, 10 avril 2014, WP 216.3

ASIP-SANTE, *Référentiel d'imputabilité*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) - Décembre 2014 - V1.0, p. 7.

ASIP-SANTE, *Référentiel d'identification des acteurs sanitaires et médico-sociaux*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), Décembre 2014, V1.0.

ASIP-SANTE, *Référentiel d'authentification des acteurs de santé*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), Décembre 2014, V2.0.

ANSSI, Rapport d'activité 2015, p. 14.

CNOM, *Santé connectée. De la e-santé à la santé connectée*, Livre Blanc, Janvier 2015.

CNNUM, *Rapport au premier ministre*, « Ambition numérique. Pour une politique française et européenne de la transition numérique », juin 2015.

MILON A., DEROCHE C., DOINEAU E., *Rapport fait au nom de la commission des affaires sociales*, Sénat, session extraordinaire de 2014-2015, 22 juillet 2015.

ROCHFELD J., *Quelle politique européenne en matière de données personnelles ?*, New Deal Foundation, Rapport d'étude, septembre 2015.

CNNUM, *Rapport remis à la Ministre des Affaires sociales*, *de la Santé et des Droits des femmes*, « La santé, bien commun de la société numérique. Construire le réseau du soin et du prendre soin », octobre 2015.

CSF, Rapport : *Créer les conditions d'un développement vertueux des objets connectés et des applications mobiles en santé*, 2016, disponible sur <https://solidarites-sante.gouv.fr/IMG/pdf/rapport-gt28-octobre-2016-vf-full.pdf>)

ASIP-SANTE, *Guide des mécanismes de protections de l'intégrité des données stockées*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) – Janvier 2017-V1.0.

ASIP-SANTE, *Guide gestion des habilitations d'accès au SI*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), V. 1.0., janvier 2017.

« Stratégie pour un marché unique numérique », Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions, Stratégie pour un marché unique numérique en Europe, COM (2015) 192 final, mars 2018, p. 27-28

VILLANI C., Rapport au premier ministre, *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*, mars 2018.

PON D., COURY A., Rapport final : *Accélérer le virage numérique*, septembre 2018, disponible sur < https://solidarites-sante.gouv.fr/IMG/pdf/masante2022_rapport_virage_numerique.pdf > (dernière consultation le 21 mai 2019).

CCNE, Avis n° 19, *Contribution du comité consultatif national d'éthique à la révition de la loi bioéthique*, 18 septembre 2018, p. 103.

CUGGIA M., POLTON D., WAINRIB G., COMBES S., *Rapport de la mission de préfiguration Health Data Hub*, octobre 2018.

PARIS D., MOREL A., L'HUISSIER P., *Rapport d'information présenté en conclusion des travaux d'une mission d'information sur les fichiers mis à la disposition des forces de sécurité*, 17 octobre 2018, p. 51.

OFFICE PARLEMENTAIRE D'EVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, « Les technologies quantiques : introduction et enjeux », note n° 13, mars 2019.

THIEULIN B., (rapporteur), *Pour une politique de souveraineté européenne du numérique*, mars 2019.

RIST S., MESNIER T., *Rapport fait au nom de la commission des affaires sociales sur le projet de loi relatif à l'organisation et à la transformation du système de santé, volume ii commentaires d'articles et annexes*, 14 mars 2019, p. 100.

FRISON-ROCHE M.A., *L'apport du droit de la compliance à la gouvernance d'internet*, Rapport commandé par Monsieur le Ministre en charge du Numérique, avril 2019.

CONFERENCE MINISTRE, 25 avril 2019, Feuille de route « Accélération du virage numérique » Ma Santé 2022, disponible sur < https://solidarites-sante.gouv.fr/IMG/pdf/190425_dossier_presse_masante2022_ok.pdf > (dernière consultation le 10 août 2019).

MILON A., rapport fait au nom de la commission des affaires sociales sur le projet de loi, adopté par l'assemblée nationale après engagement de la procédure accélérée, relatif à l'organisation et à la transformation du système de santé, 22 mai 2019, p. 100.

COMITE CONSULTATIF NATIONAL D'ETHIQUE, Avis n°130, 29 mai 2019.

ASIP-SANTE, *Principes fondateurs Politique Générale de Sécurité des Systèmes d'Information de Santé* (PGSSI-S), V1.0, Juill. 2013 <https://esante.gouv.fr/sites/default/files/media_entity/documents/Principes_Fondateurs_PGSSI.pdf>, dernière consultation le 12 octobre 2019.

§ 5 - Table de jurisprudence

A - Jurisprudence judiciaire

1 - Cour de cassation

Chambre criminelle

Crim., 22 février 1828

- *S.* 1828.1.41

Crim., 23 juin 1838

- *S.* 1838.1.626

Crim., 12 avril 1850

- *DP* 1850.1.142

Crim., 6 janvier 1855

- *S.* 1855.1.155
- *D.* 1855.1.30

Crim., 24 mai 1862

- *D.* 1862.1.545

Crim., 21 novembre 1874

- *S.* 1875.1.89, rapp. BAUDOIN et note CAUWES

Crim., 19 décembre 1885

- *S.* 1886.1.86, rapp. TANON
- *D.* 1886.1.347.

Crim., 9 juillet 1886

- *S.* 1886.1.487
- *D.* 1886.1.475

Crim., 20 mai 1899

- *S*. 1901.1.64
- *D*. 1900.1.25

Crim., 9 novembre 1901

- *D*. 1902.1.235

Crim., 26 juillet 1928, *Bull*. *Crim*., n°226

Crim., 6 juillet 1929

- *DH* 1929.494

Crim., 17 juillet 1936

- *DH* 1936.494

Crim., 3 mars 1938

- *DH*. 1938.341
- *S*. 1938.1.209, note H. ROUSSEAU

Crim., 11 mars 1942, *Bull*. *crim*., n°23

Crim., 8 mai 1947, *Bull*. *crim*., n°128

- *D*. 1948.109, note P. GULPHE
- *JCP* 1948.II.4141, note A. LEGAL
- *S*. 1947.1.106

Crim., 12 avril 1951, *Bull*. *crim*., n°103

- *D*. 1951.363

Crim., 30 juin 1955, *Bull*. *crim*., n°334

- *JCP* 1955.II.8860 bis
- *D*.1955.718
- *Dr*. *soc*. 1955.594
- *Gaz*. *Pal*. 1955.2, J. 137

Crim., 6 décembre 1956, *Bull*. *crim*., n°820

- *D*. 1957.193
- *S*. 1957.126
- *Gaz*. *Pal*. 1957.1, J. 164

Crim., 7 février 1957, *Bull*. *crim*., n°129

- *RSC* 1957.640, obs. L. HUGUENEY

Crim., 7 mars 1957, *Bull*. *crim*., n°241

Crim., 5 décembre 1957

- *D*. 1958.98

Crim., 21 janvier 1959, *Bull*. *crim*., n°59

Crim., 11 février 1960, *Bull*. *crim*., n°85

- *JCP* 1960.II.11604, note R. SAVATIER
- *D*. 1960.258, note J.-M. R.

Crim., 3 mars 1960, *Bull*. *crim*., n°138

- *RSC* 1961.105, obs. P. LEGAL

Crim., 24 mai 1960, *Bull*. *crim*., n°284

- *D*. 1960, Somm.114
- *JCP* 1960.II.11858, note SAVATIER
- *Gaz*. *Pal*. 1960. Doctr. 91
- *RSC* 1960.650, obs. HUGUENEY et 1961.356, obs. BOUZAT

Crim., 8 juin 1966, *Bull*. *crim*., n°167

- *D*. 1966.542

Crim., 22 décembre 1966

- *D*.1967.122, rapp. R. COMBALDIEU
- *JCP* 1967.II.15126, note R. SAVATIER
- *RSC* 1967.463, obs. G. LEVASSEUR

Crim., 27 juin 1967, *Bull*. *crim*., n°194

Crim., 20 décembre 1967, *Bull*. *crim*., n°338

- *D*. 1967.309, note E. LEPOINTE
- *RSC* 1968.343, obs. G. LEVASSEUR

Crim., 25 janvier 1968, *Bull*. *crim*., n°25

- *D*. 1968.153, rapp. J.-C. COSTA
- *JCP* 1968.II.15425
- *Gaz*. *Pal*. 1968.I.164
- *RSC* 1968.344, obs. G. LEVASSEUR

Crim., 24 avril 1969

- *D*. 1969.637, rapp. F. CHAPAR
- *JCP* 1970.II,16336, note R. SAVATIER

Crim., 5 février 1970, *Bull*. *crim*. n°56

- *D*. 1970.249
- *JCP* 1970.II.16311
- *RSC*. 1970.652, obs. G. LEVASSEUR

Crim., 9 juillet 1970

- *RSC* 1973.81, Comm. M. CULIOLI

Crim., 4 novembre 1971

Crim., 7 novembre 1974, *Bull*. *crim*., n° 323

- *D*. 1974, Somm.144.

