La circulation de la donnée à caractère personnel relative à la santé : disponibilité de l'information et protection des droits de la personne

Renatto Brasselet

UNIVERSITÉ DE LORRAINE | INSTITUT FRANÇOIS GÉNY
FACULTÉ DE DROIT SCIENCES ÉCONOMIQUES & GESTION DE NANCY
École doctorale Sciences Juridiques, Politiques, Économiques et de Gestion

LA CIRCULATION DE LA DONNEE A CARACTERE PERSONNEL RELATIVE A LA SANTE

DISPONIBILITE DE L'INFORMATION ET PROTECTION DES DROITS DE LA PERSONNE

Thèse

En vue de l'obtention du grade de

Docteur en Droit

(Doctorat nouveau régime - Droit privé et Sciences criminelles)

Présentée et soutenue publiquement le 3 décembre 2018 par

Renato BRASSELET

Devant le jury de *soutenance composé de :*

Directeur de recherches :	Bruno PY Professeur de Droit privé à l'Université de Lorraine
Suffragants :	François VIALLA Professeur de Droit privé à l'Université de Montpellier (Rapporteur)
	Marion GIRER Maître de conférences de Droit privé à l'Université de Lyon 3 (Rapporteur)
	Sophie HOCQUET-BERG Professeur de droit privé à l'université de Lorraine
	Florence EON Directrice du service juridique ASIP Santé

La Faculté n’entend donner ni approbation ni improbation aux opinions émises dans cette thèse, celles-ci devant être considérées comme propres à leur auteur.

À la mémoire de Catherine Courtault.

Remerciements

« Il n'y a pas de création sans épreuve. »

Fernand Ouellette

Cette thèse a été pour moi une épreuve personnelle et professionnelle mais avant tout une riche expérience humaine. Elle m'a appris beaucoup sur moi-même et sur les autres. J'en garderai, malgré les difficultés rencontrées, d'agréables souvenirs et de véritables ami(e)s. Elle représente également l'opportunité de dire merci à toutes les personnes qui ont contribué, tout au long de mon parcours, à la réussite de mes études et, par-dessus tout, à l'ouverture de mon esprit au monde, à notre société, aux autres et, aux questions qui les concernes.

« Il n'y a guère au monde un plus bel excès que celui de la reconnaissance. »

Jean De La Bruyère

Merci à Mme Catherine Penin enseignante d'histoire géographie au Lycée Louis Majorelle d'avoir la première crue en mes capacités et de m'avoir incité à me dépasser et à poursuivre mes études.

« Dans une famille unie tous ont en vue l'avantage de tous, parce que tous s'aiment et que tous ont part au bien commun. Il n'est pas un de ses membres qui n'y contribue d'une manière diverse selon sa force, son intelligence, ses aptitudes particulières : l'un fait ceci, l'autre cela, mais l'action de chacun profite à tous, et l'action de tous profite à chacun. »

Félicité Robert de Lamennais, Le livre du peuple 1838

Je remercie profondément mes parents pour leur dévouement, pour m'avoir également transmis leur angoisse et surtout pour m'avoir supporté mais aussi aidé à veiller sur mon indispensable source de distraction et de bonheur, mon fils Louca.

Je remercie également aux autres membres de ma famille, à mes ami(e)s, à mes collègues de m'avoir soutenu et de m'avoir rappelé, tout au long de ce travail, qu'il fallait être fou pour se lancer dans une telle entreprise.

Une pensée pour mon grand-père, Altiero Guardiera qui nous a quittés le 17 août 2018.

Une pensée particulière pour ceux qui ne sont plus et, qui ont contribué, en un sens, à la réalisation de cette thèse :

- Pour Catherine et Jean-Pol Courtault sans qui je ne me serais jamais engagé sur ce chemin, je vous remercie pour votre passion contagieuse pour le droit et la santé ainsi que pour tant d'autres choses.
- Pour Madame le Professeur Nathalie Loewenguth Deffains qui en raison de la richesse de ses cours et malgré sa vélocité a su susciter mon intérêt pour le Droit européen des droits de l'homme, je dis merci.

Une pensée également pour ceux qui m'ont précédé et qui ont contribué à mon éveil en tant que juriste, Bertrand Marrion, Caroline Zorn et Céline Breton dont j'ai lu et relu les travaux, Jean-Philippe Vauthier, et enfin à Julie Leonhard qui est devenue au fil des années une véritable amie, merci.

Je tiens également à remercier tout particulièrement Valérie Olech et Julien Risseur, nos échanges furent intéressants et votre aide précieuse.

Je remercie également Charlène Collet, Elaine Bucki, Mélodie Peltier-Henry, Mathieu Martinelle, sans eux je n'aurais pas pu atteindre ce but.

Enfin, je remercie Monsieur Jonathan Lotz Directeur d'Alsace e-santé envers qui je suis également reconnaissant de m'avoir donné les moyens de m'épanouir et de me dépasser professionnellement ainsi que de m'avoir laissé le temps nécessaire à la bonne réussite de mon doctorat.

Remerciements aux membres du jury

Je tiens à remercier chaleureusement Monsieur le Professeur Bruno PY, pour son constant soutien face aux obstacles qui se sont présentés tout au long de cette thèse. Sans ses précieux conseils et son aide, je n'aurai jamais pu mener ce travail à son terme. Il a été pour moi plus qu'un Directeur de thèse, un véritable bienfaiteur. Je lui en suis profondément reconnaissant.

Je tiens tout particulièrement à remercier, Madame le Professeur Sophie Hocquet-Berg d'avoir accepté initialement de codiriger ma thèse et d'avoir bien voulu accepter d'en apprécier le résultat.

Je remercie Monsieur le Professeur François Vialla ainsi que Madame Marion Girer, Maître de conférences habilité à diriger des recherches, d'avoir acceptés de participer à mon jury de thèse en qualité de rapporteur de mon travail.

Je remercie également Madame Florence Eon, Directrice du service juridique de l'Asip Santé pour l'intérêt qu'elle a manifesté à l'égard de mon travail en acceptant de participer en qualité de membre invité à ce jury.

Liste des principales abréviations

AAI	Autorité administrative indépendante
ABM	Agence de la biomédecine
AFHADS	Association Française des Hébergeurs Agréés de Données de Santé à Caractère Personnel
Al.	Alinéa
ALD	Affections de longue durée
ANAP	Agence Nationale d'Appui à la Performance
ANSM	Agence nationale de sécurité du médicament et des produits de santé
ANSP	Agence nationale de santé publique
ANSSI	Agence nationale de sécurité des systèmes d'information
APA	Allocation personnalisée d'autonomie
APL	Aide personnalisée au logement
AR	Accusé de réception+
ARH	Agence régionale d'hospitalisation
ARS	Agence régionale de santé
Art.	Article
ASIP Santé	Agence des systèmes d'information partagés de santé
ASN	Autorité de sûreté nucléaire
BayLDA	« Bayerisches Landesamt für Datenschutzaufsicht » (autorité bavaroise de protection des données)
BCR	Binding corporate rules
Bull.	Bulletin
C. ass.	Code des assurances
CA	Cour d'appel
CAH	Comité d'agrément des hébergeurs de données de santé à caractère personnel
CASF	Code de l'action sociale et des familles
Cass.	Cour de cassation

Cass. crim.	Cour de cassation, chambre criminelle
CCAS	Centre communal d'action sociale
CCMSA	Caisse centrale de la mutualité agricole
CDCJ	Comité européen de coopération juridique
CE	Conseil d'État
CEDH	Cour européenne des droits de l'Homme
CEI	Commission électrotechnique internationale
Ch. com.	Chambre commerciale
CHU	Centre hospitalier universitaire
CJCE	Cour de justice des Communautés européennes
CLIC	Centre local d'information et de coordination
CLIS	Classe pour l'inclusion scolaire
CME	Commission/Conférence médicale d'établissement
CMU	Couverture maladie universelle
CNDCH	Commission Nationale Consultative des Droits de l'Homme
CNIL	Commission nationale de l'informatique et des libertés
CNOM	Conseil national de l'Ordre des médecins
CNRSI	Caisse nationale du régime social des indépendants
CNSA	Caisse nationale de solidarité pour l'autonomie
Cofrac	Comité français d'accréditation
cons.	Considérant
Cons. const.	Conseil Constitutionnel de la République Française
Cons. UE	Conseil de l'Union européenne
Conv. EDH	Convention européenne des droits de l'Homme
CPI	Code de la propriété intellectuelle
CSS	Code de la sécurité sociale

DC	Contrôle de constitutionnalité des lois ordinaires
DGS	Direction générale de la Santé
DGOS	Direction générale de l'offre de soins
Dir.	Directive
DME	Dossier médical électronique
DMP	Dossier médical personnel devenu Dossier médical partagé depuis la LOI n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé
DP	Dossier pharmaceutique
DPD	Délégué à la protection des données
DPO	Data protection officer
DREES	Direction de la recherche, des études, de l'évaluation et des statistiques
DRH	Directeur/ Direction des ressources humaines
DS	Direction des soins
DSI	Directeur/ Direction des systèmes d'information
DSSIS	Délégation à la stratégie des systèmes d'information de santé
EGB	Échantillon généraliste des bénéficiaires
EFS	Établissement français du sang
EHPAD	Établissement d'hébergement pour personnes âgées dépendantes
ESMS	Établissements et services sociaux et médico-sociaux
Etc.	Et cetera desunt (et le reste est omis)
FAI	Fournisseur d'accès Internet
Fehap	Fédération des établissements hospitaliers et d'aide à la personne privés non lucratifs
FHF	Fédération hospitalière de France
FHP	Fédération de l'hospitalisation privée
FNORS	Fédération nationale des observatoires de santé
FSSI	Fonctionnaire de la sécurité des systèmes d'information
G29	Groupe de travail de l'Article 29 sur la protection des données

GCSMS	Groupement de coopération sociale et médico-sociale
HAD	Hospitalisation à domicile
HAS	Haute Autorité de santé
HCAAM	Haut conseil pour l'avenir de l'assurance maladie
HDS	Hébergement de données de santé
HFDS	Haut fonctionnaire de défense et de sécurité
Ibid.	Ibidem (même référence)
ICANN	Internet Corporation for Assigned Names and Numbers (Société pour l'attribution des noms de domaine et des numéros sur Internet)
IDS	Institut des données de santé
IEHEI	Institut européen des hautes études internationales
INCa	Institut national du cancer
INDS	Institut National des Données de Santé
INED	Institut national d'études démographiques
INSERM	Institut national de la santé et de la recherche médicale
InVS	Institut national de veille sanitaire
IP	Internet protocol (Protocole Internet)
IRDES	Institut de recherche et de documentation en économie de la santé
IRSN	Institut de radioprotection et de sûreté nucléaire
ISO	Organisation internationale de normalisation
JONC	Journal officiel (numéro complémentaire)
JORF	Journal officiel de la République française
JOUE	Journal officiel de l'Union européenne
LGDJ	Librairie générale de droit et de jurisprudence
LFSS	Loi de financement de la Sécurité sociale
LIR	Local internet registry (registre Internet local)
MAIA	Méthode d'action pour l'intégration des services d'aide et de soins dans le champ de l'autonomie

MAN	Metropolitan Area Network (réseau informatique métropolitain)
MCAS	Ministères chargés des affaires sociales
MCI	Mission commune d'information
MCO	Médecine, chirurgie, obstétrique
MIPS	Menaces Informatiques et Pratiques de Sécurité
MR	Méthodologie de référence
NCP	Nouveau Code pénal
NIS	Network Information Security (sécurité des réseaux informatiques)
NIR	Numéro d'inscription au répertoire
OMS	Organisation mondiale de la Santé
ONG	Organisation non gouvernementale
OFDT	Observatoire français des drogues et toxicomanies
ORS	Observatoire régional de santé
PAERPA	Personnes âgées en risque de perte d'autonomie
Paragr.	Paragraphe
PAS	Plan d'assurance sécurité
PCA	Plan de continuité d'activité
PCH	Prestation compensatrice du handicap
PE	Parlement européen
PGSSI-E	Politique générale de sécurité des systèmes d'information de l'État
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
PIA	Privacy impact assessment (Étude d'impact sur la vie privée)
PMSI	Programme de médicalisation des systèmes d'information
PSSI	Politique de sécurité des systèmes d'information
PSSI-MCAS	Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales
PTA	Plateforme territoriale d'appui
RDSS	Revue de droit sanitaire et social

Règl.	Règlement
RGPD	Règlement 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 (Règlement général sur la protection des données)
RH	Ressources humaines
RIPE NCC	Réseau internet protocol européen network coordination center (Réseaux de protocole Internet Européens – Centre de coordination de réseau)
RSSI	Responsable de la sécurité des systèmes d'information
SAFARI	Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus
SAAD	Services d'Aide et d'Accompagnement à Domicile
SGMAS	Secrétariat général des ministères chargés des affaires sociales
SI	Système d'information
SIRHEN	Système d'information de gestion des Ressources Humaines et des moyens
SNDS	Système national des données de santé
SNES	Syndicat national des enseignements de second degré
SNIIRAM	Système national d'information inter-régimes de l'Assurance maladie
SNITEM	Syndicat National de l'Industrie des Technologies Médicales
SPASAD	Service Polyvalent d'Aide et de Soins à Domicile
SRI	Sécurité des Réseaux Informatiques
SSIAD	Service de soins infirmiers à domicile
SSI	Sécurité des systèmes d'information
SSR	Soins de suite et de réadaptation
SYNTEC numérique	Syndicat professionnel des entreprises de services du numérique
TFUE	Traité sur le fonctionnement de l'Union européenne
TGI	Tribunal de grande instance

TIC	Technologies de l'information et de la communication
UE	Union européenne
URPS	Union régionale des professionnels de santé
Vol.	Volume
Web	World Wide Web
WAN	Wide area network ou réseau informatique étendu
WP	Working party

Sommaire

INTRODUCTION GENERALE

« Tout secret est, par nature, un obstacle à la libre circulation de l'information »[1]

Bruno PY

1. **De la circulation et du secret.** La donnée à caractère personnel relative à la santé constitue une donnée sensible. Sa circulation résulte d'un processus historique de recherche d'équilibre entre des intérêts qui, de prime abord, peuvent paraître antagonistes. Le secret professionnel est perçu comme un obstacle à la libre circulation de l'information relative à la santé. Il constitue davantage un instrument de régulation.