Crim., 30 janvier 1975

- *JCP G* 1975.18137, note GAVALDA
- *RSC* 1975.1011, obs. VITU

Crim., 20 janvier 1976

- *Gaz*. *Pal*. 1976.1, J. 308

Crim., 1er février 1977, *Bull*. *crim*., n°40

Crim., 23 mars 1977, *Bull*. *crim*., n°109

- *JCP* 1979.II.19039, note P. CHAMBON
- *RSC* 1977.832, obs. J. ROBERT

Crim., 8 novembre 1977, *Bull*. *crim*., n°339

Crim., 9 octobre 1978, *Bull*. *crim*., n°263

- *D*. 1979.185, note P. CHAMBON
- *Gaz*. *Pal*. 1979.1, J. 245
- *RSC* 1979.560, obs. G. LEVASSEUR

Crim., 8 janvier 1979, *Bull*. *crim*., n°13

- *D*. 1979.509, note P. CORLAY
- *D*. 1979. IR 182, obs. G. ROUJOU DE BOUBEE
- *JCP* 1981.I.3041, n°25, note M.-L. RASSAT

Crim., 8 janvier 1979, *Bull*. *crim*., n°73

Crim., 21 mai 1979, *Bull*. *crim*., n°178

- *RSC* 1980.439, obs. G. LEVASSEUR

Crim., 17 mars 1982

Crim.,19 octobre 1982, *Bull*. *crim*., n°225

Crim., 5 juin 1985, *Bull*. *crim*., 1985, n°218

- *D*. 1986. IR, 120, obs. J. PRADEL
- *D*. 1988.106, note H. FÉNAUX
- *Comm*. *com*. *électr*. 2012, Comm. 127, A. LEPAGE

Crim.,19 novembre 1985, *Bull*. *crim*., n°364

- *Dr*. *soc*. 1986.419, Comm. J. SAVATIER

Crim., 29 avril 1986, *Bull*. *crim*., n°148

- *JCP* 1987.II.20788, note H. CROZE
- *D*. 1987.131, note M.-P. LUCAS DE LEYSSAC

Crim., 3 novembre 1987

Crim., 6 janvier 1989

- *Dr*. *pénal* 1990, n°86

Crim., 12 janvier 1989, *Bull*. *crim*., n°14

- *RSC* 1990.346, obs. P. BOUZAT

- *Ibid*. 507, obs. M.-P. LUCAS DE LEYSSAC
- *RTD com*. 1990.143, obs. P. BOUZAT

Crim., 1er mars 1989, *Bull*. *crim*., n°100

- *D*. 1990, Somm.330, obs. J. HUET
- *RSC* 1990.346, obs. P. BOUZAT, et .507, obs. M.- P. LUCAS DE LEYSSAC
- *RTD com*. 1990.142, obs. P. BOUZAT

Crim., 7 mars 1989

- *JCP* 1989.IV.200

Crim., 24 octobre 1990, *Bull*. *crim*., n°355

Crim., 3 mars 1992

- *Gaz*. *Pal*, 24 avril 1994, n°114-116 chron.18
- *D*.1994, n°16 IR.106

Crim., 12 janvier 1994, *Bull*. *crim*. n°16

- *JCP G* 1994, n°17.925

Crim., 8 février 1994

- *Dr*. *pén*., 1994

Crim., 6 juillet 1994, *Bull*. *crim*. n°267

Crim., 31 janvier 1995, n°94-80562

- *D*. 1994, Somm.157, obs. G. ROUJOU DE BOUBEE
- *Dr*. *pén*. 1992, *Comm*. *N°254*

Crim., 3 avril 1995, *Bull*. *crim*., n°142

- *D*. 1995.320, obs. J. PRADEL
- *RSC* 1995.599, obs. J. FRANCILLON et .821, obs. R. OTTENHOF
- *RSC* 1996.645, obs. B. BOULOC et .660, obs. R. OTTENHOF

Crim., 25 octobre 1995, *Bull*. *crim*., n°323

Crim., 26 octobre 1995, *Bull*. *crim*., n°324

- *RSC* 1996.648, obs. B. BOULOC
- *Dr*. *pénal* 1996, Comm. 189, obs. J.-H. ROBERT

Crim., 26 octobre 1995, *Bull*. *crim*., nº 328

- *RSC* 1996.660, obs. R. OTTENHOF

Crim., 29 avril 1996, n°95-82478

Crim., 14 mai 1996, n°93-80982

Crim., 8 avril 1998, *Bull*. *crim*., n°136

- *Dr*. *pén*. 1998, Comm. n°113, obs. M. VERON
- *D*. 1999, Somm.381, obs. J. PENNEAU
- *Procédures* 1998, Comm. n°228, obs. J. BUISSON.

Crim., 24 septembre 1998, *Bull. crim.* n°336

Crim., 9 juin 1999, n°98-80052, *Bull. crim.* n°366

- *JCP G* 1999.IV.2867
- *Dr. Pén.* 1999, n°11, Comm. 138, M. VERON

Crim., 21 septembre 1999, *Bull. crim.* n°191

- *D.* 2000, Somm.383, obs. M.-C. AMAUGER-LATTES
- *RSC* 2000.200, obs. Y. MAYAUD

Crim., 28 septembre 1999, *Bull. crim.* n°201

- *RSC* 2000.202, obs. Y. MAYAUD

Crim., 4 novembre 1999, n°99-80157

Crim., 16 mai 2000, *Bull. Crim.*, n°192

- *Dr. pénal* 2000, obs. M. VERON

Crim., 25 octobre 2000

- *JCP G* 2001.II.10566, note P. MISTRETTA
- *D.* 2001.1052, note T. GARÉ

Crim., 14 novembre 2000, *Bull. crim.*, n°338

- *Dr. pén.* 2001, Comm. 28 obs. M. VERON, et chron. 16, obs. S. JACOPIN
- *D.* 2001.1423, note B. DE LAMY
- *RTD civ.* 2001.912, obs. T. REVET
- *Gaz. Pal.* 2001, 2, Somm.1219, note Y. MONNET
- *RSC* 2001.305, obs. R. OTTENHOF

Crim., 3 mai 2001, n°00-84301

Crim., 19 juin 2001, *Bull. crim.*, n°149

- *D.* 2001.2538, note B. BEIGNIER et B. DE LAMY
- *RSC* 2002.96, obs. B. BOULOC, .119, obs. J. FRANCILLON, et .592, obs. J.-P. DELMAS SAINT-HILAIRE
- *RTD com.* 2002.178, obs. B. BOULOC
- *JCP* 2002, II, 10064, concl. D. COMMARET, note A. LEPAGE

Crim., 19 juin 2001, *Bull. crim.*, n°14

- *D.* 2001.2538, note B. BEIGNIER et B. DE LAMY
- *D.* 2002, Somm.1463, obs. J. PRADEL
- *RSC* 2002.96, obs. B. BOULOC
- *RSC* 2002.119, obs. J. FRANÇILLON
- *RSC* 2002.592, obs. J.-P. DELMAS SAINT-HILAIRE
- *JCP* 2002.II.10064, concl. D. COMMARET, note A. LEPAGE

Crim., 30 octobre 2001, n°99-82136

- *Gaz. Pal.* 2002.II.1476
- *Gaz. Pal.* 2002, n°297.40, obs. A. MOLE ET H. LEBON

- *JCP E 2002*, n°23.888, obs. M. VIVANT ET N. MALET-POUJOL
- *Comm. Com. élect*. 2002, n°11, Comm. 14, note A. LEPAGE

Crim., 22 septembre 2004, *Bull. crim*., n°218

- *JCP G* 2005.I.106, n°1, obs. M. VERON
- *JCP G* 2002.II.10034, note A. MENDOZA-CAMINADE
- *D*. 2005.411, note B. DE LAMY

Crim., 19 octobre 2005, n°04-85098

Crim., 20 juin 2006, n°05-86491

Crim., 24 avril 2007, n°06-88051, *Bull. crim*., n°108

- *AJ pénal* 2007.331, obs. C. SAAS
- *RSC* 2007.815, obs. Y. MAYAUD

Crim., 3 juin 2008, n°08-80467

- *JCP E* 2009.1674, n°27, obs. M. VIVANT, N. MALLET-POUJOL et J.-M. BRUGUIERE

Crim., 14 mars 2006, *Bull. crim*., n°69

- *Comm. com. électr*. 2006, Comm. 131, note A. LEPAGE
- *D*. 2007, pan. 404, obs. T. GARE
- *AJ Pén*. 2006.260, G. ROUSSEL

Crim., 12 juin 2007, *Bull. crim*., n°157

- *JCP G* 2007.II.10159, note F. FOURMENT, C. MICHALSKI et P. PIOT
- *Dr. pénal* 2007, Comm. 143, obs. M. VERON
- *D*. 2009.123, obs. T. GARE
- *AJ pénal* 2007.439, obs. G. ROYER ; *RSC* 2008.95, obs. J. FRANCILLON
- *RTD com*. 2008.197, obs. B. BOULOC
- *RPDP* 2008.113, obs. J. –C. SAINT-PAU

Crim., 3 octobre 2007, *Bull. crim*., n°236

- *AJ pénal* 2007.535

Crim., 4 mars 2008, n°07-84002

- *D*. 2008.2213, Comm. S. DETRAZ
- *Rev. pénit*. 2008.880, obs. V. MALABAT
- *RSC* 2009.131, obs. J. FRANCILLON

Crim., 26 mars 2008, n°07-87072

Crim., 11 février 2009, n°07-86705

- *AJ pénal* 2009.183
- *D*. 2009.2403, obs. B. SARCY.

Crim., 9 juin 2009, *Bull. crim*., n°118

- *Rev. pén*. 2009.858, obs. S. FOURNIER
- *Gaz. Pal*. 25 août 2009, n°237.10, note S. DETRAZ
- *D*. 2010.306, note H. KOBINA GABA

Crim., 2 décembre 2009, n°09-82447

- *Com*. *Comm*. *élec*., n°3, Mars 2010, Comm. 28, A. LEPAGE

Crim., 18 janvier 2011, n°10-83258

Crim.,15 février 2011, n°10-82808

- *D*. 2012.765, pan. E. DREYER

Crim., 8 novembre 2011, n°10-82021

Crim., 16 novembre 2011, n°10-87866, *Bull*. *crim*., n°233

Crim., 3 avril 2012, n°11-85571

Crim., 5 septembre 2012, n°12-90045

Crim., 22 octobre 2014, n°13-82630

- *D*. 2015.415, note A. MENDOZA-CAMINADE

Crim., 25 mai 2016, *Bull*. *crim*., n°160

- *RSC* 2016.265, note Y. MAYAUD,

Crim., 22 mars 2017, n°15-85929

- *Rev*. *sociétés* 2018.56, note H. MATSOPOULOU
- *D*. 2017.762
- *ibid*.1877, obs. C. MASCALA
- *AJ pénal* 2017.232, obs. G. BEAUSSONIE
- *RTD com*. 2017.447, obs. L. SAENKO

Crim., 20 mai 2015, *Bull*. *crim*., n°119

- *D*. 2015.1466, note L. SAENKO
- *ibid*. 2465, obs. G. ROUJOUR DE BOUBEE, T. GARE, C. GINEST, M.-H. GOZZI et S. MIRABAIL
- *AJ pénal* 2015.413, note E. DREYER
- *RDC* 2015. 951, note P. BERLIOZ
- *RSC* 2015.860, obs. H. MATSOPOULOU
- *Ibid*. 887, obs. J. FRANCILLON
- *RTD com*. 2015.600, obs. B. BOULOC
- *RTD eur*. 2016.374, obs. E. MATRINGE
- *Dr. pén.* 2015, comm. 107, note M. VERON
- *Dr*. *pénal* 2015, Comm. 123, note P. CONTE
- Chron. 10, obs. A. LEPAGE, n°15
- *PI* janvier 2016, n°58.97, obs. M. VIVANT
- *JCP* 2015.887, note G. BEAUSSONIE
- *Dall*. *actu*., 5 juin 2015, obs. C. DUHIL DE BENAZE
- *Gaz*. *Pal*.18 juin 2015, n°169.8, note S. DETRAZ
- *LPA*, 29 juillet 2015, n°150.15, obs. E. CHAUVIN

Crim., 8 juillet 2015, *Bull*. *crim*., n°49

- *RSC* 2015.651, obs. Y. MAYAUD

- *D*. 2015, chron. 10, note A. LEPAGE
- *Dall*. *Actu*., 9 septembre 2015, obs. FUCINI
- *AJ pénal*, 2016.33, note AUBERT
- *Dr*. *pén*. 2015, n°9, Comm. 109, M. VERON

Crim., 10 mai 2017, n°16-81822

- *Dr*. *pén* 2017, n°12, chron. 11, n°8, Comm. A. LEPAGE

Crim., 28 juin 2017, n°16-81113, publié au *Bull*.

- *D*. 2017.1885, note G. BEAUSSONIE
- *AJ pén*. 2017.448, obs. J. LASSERRE-CAPDEVILLE
- *RSC* 2017.752, obs. H. MATSOPOULOU
- *RTD com*. 2017.713, obs. L. SAENKO

Crim., 16 janvier 2018, n°16-87168

- *D*. 2018.172
- *AJ pénal* 2018.205, obs. J.-B. THIERRY
- *RSC* 2018.480, obs. P. MISTRETTA
- *Dall*. *actu*., 12 février 2018, obs. M. RECOTILLET
- *RDS* n°83.2018.389, obs. M. MAZZUCOTELLI

Chambre des requêtes

Req., 18 juillet 1904

- *S*. 1905.1.233
- *D*. 1905.1.43

Chambre civile

Civ., 13 juillet 1936

- *Gaz*. *Pal*. 1936.2, J. 727
- *S*. 1938.1.201, note A. LEGAL
- *JCP* 1937.II.18 note A. PERRAUD-CHARMANTIER

Chambre commerciale

Com., 8 juillet 2003, *Bull*. *civ*. IV, n°119

- *RTD Com*. 2003.783, obs. M. CABRILLAC
- *D*. 2003.2170, obs. V. AVENA-ROBARDET

Première chambre civile

Civ. 1e, mai 1899

- *D*. 1899.1.585, note M. PLANIOL

- *S*. 1901.161, note A. ESMEIN

Civ. 1e, 22 janvier 1957

- *D*. 1957.445, note SAVATIER

Civ. 1e, 26 mai 1964

- *D*. 1965.109, M. DELMAS-MARTY
- *D*. 1982, chron.267

Civ. 1e, 6 juin 1987, *Bull*. *civ*. I, n°191

Civ. 1e, 3 janvier 1991, n°89-13808

Civ. 1e, 9 juin 1993, *Bull*. *civ*. I, n°214

- *RTD civ*. 1996.166, obs. J. MESTRE

Civ. 1e, 6 mars 1996

- *D*. 1997.7, note J. RAVANAS

Civ. 1e, 18 mars 1997, *Bull*. *civ*. I, n°99

- *JCP* 1997.II.22829, concl. P. SARGOS
- *D*. 1997, Somm.315, note J. PENNEAU

Civ. 1e, 16 juillet 1998

- *D*. 1999.541, note J.-C. SAINT-PAU

Civ. 1e, 6 octobre 1998, n°96-13600

- *D*. 1999. Somm.376, obs. J.-J. LEMOULAND
- *RTD civ*. 1999.62, obs. J. HAUSER

Civ. 1e, 22 mai 2002, *Bull*. *civ*. I, n°144

- *D*. 2002, IR.2029
- *Defrénois* 2002.1477, note J. MASSIP
- *D*. 2004.2682, note D. DUVAL-ARNOULD

Civ. 1e, 29 octobre 2002, *Bull*. *civ*. I, n°244

- *D*. 2002. IR. 3186

Civ. 1e , 9 décembre 2003, *Bull*. *civ*. I, n°254

- *Gaz*. *Pal*. 2005, Somm.1399, obs. P. GUERDER
- *RTD civ*. 2004.264, obs. J. HAUSER

Civ. 1e, 15 juin 2004, *Bull*. *civ*. I, n°171

- *D*. 2004.2682, note D. DUVAL-ARNOULD
- *D*. 2005 Pan.1323, obs. H. GROUTEL
- *RTD civ*. 2005.99, obs. J. HAUSER, et .384, obs. J. MESTRE et B. FAGES

Civ. 1e, 7 décembre 2004, *Bull*. *civ*. I, n°306

- *D*. 2005, IR.339, Pan.332, obs. N. FRICERO, Pan.403, obs. J. PENNEAU, et Pan.1317, obs. H. GROUTEL
- *AJDA* 2005.167

Civ. 1e, 26 septembre 2006, *Bull*. *civ*. I, n°417

Civ. 1e, 11 juin 2009, n°08-12.742

- *D*. 2009.1760

- *ibid*. 2714, obs. Ph. DELEBECQUE, J.-D. BRETZNER et T. VASSEUR
- *RTD civ*. 2009.695, obs. J. HAUSER