2. Avec le développement des technologies de l'information et de la communication, d'autres moyens de régulation ont émergés. La protection des données à caractère personnel et, plus particulièrement, la protection de leur contenu informationnel constitue une préoccupation constante de notre société de l'information. Nous cherchons à nous défendre contre les immixtions de tiers dans notre vie privée mais n'hésitons pas à la marchander, consciemment ou inconsciemment et, à publier sur les réseaux sociaux, des informations relatives à notre vie privée susceptibles de nous porter préjudice[2]. Il en est de même concernant nos données les plus sensibles, voir les plus intimes. Aussi, bien que cela semble paradoxal, pour traiter de la circulation de la donnée de santé il convient, après avoir

[1] B. PY, « Réquisitoire contre l'expression de secret médical : plaidoyer pour l'expression de secret professionnel », *Revue Droit &droit Santé*, hors-série n°50, 2013, p. 161.

[2] E. Peres, *Les données numériques : un enjeu d'éducation à la citoyenneté*. Rapport du CESE, janvier 2015, p. 46. Voir également : CNCDH, *Avis sur la protection de la vie privée à l'ère du numérique*. 22 mai 2018.

défini les termes de ce sujet, d'analyser au préalable, les causes et conséquences de sa régulation dans un processus historique.

3. **De la lumière et de l'information.** La comparaison entre la lumière et l'information pourrait paraitre hasardeuse, pourtant, avec l'arrivée du LI-FI[3], cette approche nous semble d'actualité et exprimer le mieux la difficulté rencontrée par la doctrine pour appréhender cette notion[4]. Le terme, *information,* a pour racine latine *informatio* dont le radical est *informatum* et, est employé ordinairement dans son sens générique afin de décrire un élément de connaissance ou encore l'action de renseigner. Eu égard à leur nature, l'information et la lumière présentent des similitudes.

4. **P**our la mécanique quantique, *« la lumière est bien connue pour présenter deux aspects complémentaires selon la façon dont on l'étudie. La lumière est à la fois un phénomène ondulatoire, […] et un phénomène corpusculaire, comme en témoignent les photon. »*[5] Elle est à la fois onde et particule, c'est dire tangible et intangible.

5. Pour le droit, l'information présente des particularités similaires ce qui rend sa définition difficile. De nature duale, elle peut être à la fois immatérielle et matérielle lorsqu'elle est captée par un dispositif ou que l'individu en saisie le sens et la retranscrit sur un support. Elle peut également être brute mais aussi significative si elle est considérée dans un ensemble donné. Elle peut être appropriable et insusceptible d'appropriation[6]. Il résulte invariablement de sa captation, un élément de

---

[3] « *L'acronyme Li-Fi assemble les mots anglais light, pour lumière, et fidelity, pour fidélité. Cette technologie consiste à utiliser la modulation de lumière à haute fréquence pour coder et transmettre des informations. »* Source Futura Tech (https://www.futura-sciences.com/tech/definitions/internet-li-fi15685/)

[4] A. R. Bertrand. *Informations, données, bases de données*. Dalloz. 2010.

[5] Disponible à l'adresse suivante : https://www.astronomes.com/le-big-bang/dualite-onde-particule

[6] I. DE LAMBERTERIE, *« Qu'est-ce qu'une donnée de santé? »*, RGD méd., numéro spécial "Le droit des données de santé", LÉH, 2004, pp. 11-34.

connaissance, un message qui contient une valeur-ajoutée. Cette dualité à des incidences sur le régime juridique de protection applicable. Nous envisageons dans nos travaux, l'information à la fois dans sa matérialité et son immatérialité. Il s'agit par l'emploie de ce vocable de considérer le contenu informationnel, l'élément de connaissance, quel qu'en soit le support.

6. **De l'information nominative à la donnée à caractère personnel** La loi de 1978 utilisait le terme information nominative en lieu et place de celui-ci de donnée à caractère personnel. Ainsi, son article 4 disposait « *sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelques forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent que le traitement soit effectué par une personne physique ou par une personne morale. »*[7]

7. La loi du 6 août 2004[8] reprenant les dispositions de la directive de 1995 afin de modifier la loi de 1978 a substitué au terme information nominative celui de donnée à caractère personnel. le règlement 2016/679 du 27 avril 2016 abrogeant la directive de 1995, définie la donnée 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*

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

[8] 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

physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». [9]

8. **De la notion de donnée.** La notion, donnée, regroupe des acceptations différentes entretenant un certain flou terminologique. Le plus souvent, ce terme est utilisé en opposition avec l'information considérée en tant qu'élément de connaissance. Ce terme peut également être employé pour désigner la transcription de l'information analogique sous une forme numérique c'est-à-dire composée de chiffres, de caractère spéciaux, d'espaces afin que celle-ci soit exploitable dans un système informatique. La donnée est ainsi traitée sur un support informatique physique. Par association d'idées, la donnée peut également être comparée, à une particule élémentaire qui constitue, le plus petit objet physique connu. Ainsi, elle constituerait une information réduite à sa plus petite forme, une donnée brute. Toutefois, la directive de 1995 puis, le règlement 2016/679 du 27 avril 2016 définissent, juridiquement, la donnée à caractère personnel en ayant recours au terme information[10] L'emploi de ce terme pour définir la donnée et l'utilisation indifférenciée des deux vocables par les textes, démontre que la donnée n'est pas considérée par le droit comme étant de nature différente de l'information.

9. Nous envisageons dans nos développements l'information et la donnée comme constituant toutes deux un élément de connaissance qui, lorsqu'il permet directement ou indirectement d'identifier la personne, doit être considéré comme présentant un caractère personnel. Nous opérons toutefois dans nos travaux, une distinction quant à leur forme. Ainsi, à la

[9] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libr1e circulation de ces données, art. 4. JOUE n° L 119, 4 mai 2016.

[10] *V. supra n°3*

différence de l'information, la donnée sera considérée comme possédant « *une valeur ajoutée d'ordre technologique* »[11].

10. **De la donnée de santé.** Sous la directive de 1995, la donnée à caractère personnel relative à la santé ne faisait pas l'objet de définition textuelle. Les responsables de traitement qu'ils soient ou non d'acteurs du monde de la santé, devaient définir seuls si les traitements qu'ils mettaient en œuvre portaient sur de la donnée de santé. Cette situation était source d'insécurité juridique. Ainsi, la définition de la donnée de santé était de nature prétorienne est dépendait des circonstances de l'espèce. La Commission européenne a ainsi proposé au Parlement et au Conseil de l'Union européenne de définir au sein du règlement général sur la protection des données[12] la donnée à caractère personnel relative à la santé. Le règlement 2016/679 ne reprend que quelques éléments de la santé telle qu'elle a été définie en 1946 par l'OMS dans le préambule de sa constitution. Il envisage ainsi le bien-être mais il exclue les informations d'ordre social de sa définition.

> *« La santé est un état de complet bien-être physique, mental et social, et ne consiste pas seulement en une absence de maladie ou d'infirmité. »*[13]

11. Ainsi, les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou

---

[11] I. DE LAMBERTERIE, *« Qu'est-ce qu'une donnée de santé? »*, RGD méd., numéro spécial *"Le droit des données de santé"*, LÉH, 2004, pp. 11-34, p.13.

[12] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libr1e circulation de ces données, art. 4 et considérant 35 JOUE n° L 119, 4 mai 2016.

[13] Préambule à la Constitution de l'Organisation Mondiale de la Santé, 1946.

future, 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. La qualification de la donnée à caractère personnel relative à la santé étant déterminante du champ de compétence *ratione materiae* de la réglementation relative à la protection de la donnée et des droits de la personne, nous reviendrons, un peu plus tard, dans nos développements sur le contenu de cette donnée et sur les modalités de sa protection.

12. **De la circulation et de l'information.** La circulation désigne l' *« action de se mouvoir d'une manière continue, circulairement, avec retour au point de départ »*[14]. Nous employons ce terme afin de désigner l'action de mouvoir l'information d'une manière continue au sein d'un système d'information[15].

13. Cette notion regroupe à la fois l'échange unidirectionnel et bidirectionnel ainsi que le partage licite ou illicite d'informations entre plusieurs personnes intervenant au sein du système de santé mais aussi avec des personnes étrangères au système de santé. Elle implique également le traitement de données à caractère personnel entendue comme *« 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,*

[14] Définition issue du CNITRL (http://www.cnrtl.fr/definition/circulation). Créé en 2005 il constitue un ensemble de ressources linguistiques informatisées unifiées.

[15] Un système d'information est défini comme *« un ensemble de ressources (personnel, logiciels, processus, données, matériels, équipements informatique et de télécommunication...) permettant la collecte, le stockage, la structuration, la modélisation, la gestion, la manipulation, l'analyse, le transport, l'échange et la diffusion des informations (textes, images, sons, vidéo...) au sein d'une organisation. »*. Source Encyclopedia Universalis (https://www.universalis.fr/encyclopedie/systemes-informatiquesconception-architecture-et-urbanisation-des-systemes-d-information/#i_9303)

l'organisation, la structuration, la conservation, l'adaptation ou la modification. »[16]

14. **De la disponibilité de l'information.** La libre disposition des biens est régie par le Code civil au sein du livre III qui concerne les différentes manières dont on acquiert la propriété. L'article 2059 du Code civil dispose ainsi que, *« toutes personnes peuvent compromettre sur les droits dont elles ont la libre disposition. »* L'information et la donnée à caractère personnel bien qu'elles n'échappent pas à toute valorisation[17] relèvent des droits de la personnalité. En raison de leur consubstantialité avec la personne humaine, elles ne peuvent, en l'état de la réglementation, être exclusivement considérées à la lumière du droit de la propriété[18].

15. Le Code de la santé publique reconnait aux articles L. 1110-1 et L. 1110-3 l'égal accès aux soins pour tous ainsi que *« la prévention, […] la continuité des soins et la meilleure sécurité sanitaire possible. »*[19]. Le respect de ces droits repose sur une information disponible et de qualité. En l'absence de disponibilité de l'information de santé, les professionnels intervenant dans le système de santé ne bénéficieraient pas des informations indispensables à la délivrance de soins de qualités. Il leur serait également difficile d'assurer des soins continus et longitudinaux, selon les besoins du patient et la sécurité sanitaire serait ineffective. Il en résulte que tout système d'information de santé *« doit garantir la disponibilité des données en fonction des besoins. Le besoin de disponibilité des données de santé et des fonctions d'un système d'information de santé dépend de la finalité de ce système. Selon la disponibilité requise, les réponses possibles sont variées et peuvent être*

---

[16] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libr1e circulation de ces données, art. 4. JOUE n° L 119, 4 mai 2016.

[17] *V. infra n°735*

[18] *Ibid.* Voir également le code de propriété intellectuelle en ce qui concerne la protection de la base de données par le droit de propriété intellectuel ou par le droit suis generis du producteur de la base.

[19] C. santé publ. art. L. 1110-1, *in fine.*

plus ou moins lourdes à mettre en œuvre. Ainsi, un système destiné à assurer des fonctions liées à la production ou à la coordination des soins aura des exigences de disponibilité a priori très supérieures à un système destiné à la recherche médicale.»[20]

16. Nous considérons donc, la disponibilité au sens qui lui est donné par les spécialistes de la sécurité des systèmes d'information. Il s'agit du premier pilier de ce domaine d'activité qui consiste en la mise à disposition contrôlée de l'information. La disponibilité constitue ainsi, la caractéristique d'une information d'être accessible et utilisable par son destinataire autorisé à l'endroit et à l'heure prévue.

17. **Des droits de la personne.** *« 'Les droits de la personnalité font la synthèse de l'individualité et de l'autonomie. Ainsi, un premier élément fédérateur des droits de la personnalité réside dans leur fondement, le respect de la personnalité. Outre cela il présente une valeur commune, celle du droit de contrôle'*[21]*. La doctrine évoque 'une scissiparité du droit'* [21]*, 'un droit unique le droit de la personnalité scindé en un faisceau de droits devenus peu à peu distinct'»*[22].Les droits de la personnalité relèvent des droits extrapatrimoniaux. Il s'agit de droit subjectifs qui impliquent de manière non exhaustive, le droit à la dignité, le droit au respect à la vie privée et à l'intimité, le droit à la santé, le droit à l'autodétermination informationnelle.

18. Le droit à la santé reconnu par l'Organisation mondiale de la Santé (OMS) comme *« la possession du meilleur état de santé qu'il est capable d'atteindre constitue l'un des droits fondamentaux de tout être humain,*

[20] Politique générale de sécurité des systèmes d'information de santé. 21 A. Lepage, *« Droit de la personnalité »*, Rép. civ. 2013, sous n°4.

[21] P. Mallaurie, *Les droits de la personnalité,* Mélanfes offerts à A. Decoq, 2004, éd. Litec, p. 469.