Civ. 1e, 14 janvier 2010, *Bull*. *civ*. I, n°4

- *D*. 2010.1125, obs. V. AVENA-ROBARDET, note J. MORET-BAILLY
- *ibid*. 2671, obs. P. DELEBECQUE, J.-D. BRETZNER et I. GELBARD-LE DAUPHIN
- *ibid*. 2011.552, obs. B. Blanchard

Civ. 1e, 22 septembre 2011, *Bull*. *civ*. I, n°148

Civ. 1e, 9 avril 2014, *Bull*. *civ*. I, n°67

- CCE, n°6, Juin 2014, Comm. 57 A. LEPAGE

Civ. 1e, 3 novembre 2016, n°15-22595

- *AJDA* 2017.23
- *D*. 2016.2285
- *Dalloz IP/IT* 2017.120, obs. G. PERONNE et E. DAOUD
- *RTD civ*. 2017.94, obs. J. HAUSER
- *Légipresse* 2017, n°345.27, obs. N. BOTCHORICHVILI
- *JCP G* 2016.1310, obs. R. PERRAY
- *Dr*. *pén*. 2015, chron. 11, n°12, obs. A. LEPAGE
- *Gaz*. *Pal*. 15 novembre 2016, n°40. 24, obs. Ph. INGALL-MONTAGNIER
- *RLDI* 2016, n°4087, obs. L. COSTES

Deuxième chambre civile

Civ. 2e, 12 juillet 1966, *Bull*. *civ*. II, n°778

- *D*. 1967.181, note P. MIMIN

Civ. 2e, 7 janvier 1976, *Bull*. *civ*. II, n°3

Civ. 2e, 24 avril 2003, *Bull*. *civ*. II, n°114

- *Dr*. *et patr*. juillet-août 2003.86, obs. G. LOISEAU
- *D*. 2006.689, pan. J. PENNEAU

Civ. 2e, 18 mars 2004, n°02-13529

Civ. 2e, 3 juin 2004, *Bull*. *civ*. II, n°273

- *D*. 2004.2069, note J. RAVANAS
- *D*. 2005.2651, obs. L. MARINO
- *Dr*. *fam*. 2004, Comm.172, note V. LARRIBAU-TERNEYRE
- *RTD civ*. 2004.489, obs. J. HAUSER

Civ. 2e, 2 juin 2005, *Bull*. *civ*. II, n°142

- *D*. 2006.1784, obs. H. GROUTEL

Civ. 2e, 22 novembre 2007, n°06-18250

- *D*. 2008. AJ.95, et Pan.506, spéc. 510, obs. J. PENNEAU

Civ. 2e, 13 novembre 2008, *Bull*. *civ*. II, n°240

- *D*. 2008. AJ.2948
- *RDSS* 2009.185, obs. T. TAURAN

Civ. 2e, 25 juin 2009, *Bull. civ.* II, n°175

Civ. 2e, 12 Mars 2015, n°14-13.485

Chambre commerciale

Com. 3 mai 2012, *Bull. civ.* IV, n°87

- *D.* 2012.1343
- *Rev. sociétés* 2012.721, note E. STERU et E. DEZEUZE

Com. 10 février 2015, *Bull. civ.* IV, n°20

- *D.* 2015.428
- *D.* 2015.959, obs. J. LASSERRE CAPDEVILLE
- *RDT* 2015.191, obs. P. ADAM
- *Dall. actu.*, 24 février 2015, obs. V. AVENA-ROBARDET
- *JCP* 2015.226, obs. C. BARRIERE
- *LEDB* mars 2015, obs. R. ROUTIER

Chambre sociale

Soc. 3 novembre 2011, *Bull. civ.* V, n°247

- *JCP G* 2011, act. 1284, obs. N. DEDESSUS-LE-MOUSTIER
- *JCP E* 2011.1926, note D. CORRIGNAN-CARSIN
- *Gaz. Pal.* 17 novembre 2011, n°321.28, obs. C. BERLAUD
- *JCP S* 2012, n°6.1054, obs. G. LOISEAU
- *Comm. com. électr.* 2012, Comm. 32, obs. A. LEPAGE
- *RJEP* 2012, chron.2, obs. G. HENON et N. SABOTTIER
- *Dr. pén.* 2012, chron.10, obs. A. LEPAGE
- *LPA* 3 juin 2013, n°110.5, obs. A. FIORENTINO

Soc. 20 avril 2017, n°15-27927 et n°15-27955

- *D.* 2017, IR.920
- *Dall. actu.*, 5 mai 2017, Comm. J. SIRO
- *Les cahiers sociaux*, n° 297.302, F. CANUT
- *Gaz. Pal.*, n°19.41, C. BERLAUD
- *LPA*, 6 septembre 2017, n°177-178.16. P.VERON

2 - B. Juridictions du fond

a - Juridictions du second degré

Bordeaux, 29 novembre 1893

- *DP* 1894. 2.86

Grenoble, 3 mars 1905

- *D.* 1907.2.194

Angers, 2 Juillet 1998, JurisData, n°1998-045334

Chambéry, 22 Mai 1986, JurisData, n°1986-600290

Colmar, 13 décembre 1951

- *D*. 1952.132

Grenoble, 22 mai 1952

Paris, 6 mai 1958

- *JCP* 1958.II.10833, concl. LECOURTIER
- *RSC* 1959.122, obs. HUGUENEY

Orléans, 20 janvier 1961

- *D*. 1961.485
- *S*. 1961.284
- *JCP* 1961.II.12132
- *Gaz*. *Pal*. 1961.419
- *RSC* 1961.590, obs. HUGUENEY

Paris, 27 mars 1963

- *D*. 1963, Somm.87

Paris, 9 novembre 1966

- *JCP* 1968.II.15368, note R. DE LESTANG
- *D*. 1952.445

Paris, 21 décembre 1970

- *JCP* 1971.II.16653, note R. LINDON

Paris, 13 juillet 1973

- *D*. 1974.16, note E.-S. de la MARNIERRE

Paris, 9 juillet 1980

- *D*. 1981.72, 2e esp., note R. LINDON

Paris, 11 Janvier 1985, JurisData, n°1985-600480

Paris, 17 mars 1986

Rennes, 24 juin 1986

Paris, 26 juin 1986

- *D*. 1987. Somm.136

Paris, 24 septembre 1990, *JurisData*, n°1990-023624

Paris, 17 Décembre 1991, *JurisData* n°1991-024673

Rennes, 13 janvier 1992

- *JCP E*, 1993.II.432, note Ch. GAVALDA
- *D*. 1993, Somm.54, obs. M. VASSEUR
- *D*. 1994, Somm.287, obs. H. MAISL

Paris, 5 avril 1994

- *JCP E* 1995.I.461, obs. F. VIVANT et C. LE STANC
- *LPA* 1995, n°80.13, chron. V. ALVAREZ

Paris, 24 mai 1994, JurisData, n°022205

Paris, 5 décembre 1997

- *D*. 1998. IR 32

Paris, 30 octobre 1998

- *D*. 1998. IR 259
- *RTD civ*. 1999.61, obs. J. HAUSER

Paris, 1er juillet 1999

- *D*. 1999, IR.230

Grenoble, 4 mai 2000

- *JCP G* 2001.IV.1473

Grenoble, 30 octobre 2000, JurisData n°2000-146355

Nîmes, 28 mai 2002, n°612/02, JurisData n°2002-197846

Versailles, 16 janvier 2003

- *Légipresse* 2003.I.106

Paris, 21 octobre 2004, JurisData n°2004-253278

- *CCE* Mars 2005, n°3, comm. A. LEPAGE

Grenoble, 11 mars 2009, JurisData n°2009-002946

- *JCP G*, n°27.2009.65, obs. A.- G. ROBERT

Amiens, 9 mars 2011, n°10/03137

Orléans, 6 février 2014, n°13/01878

Paris, 15 septembre 2017, pôle 4, ch. 11 (disponible sur <www.legalis.net>)

b - Juridictions du premier degré

TGI Avesne sur Helpe, 2 avril 1951

- *JCP* 1951.IV.128

T. civ. Versailles, 10 juillet 1957

- *D*. 1958, Somm.48
- *JCP* 1958.II.10436, note SAVATIER
- *Gaz*. *Pal*. 1958.77, *RSC* 1958.399, obs. HUGUENEY et .407, obs. BOUZAT

T. corr. Montbéliard, 28 juin 1963

- *S*. 1963.299
- *D*. 1963.544

T. corr. Avignon, 30 septembre 1965

- *Gaz*. *Pal*. 1965.2.347
- *D*. 1966, Somm.11

TGI Paris, 8 juillet 1970

- *JCP G* 1970.II.16550, note R. LINDON

TGI Paris, 3 juillet 1971

- *D*. 1972, Somm.47

TGI Paris, 20 juin 1973

- *D*. 1974.766, note R. LINDON

TGI Paris, 2 juin 1976

- *D*. 1977.364, 2e esp., note R. LINDON

TGI Nantes, 16 décembre 1985

- *D*. 1986.471, note J. FRAYSSINET
- *JCP E* 1986.II.15791, obs. M. VIVANT et A. LUCAS