[22] C. BRETON-RAHALI, *Le secret professionnel et l'action médico-sociale*, Thèse, Nancy, 2014, p. 139.

quelles que soit sa race, sa religion, ses opinions politiques, sa condition économique ou sociale. »[23]

19. Les droits de la personne comprennent également, le droit à la protection des données. En raison de son objet et du fait qu'il s'inscrit dans un processus historique est apparu, dans un premier temps, comme une déclinaison du droit au respect de la vie privée. Le considérant n°10 de la directive de 95 rappelait à ce titre, que *« l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire. »*[24] Il constitue désormais un droit autonome entrant dans l'objet de notre étude.

20. **Du droit à la vie privée.** Le droit à la vie privée n'a été reconnu que depuis le XVIIIème siècle[25]. La reconnaissance de sa valeur constitutionnelle est intervenue progressivement. En 1995, le Conseil constitutionnel a été *« appelé à se prononcer sur la constitutionnalité de dispositions encadrant l'installation de systèmes de vidéosurveillance, le Conseil constitutionnel jugera "que la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle.*[26]*" Dans cette compréhension, certes 'subtile'*[27]*, le droit au respect de la vie privée n'était, au fond, que l'un des aspects de la liberté individuelle garantie par l'article 66 de la Constitution, à laquelle elle empruntait son régime. Cette conception dite extensive de la liberté*

---

[23] La Constitution a été adoptée le 22 juillet 1946 par la Conférence internationale de la Santé, tenue à New York du 19 juin au 22 juillet 1946 et est entrée en vigueur le 7 avril 1948.

[24] Dir. (UE). PE et Cons. UE 1995/46, préc. considérant 10.

[25] *Ibid.*

[26] Cons. const. 18 janv. 1995, n° 94-352 DC, cons. 3 ; rappr. 22 avr. 1997, n° 97-389 DC, cons. 44.

[27] N. Molfessis, *Le Conseil constitutionnel et le droit privé*, th. préc. n° 157 (*in fine*) et n° 163.

individuelle pouvait fort bien accueillir le droit au respect de la vie privée, dans la mesure où ce dernier implique une défense contre les intrusions extérieures, mais aussi une liberté d'agir dans la sphère privée. »[28]

21. Ce droit a été élevé au rang des *« droits naturels, inaliénables et sacrés de l'Homme »*[29] définis par la Déclaration des Droits de l'Homme et du Citoyen du 26 août 1789. Qui fait-elle même partie intégrante de la Constitution du 4 octobre 1958 au titre des normes complémentaires écrites auxquelles la Constitution renvoie. Ce droit est également reconnu à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et à l'article 7 de la Charte des droits fondamentaux de l'Union européenne.

> *« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. »* [30]

22. Protégé par l'article 9 du Code civil[31], le droit à la vie privée constitue un droit subjectif qui permet à chacun de déterminer librement les limites de sa vie privé qui doivent être respectées par les tiers.

23. Le droit à la vie privée ainsi que le droit à la protection des données à caractère personnel ne sont pas des droits absolus. Chacun de

---

[28] V. MAZEAUD. Nouveaux Cahiers du Conseil constitutionnel n° 48 (dossier : vie privée) - juin 2015 - p. 7 à 20. Disponible sur le site https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseilconstitutionnel/la-constitutionnalisation-du-droit-au-respect-de-la-vie-privee#ref-note-12, dernière consultation le 12. oct. 2018

[29] Dans sa décision n° 2008-562 DC du 21 février 2008, le Conseil constitutionnel affirme que le respect de la vie privée, protégée par l'article 4 de la DDHC, fait partie des libertés constitutionnellement garanties.

[30] CEDH. 4 nov. 1950. art. 8 § 1.

[31] Loi °70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens.

ces droits *« doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. »*[32]

24. La conciliation du droit à la santé et à la vie privé repose sur le secret professionnel instrument de confiance qui permet à la personne dans une situation de vulnérabilité de révéler des informations la concernant au professionnel sans craindre de voir sa vie privée révélée[33]. Par ce moyen, nulle pratique professionnelle ne peut venir troubler ce droit essentiel. A ce titre, *« il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, […] à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »*

25. Le droit à la vie privée est également lié au droit fondamental de disposer librement de ses propres informations. Celui-ci est attaché à l'autodétermination informationnelle, qui permet à la personne de consentir ou de s'opposer librement à ce que des informations la concernant soient divulguées dès lors qu'elle estime que celles-ci relèvent de sa vie privée et que leur révélation serait de nature à lui porter un préjudice.

26. Il trouve son équivalence dans *« le droit à la protection des données personnelles (…), c'est-à-dire le droit de l'individu de décider de*

---

[32] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, considérant 4.

[33] Toutefois, à côté de la conception absolutiste du secret professionnel qui affirme la primauté du devoir de silence du professionnel dans l'intérêt général mais aussi dans l'intérêt du patient il existe une conception relativiste. Cette conception du secret permet au professionnel dans l'intérêt général de concourir, à la lutte contre la propagation des épidémies et de participer à la protection des personnes vulnérables contre les sévices. En effet, la loi prévoit des mesures de transmission de certaines informations qui peuvent être utiles dans le but de protéger la santé publique en prenant des mesures appropriées. Ainsi en est-il des cas de maladies à déclaration obligatoire, dont la plupart sont contagieuses ou graves.

la communication et de l'utilisation de ses données à caractère personnel »[34.]

27. Dans le cadre de nos développements nous considérerons essentiellement le droit à la vie privée mais désignerons également par le vocable de droits de la personne l'ensemble des droits reconnus à la personne physique à l'égard du traitement des données à caractère personnel [35] qui sont définies au chapitre III, *Droits de la personne concernée,* du Règlement 2016/679

28. **Les prémices du secret.** Autrefois, la médecine archaïque empreinte de mysticisme, était fondée sur l'idée de secret. Le chaman ou le guérisseur était le seul à connaître les paroles sacrées, les rites et incantations ainsi que les plantes médicinales nécessaires pour entrer en contact avec le monde des esprits et prodiguer des soins aux membres de son clan. Ce médecin archaïque vivait à l'écart du groupe et gardait confidentielles ses pratiques ainsi que les maux qui affectaient les siens afin de conserver son pouvoir au sein de sa communauté.

29. Le secret n'est donc pas une notion contemporaine, et il n'est par ailleurs pas limité au domaine médical. L'Ancien testament comportait déjà l'obligation morale de garder le silence : *« défends ta cause contre ton prochain, mais ne révèle pas le secret d'un autre, de peur qu'en l'apprenant il ne te couvre de honte »*[36].

30. **Le secret comme devoir éthique.** Dans l'Athènes du Vème siècle avant notre ère, la médecine connait une importante mutation. Elle demeure un savoir dont les connaissances sont âprement conservées par une élite. Cependant, sous l'influence d'Hippocrate, elle se rationnalise au

---

[34] *Ibid.*

[35] Charte des droits fondamentaux de l'Union européenne, 7 décembre 2000, article (art.) 8, paragraphe (§) 1. Voir également, art. 16, paragraphe (§1) du Traité sur le fonctionnement de l'Union européenne (TFUE), 25 mars 1957.