T. corr. Briey, 15 septembre 1992

- *Gaz*. *Pal*. 1993.1. 201

- *D*. 1994, Somm.289, obs. H. MAISL

TGI Paris, 20 novembre 1985

- *D*. 1987. Somm.140
- *Gaz*. *Pal*. 1988.1.Somm.145

TGI Créteil, 10 juillet 1987

- *DS* 1988.319, note J. FRAYSSINET

TGI Nanterre, 12 décembre 2000

- *Légipresse* 2001, I.45

TGI Paris, 3 mars 2003

- *Légipresse* 2003, I.123

TGI Paris, 9 février 2005

- *Légipresse* 2005, I.54

TGI Nanterre, 4 avril 2005

- *Légipresse* 2005, I, p.145

TGI Nanterre, 20 juin 2005

- *Légipresse* 2005, I.127

TGI Nanterre, 27 avril 2006

- *Légipresse* 2006, I.125

TGI Paris, 5 mars 2007

- *Légipresse* 2007, I.162

TGI Nanterre, 1re ch., 28 avril 2011

- *Legipresse* juin 2011.341

T. com. Paris, 28 janvier 2014, *M. X. c/ Google Inc. et Google France*

- *RLDI* avril 2014, n°103, n°3438.57, obs. L. COSTES

- *RLDI* juin 2014, n°3494.36, note M. COMBE

TGI Marseille, 7 juin 2017

B - Jurisprudence administrative

1 - Conseil d'Etat

CE Ass., 12 avril 1957, *Devé*, *Rec*. *Lebon*

CE, 20 novembre 1959, *Rec*. *Lebon*

- *JCP* 1960.II.11431, concl. POUSSIERE
- *D*. 1960.157, note R. SAVATIER

CE, Sect., 11 février 1972, *M*. *Crochette*, n°76799, *Rec*. *Lebon*

- *R.D*. *publ*. 1972.959, concl. G. GUILLAUME
- *Dr*. *soc*. 1972.404
- *D*. 1972.426, note M. LE ROY

CE 5/3 SSR, 26 janvier 1979, n°99910

CE 5/3 SSR, 26 janvier 1979, n°99511, *Rec*. *Lebon*

CE Ass., 12 mars 1982, *Conseil national de l'Ordre des médecins*, n°11413, 11414, 11466, 11099, 11100, 11451, *Rec*. *Lebon*

- *R.J.F*. 1982, Comm. n°475, concl. VERNY
- JCP 1982.II.19857, note J. DUFFAR
- Dr. fisc. 1982, Comm. n°1225
- C. DAVID, O. FOUQUET, B. PLAGNET et J.-F. RACINE, Les grands arrêts de la jurisprudence fiscale, 4ème éd. Dalloz, Paris, 2003, n°8.156

CE Ass., 19 mai 1983, *Rec*. *Lebon*

CE, 27 juillet 1984, n°18281

- *RJF* 11/1984, n°693

CE 7/8 SSR, 10 février 1988, n°67016

- *RJF* 4/1988, n°491

CE 8/9 SSR, 1 juin 1994, n°150870, *tables Rec*. *Lebon*

CE 10/7 SSR, 7 juin 1995, n°148659, *Rec*. *Lebon*

- *AJDA* 1996.162, note J. FRAYSSINET

CE 10/7 SSR, 18 février 1998, n°171851

CE 8/9 SSR, 20 janvier 1999, n°181011

- *Méas* : *Procédures* 1999, Comm. n°221, obs. J.-L. PIERRE

CE 4/6 SSR, 8 décembre 2000, n°162995, *Rec*. *Lebon*

- *D*. 2002.615, obs. J.-J. LEMOULAND

CE Sect., 30 octobre 2001, *Association française des sociétés financières*, n°204909

- *Comm*. *Com*. *électr*. 2002, Comm. 79, note A. LEPAGE

CE 3/8 SSR, 7 juillet 2004, n°253711, *Rec*. *Lebon*

- *RJF* 2004, n°102

CE 10/9 SSR, 28 juillet 2004, *M*. *Mechri*, n°262851, *Rec*. *Lebon*

CE réf., 5 septembre 2008, *Sté DirectAnnonces*, n°319071

CE Sect., 31 octobre 2008, n°293785, *Rec*. *Lebon*

CE 10/9 SSR, 27 juillet 2012, n°340026, *Société AIS2*, *Rec*. *Lebon*

- *JCP E*, 2012, n°37.1534, Pan.
- *JCP A*, 2012, n°35, act. 570, note C.-A. DUBREUIL
- *RSC* 2012.614, obs. J. FRANCILLON

CE 2/7 SSR, 17 octobre 2012, n°348440, *Rec*. *Lebon*

- *AJDA* 2013.362, note H. RIHAL
- *JCP A* 2013.2025, note C. VOCANSON
- *RDSS* 2015.440, note E. PECHILLON

CE 10/9 SSR, 9 novembre 2015, n°383313, *inédit au rec*. *Lebon*

- *AJDA* 2016.527

CE 10/9 SSR, 10 avril 2009, n°289793, n°289794, n°289795

- *RDS* 2009, n°30.341, Comm. F. VIALLA,
- *RDSS* 2009.688, F. DIEU

CE 10/9 SSR, 19 juillet 2010, *Fristot et Charpy*, n°334014, *tables Rec*. *Lebon*

CE 10 SSJS, 11 avril 2014, n°348111

CE 10/9 SSR, 11 avril 2014, n°352473, *inédit au Rec*. *Lebon*

CE 1/6 SSR, 22 octobre 2014, n°362681, *inédit au Rec*. *Lebon*

- *AJ pénal* 2014.595, obs. E. PECHILLON
- *RPDP* 2014.891, obs. E. PECHILLON

CE 10/9 SSR, 23 mars 2015, n°353717, *Association Lexeek*, *tables Rec*. *Lebon*

- *Gaz*. *Pal*. 16 avril 2015, n°106.28
- *AJDA* 2015.1398
- *Comm*. *com*. *électr*. 2015, Comm. 52, note A. DEBET

CE 9/10 SSR, 24 juin 2015, n°367288, *Rec*. *Lebon*

CE 10/9 SSR, 12 novembre 2015, n°372121, *Rec*. *Lebon*

- *AJDA* 2015.2175
- *D*. 2015.2382
- *D*. 2016.752, obs. J.-C. GALLOUX et H. GAUMONT-PRAT
- *AJ fam*. 2015.639, obs. A. DIONISI-PEYRUSSE
- *Dr*. *fam*. 2016. Étude 1, J.-R. BINET
- *JCP* 2016.62, note A. MIRKOVIC
- *RTD civ*. 2016.334, obs. J. HAUSER

CE 10 SSJS, 30 décembre 2015, n°376845, *Association Juricom et associés c/ CNIL*

- *Comm*. *com*. *électr*. 2016, Comm. 36, note A. DEBET

CE 10/9 SSR, 4 mai 2016, n°387466, *tables Rec*. *Lebon*

- *Dall*oz *actu*., 10 mai 2016, obs. A. PORTMANN

CE 4SSJS, 27 Janvier 2016, n°392033

CE 10/9 SSR, 8 février 2017, n°393714, *Société JC Decaux*, *tables Rec*. *Lebon*

- AJDA 2017.325

- *JCP A* 2017, act. 125, obs. C. FRIEDRICH
- *RLDI* 2017, n°4961, obs. L. COSTES
- *RLDI* 2017, n°4954, note E. DROUARD et C. MAROLLA
- *CCE* 2017. Comm. 37, note N. METALLINOS
- *Dalloz IP/IT* 2017.286, obs. R. PERRAY et J. UZAN-NAULIN

CE 4/5 SSR, 11 Octobre 2017, n°403576, *tables Rec*. *Lebon*

CE Sect., 17 novembre 2017, n°401212, *Fondation Jérôme Lejeune*

- *AJDA* 2018.428
- *D*. 2018.1033, obs. B. FAUVAQUE-COSSON et W. MAXWELL
- *AJ Fam*. 2017.615, A. DIONISI-PEYRUSSE.