[36] La Bible, Ancien testament, Chapitre 25 verset 9, Livre des Proverbes.

point de devenir une véritable science. Ce membre de la famille des Asclépiades de Cos désacralise la maladie qui n'est désormais plus l'œuvre d'êtres supranaturels. Il fonde sa médecine sur le colloque singulier, l'anamnèse ainsi que l'étude clinique. Le médecin exerce et enseigne son art au sein de l'asclépion ou éventuellement au domicile du malade. En conséquence, l'exercice de la profession et son apprentissage reposent essentiellement sur la nécessaire confiance du patient en la discrétion du médecin concernant les informations portées à sa connaissance ou dont il a pu prendre connaissance dans l'exercice de sa profession. Fort de ce constat, Hippocrate dote les sciences médicales d'une véritable éthique et d'une déontologie. À cette fin, dès la genèse de la médecine, il concrétise au sein du *Corpus Hippocraticum*, dans *le Serment*, l'engagement solennel du futur médecin de respecter l'obligation de discrétion :

> *« (…) Dans quelque maison que je rentre, j'y entrerai pour l'utilité des malades, me préservant de tout méfait volontaire et corrupteur, et surtout de la séduction des femmes et des garçons, libres ou esclaves. Quoi que je voie ou entende dans la société pendant, ou en dehors de l'exercice de ma profession, je tairai ce qui n'a jamais besoin d'être divulgué, regardant la discrétion comme un devoir en pareil cas. »*[37]

31. La médecine hippocratique est fondée sur une approche rationnelle, éthique et déontologique. L'information concernant le malade y est conservée sous le sceau du secret. Elle ne circule que par exception et uniquement à des fins de soin, d'enseignement, de santé publique[38].

---

[37] *Œuvres complètes d'Hippocrate*, Emile Littré, Paris, Baillière, 1819-1861, v. 4.

[38] F. ROUBAUD, *«Des hôpitaux aux points de vue de leur origine et de leur utilité, des conditions hygiéniques qu'ils doivent présenter, et de leur*

32. Durant l'Empire romain et jusqu'à la Renaissance, nous disposons de peu d'informations sur le secret médical[39] en raison de l'absence de manuscrit retraçant les us et coutumes durant cette période. Le droit romain classique reste donc silencieux sur la notion de secret médical. Ainsi, à l'exception de Cicéron qui dans son *Traité des devoirs* rappelle que *« les médecins qui pénètrent sous les toits et dans les chambres d'autrui doivent cacher beaucoup de choses, même sous l'offense, quoiqu'il soit difficile de se taire quand on pâti »t*[40], le Code Justinien, les Institut es ou encore le Digeste n'en font nullement état.

33. Au regard de ces éléments, bien qu'il n'existe, durant cette période, que très peu d'écrits faisant état du secret médical, cela ne signifie pas, pour autant, que le médecin était libéré de tout devoir de silence. Hormis le cas spécifique de l'enseignement, l'exercice de la médecine ne nécessitait pas le partage d'informations. Par ailleurs, vis-à-vis des tiers et pour des considérations liées à la confiance des patients en la personne du médecin, le secret en tant que devoir éthique semble avoir subsisté jusqu'au Moyen Age. Ainsi le médecin voulant échapper à l'opprobre avait tout intérêt à s'astreindre au silence.

34. **Le Moyen-Âge et la disparition de l'objet du secret.** Au Moyen-Âge, en occident, cette première pierre posée par Hippocrate semble s'effriter au point de, pour ainsi dire, disparaître. *« La plupart des versions médiévales du serment d'Hippocrate ne font plus référence au*

---

administration », Paris, Baillière : Librairie de l'académie impériale de médecine, 1853, p. 45. Hippocrate a, au sein de l'asclépion, sous le platane de la ville de Cos mais également au chevet de ses malades, porté à la connaissance de ses deux fils Thessalos et Draco ainsi qu'à son gendre Polybe, des informations relatives à la santé de ses patients afin d'enseigner à ses disciples ses connaissances et son savoir-faire.

[39] Le terme secret médical est ici utilisé volontairement, il résulte des modalités d'exercice de la médecine, la notion de secret professionnel apparaitra bien plus tard.

[40] CICERON, DE OFFICIIS (« Traité des devoirs »), cité également par VILLEZ, « *Histoire du secret médical*, 10 mars, Paris, Seghers, 1986, p. 17.

secret. » [41] À l'image de la société qui, sous l'influence grandissante de la religion chrétienne, confond spirituel et corporel, la médecine se préoccupe essentiellement de l'esprit au détriment du corps. *« Les professions médicales et les ministres du culte sont les deux piliers principaux qui ont permis la construction de la notion de secret professionnel. »* [42] Ainsi, les maux y trouvent le plus souvent une explication religieuse et la médecine est exercée par les ministres du culte, moines, clercs. Ce faisant, le secret se confond avec la confession et prend la forme d'un contrat moral conclu entre le croyant et le confesseur.

35. Comme le souligne, C. BRETON-RAHALI, F. Kusz ou encore R. Villey, dans la société médiévale l'individu disparait au profit de la collectivité :

> *« La mentalité médiévale est influencée par un mode de vie communautaire et des relations de pouvoir propres à cette communauté. Les fondements du système féodal nient l'individu. Les libertés individuelles sont quasi inexistantes et la vie privée ne fait l'objet d'une protection particulière. Le devoir de secret du médecin semble être en retrait pendant cette période de l'Histoire peu propice à l'individualisme. »*[43]

36. **La Renaissance de la vie privée.** La seconde moitié du XIIIème et le début du XIVème siècle marquent le début de la Renaissance, période à laquelle, la société est stimulée par la redécouverte des pensées Antiques,

---

[41] F. KUSZ, *Secret professionnel du médecin généraliste et maltraitance à enfants*,.,, Thèse, Nancy, 2004, p. 29.

[42] C. BRETON-RAHALI, *op. cit.*,, p. 49.

[43] C. BRETON-RAHALI., *Le secret professionnel et l'action médico-sociale*, Thèse, Nancy, 2014, p. 51. Voir également Fabienne. F. KUSZ, *op. cit*, p. 29, R. VILLEY, *op. cit*, p. 27.

et la perte de pouvoir du religieux. À nouveau, la médecine est progressivement exercée par des praticiens laïques et l'individu reprend une place importante au sein de la société. Le secret médical réapparaît dans les écrits où il trouve toujours, comme le souligne Jean Verdier, une justification de l'ordre de l'éthique, de la déontologique, de la morale ou du religieux mais ne dispose pas encore d'un fondement légal.