CE, 7 décembre 2017, avis n°393836

- *CCE* 2018, Étude 17, obs. A. DEBET et N. METALLINOS
- *RFDA* 2018.1101, obs. L. CLUZEL-METAYER et E. DEBAETS
- *Dalloz IP/IT* 2018.459, note N. MARTIAL-BRAZ

CE, 21 juin 2018, n°416505, *tables Rec*. *Lebon*

CE 4/1 SSR, 26 septembre 2018, *M. A*.., n°407856 et 410550, *tables Rec*. *Lebon*

- *RDSS* 2018 p.1035

2 - Cours administratives d'appel

CAA Nancy, 12 mai 1999, n°95NC01386

- *AJFP* 1999.23

CAA Nancy, 30 mai 2002, *Centre hospitalier Général Maillot*

- *AJDA* 2003.35, chron. P. ROUSSELLE

CAA Paris, 29 janvier 2003, *AP-HP*

- *Rec. CE* 2003, tables.788

CAA Paris, 30 septembre 2004, n°03PA01769

- *RDS* 2005, n°5.201, obs. F. VIALLA et E. TERRIER
- *RGDM*, n°spécial 2004.89, Comm. N. MALLET-PUJOL
- *LPA* , 19 juin 2002, n°122.19, note N. VIGNAL
- *RDSS* 2012.1074, note J.MORET-BAILLY

CAA Lyon, 4 juillet 2012, n°11LY02325 et n°11LY2326 : JurisData n°2012-014986

- *Gaz*. *Pal*. 13 septembre 2012, n°257.28
- *JCP A* 2012, n°40.2318, note J.-M. BRUGUIERE

3 - Tribunaux administratifs

TA Rennes, 16 janvier 1985

TA Lyon, 28 octobre 2004

- *Gaz*. *Pal*. 14-16 novembre 2004.22, note J.-J. ISRAEL

TA Nice, 9 mars 2007, n°0404779

- *AJDA* 2007.1089, Comm. F. DIEU

TA Besançon, 25 février 2010, n°0900393

- *AJFP* 2010.203.

TA Montreuil, 14 juin 2012, n°1009924

- *AJDA* 2012.1188
- *D*. 2012.1618, obs. A. MIRKOVIC
- *AJ fam*. 2012.408, obs. C. XEMARD

C - Jurisprudence constitutionnelle

Cons. const., 22 janvier 1990, n°89-269 DC

Cons. const., 18 décembre 1997, n°97-393 DC

Cons. const., 12 août 2004, n°2004-504 DC

Cons. const., décembre 22 mars 2012, n°2012-652 DC

- *RLDI* juin 2012, n°2783, obs. L. COSTES
- *AJDA* 2012.623, note R. GRAND
- *Dr. famille* 2012, alerte 29, obs. M. BRUGGEMAN

Cons. const., 16 mai 2012, n°2012-248 QPC

- *AJDA* 2012.1036
- *AJ fam*. 2012.406, obs. F. CHENEDE
- *RDSS* 2012.750, note D. ROMAN
- *RTD civ*. 2012.520, note J. HAUSER

Cons. const., 19 septembre 2014, n°2014-412 QPC

- *AJDA* 2014.1798
- *D*. 2014.1826
- *Com. Comm. électr*., 2015, n°1, Comm. 7, A. DEBET

D - Jurisprudence de l'Union européenne

CJCE, 6 novembre 2003, aff. C-101/01, *Bodil Lindvist*

- *D*. 2004.1062, obs. L. BURGOGUE-LARSEN
- *RSC* 2004.712, obs. L. IDOT
- *Europe*, 2004, Comm. 18, note F. MARIATTE
- *RLDC* janvier 2004.29, note G. MARRAUD DES GROTTES
- *Comm. com. electr*. 2004, Comm. 46, note R. MUNOZ

CJCE, 16 décembre 2008, aff. C-524/06, *Heinz Huber*

- *Rec. CJCE* 2008.I.9705
- *Europe* 2009, Comm. 53, obs. F. KAUFF-GAZIN
- *JCP A* 2009, n°30.2189, obs. M. GAUTIER

CJUE 24 novembre 2011, aff. C-70/10, *Sté Scarlet Extended c/ Société belge des auteurs, compositeurs et éditeur SCRL*

- *D*. 2011.2925, obs. C. MANARA
- *D*. 2012.2343, obs. J. LARRIEU, C. LE STANC et P. TREFIGNY
- *D*. 2012.2836, obs. P. SIRINELLI
- *RSC* 2012.163, obs. J. FRANCILLON
- *RTD eur*. 2012.404, obs. F. BENOIT-ROHMER

- *RTD eur*. 2012.957, obs. E. TREPPOZ
- *Gaz*. *Pal*. 16 février 2012, n°47, note L. MARINO

CJUE, 11 décembre 2014, aff. C-212/13, *František Ryneš c/ Úřad pro ochranu osobních údajů*

- *Comm*. *com*. *électr*. 2015, Comm. 15, note A. DEBET
- *RLDI* janvier 2015, n°3655.30, obs. L. COSTES
- *RLDI* décembre 2015, n°3875.21, note J. UZAN-NAULIN et R. PERRAY

CJUE, 19 octobre 2016, aff. C-582/14, *Breyer c/ Bundesrepublik Deutschland*

- *D*. 2016.2215
- *Dalloz* IP/IT 2017.120, obs. G. PERONNE et E. DAOUD
- *RLDI* 2017, n°4944, note B. PAUTROT
- *CCE* 2016, Comm. 104, note N. METALLINOS
- *Rev*. *int*. *compliance* 2016. Comm. 130, note M. GRIGER et J. SCHWARTZ

Trib. UE, 26 octobre 2011, aff. T-436/2001, *Julien Dufour c/ CBE*

E - Jurisprudence du Conseil de l'Europe

CEDH 24 avril 1990, n°11801/85 et 11105/84, *Kruslin c/ France et Huvig c/ France*

CEDH 16 décembre 1992, n°13710/88, *Niemietz c/ Allemagne*

CEDH 24 octobre 1996, n°15773/89, 15774/89, *Guillot c/ France*

- *RTD civ*. 1997.551, obs. J.-P. MARGUENAUD

CEDH 25 février 1997, n°22009/93, *Z c/ Finlande*

CEDH, 27 août 1997, n°20837/92, *M.S. c/ Suède*

CEDH 6 février 2001, n°44599/98, *Bensaïd c/ Royaume-Uni*

- *JCP G*, 2001.I.342, obs. F. SUDRE

CEDH 14 mai 2002, n°38621/97, *Zehnalova et Zehnal c/ Rép*. *Tchèque*

CEDH 18 mai 2004, n°58148/00, *Edition Plon c/ France*

CEDH 22 février 1994, n°16213/90, *Burghartz c/ Suisse*

CEDH 31 janvier 1995, n°15225/89, *Friedl c/ Autriche*

CEDH 29 avril 2002, n°2346/02, *Pretty c/ Royaume-Uni*

CEDH 17 février 2005, *K.A et A.D c/ Belgique*

- *D*. 2005.2973, chron. M. FABRE-MAGNAN
- *D*. 2006.1200, obs. J.-C. GALLOUX et H. GAUMONT-PRAT
- *RTD civ*. 2005.341, obs. J.-P. MARGUENAUD

CEDH 16 octobre 2008, n°5608/05, *Renolde* c/ *France*

- *AJDA* 2008.1983
- *AJ pénal*.609, obs. J.-P. CERE
- *D*. 2008.2723, obs. M. LENA
- *ibid*. 2009.123, obs. G. ROUJOU DE BOUBEE, T. GARE et S. MIRABAIL
- *ibid*.1376, obs. J.-P. CERE, M. H-EVANS et E. PECHILLON
- *AJ pénal* 2009.41, obs. J.-P. CERE
- *RDSS* 2009.363, obs. P. HENNION-JACQUET
- *RSC* 2009.173, obs. J.-P. MARGUENAUD
- *ibid*. 431, chron. P. PONCELA

CEDH 19 juillet 2012, n°38447/09, *Ketreb c/ France*

- *AJ pénal* 2012.609, obs. J.-P. CERE

CEDH 8 octobre 2015, n°32432/13 *Sellal c/ France*

CEDH, 4 février 2016, n°58828/13, *Isenc c/ France*

- *AJDA* 2016.232
- *D*. 2016.1220, obs. J.-P. CERE, M. H-EVANS et E. PECHILLON
- *AJ pénal* 2016.158, obs. J.-P. CERE

CEDH 8 janvier 2009, *Schlumpf c/ Suisse*

- *AJDA* 2009.872, note. J.-F. FLAUSS
- *RTD civ*. 2009.291, note J.-P. MARGUENAUD

F - Décisions d'autorités administratives indépendantes

1 - Commission d'accès aux documents administratifs

Avis n°20150229, 19 mars 2015

Avis n°20142528, 18 septembre 2014

Avis n°20150229, 19 mars 2015

Avis n°20101534, 22 avril 2010

Avis n°20051366, 31 mars 2005

Avis n°20104684, 21 décembre 2010

2 - Commission nationale de l'informatique et des libertés

Cette liste contient toutes les délibérations qui ont été consultées.