> *« Les secrets qui sont confiés aux médecins sont des dépôts sacrés qui ne leur appartiennent point. La raison, la religion et les statuts leur enjoignent de garder sur eux un silence inviolable. L'obligation du secret est si forte chez eux, que la plus saine partie des théologiens, canonistes, jurisconsultes et médecins, disent qu'un médecin ne peut être tenu par le commandement d'aucun Supérieur à rendre compte de ce que son ministère lui a fait connaître. »*[44]

37. Précurseur, Jean Verdier souligne dans ses écrits que le médecin n'est pas propriétaire des informations qui lui ont été confiées sous le sceau du secret. Ainsi, personne ne peut l'en délier et les informations qu'il recueille ou constate lors de son activité ne constituent pas des biens dont il pourrait librement disposer. *« De ce fait, malgré la moindre obligation légale, on commence à voir des procès intentés à des médecins pour violation du secret, quand il en résulte un préjudice pour le malade »*[45].

38. L'obligation de secret réapparait également dans les écrits en rapport avec l'exercice ou l'enseignement de la médecine, notamment *« dans les statuts des établissements […]. C'est le cas de la faculté de*

---

[44] P. VERDIER, *Essai sur la jurisprudence de la médecin en France, ou Abrégé, historique et juridique des établissements,* 1763, p. 56.

[45] F. KUSZ, op. *cit.* p. 30.

médecine de Paris qui introduit cette obligation dans ses statuts dès 1598. Dès 1699, il est mentionné dans le règlement des chirurgiens ou encore la faculté de Montpellier qui l'inscrivent en première page de leurs thèses »[46].

39. **Napoléon et la consécration législative du secret.** La notion de secret médical s'est adaptée aux époques et aux nécessités de la santé publique. La Révolution française en mettant brutalement fin à l'Ancien Régime marque un tournant. L'Assemblée constituante, à travers la Déclaration des droits de l'homme et du citoyen du 26 août 1789, pose les fondements juridiques de la nouvelle société française en reconnaissant aux citoyens des droits et libertés. Il faut toutefois attendre 1810 pour que le secret dépasse le cadre déontologique.

40. Le Code pénal Napoléonien, en considérant la violation du secret comme un délit pénal, apporte pour la première fois dans notre droit national mais aussi en Europe[47] une consécration légale au secret médical.

41. Celui-ci fait désormais l'objet d'une réponse disciplinaire mais aussi d'une réponse pénale. Figurent au sein de l'ancien article 378 au premier rang des personnes qui y sont astreintes, les médecins et les professionnels de santé :

> *« Les médecins, chirurgiens et autres officiers de santé, ainsi que les pharmaciens, les sages-femmes et toutes autres personnes dépositaires, par état ou profession ou par fonctions temporaires ou permanentes, des secrets qu'on leur confie, qui, hors le cas où la loi les oblige ou les autorise à se porter*

[46] C. BRETON-RAHALI.,.,. Breton-Rahali, *op. cit*, p. 51. Voir également BRISSAUD, Brissaud, *Secret médical, Responsabilité pénale et civile du médecin*, Thèse, Bordeaux, 1912, 1912, p. 9.

[47] A. LECA, J-C. CAREGHI, « Le secret médical, au crible d'une analyse historique », *CDSA*, éd. LEH n° 15, 2012, p. 15.

*dénonciateurs, auront révélé ces secrets, seront punis d'un emprisonnement d'un mois à six mois [*durée*] et d'une amende de 500 à 15000 F [*taux résultant de la loi 85-835 du 7 août 1985*] [*infraction, sanction*]. »*[48]

42. **Une extension des personnes assujetties au secret.** Le Code pénal de 1810, élargit les contours du secret en y assujettissant, au même titre que les médecins, l'ensemble des professions de santé. Toutefois, sous son égide, et pour des considérations historiques, le législateur semble s'inscrire dans une logique séparatiste en opérant un distinction entre les professions de santé d'une part et, d'autre part, les *« autres personnes dépositaires, par état ou profession ou par fonction »* incluant, par exemple, les assistants des services sociaux.

43. La liste des professions soumises au secret n'a cessé d'être étendue, par le législateur ainsi que la jurisprudence afin d'y inclure, notamment, quelques-unes des professions du droit telles que les avocats et notaires mais aussi les professions du secteur bancaires, etc. Cet accroissement constant des professionnels assujettis a conduit le législateur à changer son approche de la protection du secret afin d'avoir plus de visibilité, de clarté mais surtout de sécurité juridique.

44. **Le Nouveau Code pénal, un instrument de sécurité**. Refondu par les lois du 22 juillet 1992, le Nouveau Code a introduit aux articles 226-13 et 226-14 les nouvelles dispositions concernant l'obligation au secret. À travers ces nouvelles dispositions, le législateur n'a pas souhaité, dans un souci de concision et de clarté [49], reproduire la liste des professionnels tenus au secret.

---

[48] C. pén., art. 378 créé par la loi 1810-02-19 promulguée le 1er mars 1810.

[49] Voir notamment B. PY, *Le secret professionnel*, L'Harmattan, coll. *« La justice au quotidien »*, Paris, 2005.

45. La protection pénale du secret professionnel relève du chapitre six, du titre deux, du livre deux, correspondant aux atteintes à la personnalité. Ainsi, les dispositions de l'article 226-13 du Code sanctionnent toutes atteintes à la vie privée et familiale résultant d'une révélation de l'information à caractère secret effectuée par une personne qui en est dépositaire en raison de son état, sa profession, sa fonction ou sa mission. L'article 226-13 du Code pénal semble supprimer toute hiérarchie selon le statut juridique du dépositaire. Ainsi, que le dépositaire soit médecin ou assistant des services sociaux, il est soumis à la même obligation de se taire. Par ces nouvelles dispositions, le législateur a voulu protéger l'intégrité de toute personne en s'assurant de la sécurité des confidences « forcées » faites par celle-ci à un professionnel dans un esprit de nécessité et de confiance. Ce principe est rappelé au sein du Code de la santé publique sous l'angle des droits de la personne.

46. **Le secret et le soin.** Dans le domaine de la santé, le secret est inhérent à la relation thérapeutique. Celle-ci constitue un rapport déséquilibré entre le médecin et son patient, ce-dernier étant, par suite d'une maladie, dans l'obligation de recourir aux services du premier et de se confier à celui-ci afin qu'il lui apporte une réponse thérapeutique adaptée. Par l'institution du secret et la sanction de sa méconnaissance, le pouvoir législatif corrige ce déséquilibre et de la sorte, instaure la confiance nécessaire au patient afin que celui-ci confie au médecin les informations indispensables à l'exercice de sa profession. Le patient est prémuni contre toute utilisation des informations obtenues par le professionnel de santé à d'autres fins que le soin, mais également contre toute inquisition susceptible d'être exercée par la société quant à la recherche d'informations relevant de sa vie privée.

47. Ce fondement n'exclut pas toute conception supra-individuelle de la protection pénale du secret. Au-delà de la relation thérapeutique, le secret professionnel par la sphère de confiance qu'il génère a également vocation à satisfaire un intérêt social.