Toutes ne figurent pas dans le corps de la thèse

Délibération n°84-32 du 25 septembre 1984

Délibération n°85-07 du 19 février 1985

Délibération n°85-24 du 25 juin 1985

Délibération n°85-39 du 10 septembre 1985

Délibération n°86-42 du 08 avril 1986

Délibération n°86-112 du 25 novembre 1986

Délibération n°86-123 du 16 décembre 1986

Délibération n°88-46 du 26 avril 1988

Délibération n°88-73 du 21 juin 1988

Délibération n°89-05 du 24 janvier 1989

Délibération n°89-35 du 25 avril 1989

Délibération n°89-51 du 13 juin 1989

Délibération n°89-56 du 27 juin 1989

Délibération n°90-104 du 2 octobre 1990

Délibération n°91-014 du 12 février 1991

Délibération n°92-041 du 7 avril 1992

Délibération n°92-061 du 9 juin 1992

Délibération n° 95-065 du 23 mai 1995

Délibération n°96-014 du 12 mars 1996

Délibération n°96-054 du 18 juin 1996

Délibération n°99-061 du 21 décembre 1999

Délibération n°00-001 du 13 janvier 2000

Délibération n°00-002 du 13 janvier 2000

Délibération n°00-003 du 13 janvier 2000

Délibération n°01-054 du 18 octobre 2001

Délibération n°02-003 du 05 février 2002

Délibération n°2004-081 du 09 novembre 2004

Délibération n°2005-018 du 03 février 2005

Délibération n°2005-024 du 17 février 2005

Délibération n°2005-025 du 17 février 2005

Délibération n°2005-026 du 17 février 2005

Délibération n°2005-027 du 17 février 2005

Délibération n°2005-030 du 17 février 2005

Délibération n°2005-048 du 22 mars 2005

Délibération n°2005-070 du 20 avril 2005

Délibération n°2005-088 du 12 mai 2005

Délibération n°2005-107 du 19 mai 2005

Délibération n°2005-152 du 14 juin 2005

Délibération n°2005-214 du 11 octobre 2005

Délibération n°2005-216 du 11 octobre 2005

Délibération n°2005-229 du 11 octobre 2005

Délibération n°2005-230 du 11 octobre 2005

Délibération n°2005-287 du 22 novembre 2005

Délibération n°2005-303 du 08 décembre 2005

Délibération n°2005-316 du 20 décembre 2005

Délibération n°2006-029 du 02 février 2006

Délibération n°2006-030 du 02 février 2006

Délibération n°2006-067 du 16 mars 2006

Délibération n°2006-203 du 14 septembre 2006

Délibération n°2007-063 du 25 avril 2007

Délibération n°2007-064 du 25 avril 2007

Délibération n°2007-065 du 25 avril 2007

Délibération n°2007-066 du 25 avril 2007

Délibération n°2007-067 du 25 avril 2007

Délibération n°2007-068 du 25 avril 2007

Délibération n°2007-069 du 25 avril 2007

Délibération n°2007-070 du 25 avril 2007

Délibération n°2007-071 du 25 avril 2007

Délibération n°2007-072 du 25 avril 2007

Délibération n°2007-073 du 25 avril 2007

Délibération n°2007-074 du 25 avril 2007

Délibération n°2007-075 du 25 avril 2007

Délibération n°2007-076 du 25 avril 2007

Délibération n°2007-207 du 10 juillet 2007

Délibération n°2007-209 du 10 juillet 2007

Délibération n°2007-235 du 13 septembre 2007

Délibération n°2007-234 du 13 septembre 2007

Délibération n° 2008-004, 10 janvier 2008

Délibération n°2008-079 du 27 mars 2008

Délibération n°2008-099 du 10 avril 2008

Délibération n°2008-100 du 10 avril 2008

Délibération n°2008-139 du 29 mai 2008

Délibération n°2008-140 du 29 mai 2008

Délibération n°2008-142 du 29 mai 2008

Délibération n°2008-198, 9 juillet 2008

Délibération n°2008-203 du 17 juillet 2008

Délibération n°2008-211 du 17 juillet 2008

Délibération n°2008-213 du 17 juillet 2008

Délibération n°2008-218 du 17 juillet 2008

Délibération n°2008-229 du 17 juillet 2008

Délibération n°2008-230 du 17 juillet 2008

Délibération n°2008-231 du 17 juillet 2008

Délibération n°2008-239 du 17 juillet 2008

Délibération n°2008-242 du 17 juillet 2008

Délibération n°2008- 287 du 17 juillet 2008

Délibération n°2008-384 du 6 novembre 2008

Délibération n°2008- 522 du 18 décembre 2008

Délibération n°2009-071 du 29 janvier 2009

Délibération n°2009-056 du 29 janvier 2009

Délibération n°2009-072 du 29 janvier 2009

Délibération n°2009-073 du 29 janvier 2009

Délibération n°2009-074 du 29 janvier 2009

Délibération n°2009-075 du 29 janvier 2009

Délibération n°2009-144 du 26 février 2009

Délibération n°2009-175 du 26 mars 2009

Délibération n°2009-255 du 7 mai 2009

Délibération n°2009-308 du 7 mai 2009

Délibération n°2009-309 du 7 mai 2009

Délibération n°2009-415 du 2 juillet 2009

Délibération n°89-90 du 12 septembre 2009

Délibération n°2009-648 du 26 novembre 2009

Délibération n°2009-649 du 26 novembre 2009

Délibération n°2009-650 du 26 novembre 2009

Délibération n°2010-010 du 28 janvier 2010

Délibération n°2010-011 du 28 janvier 2010

Délibération n°2010-012 du 28 janvier 2010

Délibération n°2010-013 du 28 janvier 2010

Délibération n°2010-014 du 28 janvier 2010

Délibération n°2010-031 du 4 février 2010

Délibération n°2010-034 du 11 février 2010

Délibération n°2010-090 du 8 avril 2010

Délibération n°2010-092 du 8 avril 2010

Délibération n°2010-108 du 22 avril 2010

Délibération n°2010-129 du 20 mai 2010

Délibération n°2010-260 du 24 juin 2010

Délibération n°2010-284 du 15 juillet 2010

Délibération n°2010-285 du 15 juillet 2010

Délibération n°2010-286 du 15 juillet 2010

Délibération n°2010-287 du 15 juillet 2010

Délibération n°2010-288 du 15 juillet 2010

Délibération n°2010-289 du 15 juillet 2010

Délibération n°2010-317 du 22 juillet 2010

Délibération n°2010-318 du 22 juillet 2010

Délibération n°2010-319 du 22 juillet 2010

Délibération n°2010-320 du 22 juillet 2010

Délibération n°2010-359 du 30 septembre 2010

Délibération n°2010-362 du 30 septembre 2010

Délibération n°2011-002 du 13 janvier 2011

Délibération n°2011-006 du 13 janvier 2011

Délibération n°2011-008 du 13 janvier 2011

Délibération n°2011-011 du 13 janvier 2011

Délibération n°2011-021 du 20 janvier 2011

Délibération n°2011-044 du 10 février 2011

Délibération n°2011-049 du 17 février 2011

Délibération n°2011-035, 17 mars 2011

- *CCE* 2012. Étude 1, obs. A. DEBET

Délibération n°2011-100 du 14 avril 2011

Délibération n°2011-101 du 14 avril 2011

Délibération n°2011-196 du 30 juin 2011

Délibération n°2011-238, 12 juillet 2011

- *Comm. com. électr*. 2011, Comm. 115, obs. A. LEPAGE

Délibération n°2011-328 du 18 octobre 2011

Délibération n°2012-036 du 2 février 2012

Délibération n°2012-056 du 16 février 2012

Délibération n°2012-061du 8 mars 2012

Délibération n°2012-145 du 2 mai 2012

Délibération n°2012-146 du 2 mai 2012

Délibération n°2012-162 du 24 mai 2012

Délibération n°2012-181 du 31 mai 2012

Délibération n°2012-182 du 31 mai 2012

Délibération n°2012-189 du 7 juin 2012

Délibération n°2012-190 du 7 juin 2012

Délibération n°2012-220 du 5 juillet 2012

Délibération n°2012-228 du 5 juillet 2012

Délibération n°2012-239 du 12 juillet 2012

Délibération n°2012-263 du 19 juillet 2012

Délibération n°2012-274 du 19 juillet 2012

Délibération n°2012-276 du 19 juillet 2012

Délibération n°2012-278 du 19 juillet 2012

Délibération n°2012-280 du 19 juillet 2012

Délibération n°2012-284 du 19 juillet 2012

Délibération n°2012-317 du 13 septembre 2012

Délibération n°2012-318 du 13 septembre 2012

Délibération n°2012-319 du 13 septembre 2012

Délibération n°2012-343 du 27 septembre 2012

Délibération n°2012-344 du 27 septembre 2012

Délibération n°2012-345 du 27 septembre 2012

Délibération n°2012-346 du 27 septembre 2012

Délibération n°2012-347 du 27 septembre 2012

Délibération n°2012-348 du 27 septembre 2012

Délibération n°2012-350 du 27 septembre 2012

Délibération n°2012-359 du 4 octobre 2012

Délibération n°2012-360 du 4 octobre 2012

Délibération n°2012-371 du 11 octobre 2012

Délibération n°2012-372 du 11 octobre 2012

Délibération n°2012-373 du 11 octobre 2012

Délibération n°2012-421 du 29 novembre 2012

Délibération n°2012-425 du 29 novembre 2012

Délibération n°2012-428 du 29 novembre 2012

Délibération n°2013-004 du 10 janvier 2013

Délibération n°2013-007 du 10 janvier 2013

Délibération n°2013-013 du 10 janvier 2013

Délibération n°2013-046 du 28 février 2013

Délibération n°2013-048 du 28 février 2013

Délibération n°2013-050 du 28 février 2013

Délibération n°2013-084 du 28 mars 2013

Délibération n°2013-096 du 25 avril 2013

Délibération n°2013-099 du 25 avril 2013

Délibération n°2013-100 du 25 avril 2013

Délibération n°2013-101 du 25 avril 2013

Délibération n°2013-102 du 25 avril 2013

Délibération n°2013-103 du 25 avril 2013

Délibération n°2013-111 du 25 avril 2013

Délibération n°2013-125 du 16 mai 2013

Délibération n°2013-126 du 16 mai 2013

Délibération n°2013-127 du 16 mai 2013

Délibération n°2013-143 du 30 mai 2013

Délibération n°2013-155 du 6 juin 2013

Délibération n°2013-157 du 6 juin 2013

Délibération n°2013-181 du 27 juin 2013

Délibération n°2013-250 du 12 septembre 2013

Délibération n°2013-251 du 12 septembre 2013

Décision n°2013-037, 25 septembre 2013

Délibération n°2013-285 du 10 octobre 2013

Délibération n°2013-373 du 28 novembre 2013

Délibération n°2013-373 du 28 novembre 2013

Délibération n°2013-405 du 19 décembre 2013

Délibération n°2014-041, 29 janvier 2014

Délibération n°2014-077 du 13 mars 2014

Délibération n°2014-078 du 13 mars 2014

Délibération n°2014-084 du 13 mars 2014

Délibération n°2014-114 du 27 mars 2014

Délibération n°2014-117 du 27 mars 2014

Délibération n°2014-118 du 27 mars 2014

Délibération n°2014-119 du 27 mars 2014

Délibération n°2014-135 du 3 avril 2014

Délibération n°2014-138 du 3 avril 2014

Délibération n°2014-139 du 3 avril 2014

Délibération n°2014-149 du 17 avril 2014

Délibération n°2014-182 du 6 mai 2014

Délibération n°2014-238 du 12 juin 2014

Délibération n°2014-302 du 10 juillet 2014

Délibération n°2014-441 du 23 octobre 2014

Délibération n°2014-533 du 18 décembre 2014

Délibération n°2014-534 du 18 décembre 2014

Délibération n°2014-536 du 18 décembre 2014

Délibération n°2014-537 du 18 décembre 2014

Délibération n°2014-539 du 18 décembre 2014

Délibération n°2015-029 du 22 janvier 2015

Délibération n°2015-031 du 22 janvier 2015

Délibération n°2015-032 du 22 janvier 2015

Délibération n°2015-035 du 22 janvier 2015

Délibération n°2015-092 du 19 mars 2015

Délibération n°2015-094 du 19 mars 2015

Délibération n°2015-161 du 28 mai 2015

Délibération n°2015-174 du 11 juin 2015

Délibération n°2015-212 du 2 juillet 2015

Délibération n°2015-218 du 2 juillet 2015

Délibération n°2015-223 du 2 juillet 2015

Délibération n°2015-224 du 2 juillet 2015

Délibération n°2015-255, 16 juillet 2015

Délibération n°2015-288 du 10 septembre 2015

Délibération n°2016-028 du 11 février 2016

Délibération n°2016-043 du 18 février 2016

Délibération n°2016-045 du 18 février 2016

Délibération n°2016-142 du 12 mai 2016

Délibération n°2016-058 du 30 juin 2016

Délibération n°2016-083 du 26 septembre 2016

Délibération n°2016-325 du 3 novembre 2016

Délibération n°2016-394 du 15 décembre 2016

Délibération n°2017-013 du 19 janvier 2017

Délibération n°2017-014 du 19 janvier 2017

Délibération n°2017-028 du 16 février 2017

Délibération n°2017-056 du 9 mars 2017

Délibération n°2017-174 du 1er juin 2017

Délibération n°2017-299 du 30 novembre 2017

Délibération n°2017-311 du 7 décembre 2017

Délibération n°2017-330 du 14 décembre 2017

Délibération n°2018-013 du 25 janvier 2018

Délibération n°2018-050 du 15 février 2018

Délibération n°2018-121 du 5 avril 2018

Délibération n°2018-145 du 3 mai 2018

Délibération n°2018-150 du 3 mai 2018

Délibération n°2018-152 du 3 mai 2018

Délibération n°2018-155 du 3 mai 2018

Délibération n°SAN-2018-002 du 7 mai 2018

Délibération n°2018-295 du 19 juillet 2018

Délibération n°SAN-2018-010 du 6 septembre 2018

Délibération n°2018-354 du 13 décembre 2018

Délibération n°2019-001 du 21 janvier 2019

- *Dalloz act.* 28 janvier 2019, obs. N. MAXIMIN ;
- *Dalloz IP/IT* 2019. 165, obs. E. NETTER ;
- *CCE* 2019. Comm. 32 et 43, obs. N. METALLINOS ;
- *JCP E* 2019. 1059, note J. DEROULEZ.

Délibération n°2019-008 du 31 janvier 2019

G - Décisions du Conseil national de l'Ordre des médecins

CDNOM, 2 décembre 2008, disponible en ligne sur : https://www.legalis.net/jurisprudences/ordre-des-medecins-dile-de-france-chambre-disciplinaire-de-1ere-instance-decision-du-02-decembre-2008/ (dernière consultation le 12 septembre 2019).

H - Jurisprudence étrangère

Tribunal constitutionnel federal d'Allemagne.

Bundesverfassungsgericht, 15 décembre 1983, BVerfGE 65, 1.

INDEX ALPHABETIQUE

(Les nombres renvoient aux numéros de paragraphes)

TABLE DES MATIERES

Le secret médical et les technologies de l'information et de la communication

Tout aurait été dit à propos du « secret médical ». Les disputes doctrinales relatives au fondement du secret professionnel se seraient taries puisqu'il serait désormais délimité par le seul intérêt du malade, ce qui expliquerait par ailleurs la généralisation du secret professionnel à l'ensemble des personnes intervenant dans le sytème de santé. Pourtant, lorsqu'il s'agit d'interroger le rapport entre les technologies de l'information et de la communication et le « secret médical » le discours de la doctrine maque de clarté. Les uns prédisent la disparition du « secret médical », les autres son renforcement. Quel est l'impact des techniques de l'information et de la communication sur le « secret médical » ? La question mérite d'être posée en explorant des cadres d'analyse différents car l'absence de distinction entre le nom de la notion et les notions qu'elle désigne et l'illusion d'une notion unitaire masquent la question épistémologique : Cette dernière consiste à savoir ce que révèle le mouvement de fond qui fait pressentir que le « secret médical » est à la fois « protégé » par le droit et « atteint » par les techniques de l'information et de la communication. La définition classiquement admise de la notion de « secret médical » constitue un écran qui le rende difficilement perceptible.

Medical secrecy and information and communications technologies

Is there something to add about "medical secrecy"? Scholar disputes over the professional secrecy foundations are supposed to be dried up, since it is now limited to the patient's interest alone, which would explain the generalization of medical secrecy to all persons of the care system. Yet, when it comes to the matter of the relationship between information and communications technologies and medical secrecy, the scholar discourse suffer from a lake of clarity. Some will predict the end of "medical secrecy", while the others foresee its strengthening. What is the impact of the information and communications technologies on the "medical secrecy"? It is a question worth asking by exploring different analytical frameworks, because the absence of distinction between how the notion is called and what notions it refers to, as well as the illusion of a unitary notion, hide the epistemological issue. The latter is about studying the structural movement according to which the medical secrecy is at the same time "protected" by Law and "affected" by the information and communications technologies. The classical definition of the notion of "medical secrecy" is a veil making it hardly discernible.