« En protégeant la confiance placée en la pers1onne du dépositaire du secret, la loi veut garantir la sécurité des confidences qu'un particulier est dans la nécessité de faire à une personne dont l'état ou la profession, dans un intérêt général et d'ordre public, fait d'elle un confident nécessaire. »[50]

48. Ainsi, le patient n'a pas à réaliser un choix entre le recours aux soins et le respect de sa vie privée. Ce faisant, le secret garantit la bonne santé de la population ainsi que la pérennité du système de santé[51]. Avec le progrès médical, la médecine s'est hyperspécialisée réformant au passage les modes d'exercice favorisant l'élaboration de parcours de soins, la constitution d'équipes de soins pluri et transdisciplinaire, accroissant la place occupée par la prise en charge hospitalière, la relation avec la médecine de ville et le secteur médico-social requérant un besoin impérieux de partager de l'information relative à la personne prise en charge[52].

49. Cette néo-médecine est à la recherche d'un équilibre entre secret professionnel et circulation de l'information entre les professionnels assurant la prise en charge d'un même patient.

50. **Une diversification de la protection de la vie privée.** *« En France, paradoxalement, alors que le principe de respect de la vie privée*

[50] Crim, 19 nov. 1985, n° 83-92813, Bull. crim. n° 364.

[51] A. TEIL, « Qu'appelle-t-on système de soins ? »,, *ADSP*, n° 33, 2000, p. 26.

[52] F. GIRAUD, G. DERIOT, J.-L. LORRAIN, *Rapport fait au nom de la commission des Affaires sociales sur le projet de loi relatif aux droits des malades et à la qualité du système de santé*, n° 174, Sénat, Session ordinaire de 2001-2002.

irrigue notre droit depuis le XIXème siècle, il a fallu attendre 1970 pour que cette notion soit inscrite expressément dans notre législation »[53].

51. Outre une diversification pénale de la protection de la vie privée, afin de tenir compte des moyens techniques modernes permettant la captation ou la transmission, *« des paroles prononcées [ou son image] dans un lieu de vie privée par une personne, sans le consentement de celle-ci »*[54], la loi du 17 juillet 1970 consacre en son article 22 la protection civile de la vie privée.

> *« Auparavant, on considérait que la protection de la vie privée découlait implicitement du principe constitutionnel plus large de liberté individuelle : c'est d'ailleurs ce qu'a expressément reconnu le Conseil constitutionnel dans sa décision 99416 DC du 23 juillet 1999, en affirmant dans son considérant 45 sur la carte vitale que "la liberté proclamée par (l'article 2 de la Déclaration des droits de l'homme et du citoyen) implique le respect de la vie privée." »*[55]

52. Ainsi, elle créée, au sein du Code civil un nouvel article 9 mais ne propose, toutefois, aucune définition juridique de la notion :

---

[53] Y. DETRAIGNE et A.-M. ESCOFFIER , *Rapport d'information fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques*, n° 441, Sénat, Session ordinaire de 2008-2009, p. 14.

[54] C. pén., article (art. 368 à 372 introduits par l'art. 23 de la Loi n°70-643 du 17 juillet 1970, *JORF* 19 juillet 1970. Voir également R. NERSON, « La protection de la vie privée en droit positif français », *RIDC* 1971, p. 739.

[55] *Ibid.*

« Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé. »[56]

53. Comme le souligne Robert Badinter, plutôt que d'en définir à travers ce nouvel article 9 le contenu de la notion de vie privée, *« les juristes français se sont plus volontiers attaches a [en] dépeindre le contenant »*[57]. Il en résulte pour la doctrine majoritaire qu'en l'absence de toute définition positive de la vie privée, il convient de définir cette notion par opposition à la vie publique entendue comme *« la part de notre vie qui se déroule nécessairement en présence du public, notre participation publique à la vie de la cité »*[58].

54. L'intérêt de cette démarche est, en effet, de *« mettre l'accent sur la primauté de la vie privée, celle-ci, interdite à toute intrusion indiscrète, étant pour chacun le sort commun, le reste, c'est-à-dire la vie publique ouverte à la curiosité de tous, étant l'exception »*[59]

---

[56] C. civ., art. 9 créé par la loi 1803-03-08 modifié par la Loi n°70-643 du 17 juillet 1970, art. 22.

[57] R. BADINTER, « Badinter, Le droit au respect de la vie privée »,, *JCP G* 1968, I, 2136.

[58] *Ibid.*

[59] N. MALLET-POUJOL, « , Protection de la vie privée et des données personnelles »,, Legamedia, février 2004, p. 6.

Voir également, R. LINDON, « Lindon, La presse et la vie privée »,, *JCP G* 1965, I, 1887.

55. Ainsi *« Depuis Royer-Collard, le célèbre mur de la vie privée se découpe bien nettement sur l'horizon juridique, mais quant au domaine qu'il enclot, ses dimensions s'avèrent singulièrement variables »*[60].

56. D'une manière générale, il ressort de la jurisprudence que *les « différentes facettes de la vie privée […] correspondent aux aspects principaux de la vie : la vie familiale, la vie sentimentale, les loisirs, la santé, les mœurs, les convictions philosophiques et religieuses, les circonstances de la mort ainsi que le droit à l'image […] le numéro de sécurité sociale et les références bancaires ressortissent à la vie privée de chacun à l'encontre de toute personne dépourvue de motif légitime à en connaître »* [61].

57. Le contenu de la vie privée se révèle ainsi, varié et étendu mais surtout, au regard d'une analyse de la jurisprudence, évolutif puisqu'il est fonction des mœurs ou des circonstances de la vie de l'individu.

58. Il en résulte une notion aux contours imprécis dont le contenu découle d'une construction prétorienne. Elle recouvre à la fois l'intimité, autrement dit l'existence d'une sphère réservée et préservée de toute immixtion extérieure, mais également la notion d'autonomie[62] entendue comme *« le droit pour une personne d'être libre de mener sa propre existence comme elle l'entend avec un minimum d'ingérences de l'extérieur »*[63].

59. Cette notion d'autonomie alors naissante, confrontée au développement des technologies de l'information et de la communication

---

[60] *Ibid.*

[61] *Ibid.*

[62] B. BEIGNIER, « Vie privée et vie publique », *Arch. Phil. Droit*, n° 41, 1997, p. 163.

[63] J. CABANNES, « Cabannes, Le droit au respect de la vie privée : fondement et quantum de la responsabilité du journaliste indiscret »,, conclusions sous CA Paris, 15 mai 1970, *D.* 1970, p. 466.

(TIC)[64], va progressivement, s'étoffer faisant ainsi évoluer la protection de la personne concernant les traitements de données à caractère personnel d'une déclinaison du droit au respect de la vie privée, à la reconnaissance d'un véritable droit autonome à la protection de ses données.

60. S'agissant du droit au respect de la vie privée, le législateur ainsi que les juges cherchent à concilier cette notion avec d'autres intérêts tels que les intérêts sanitaires, la maîtrise des dépenses de santé, etc. mais aussi d'autres principes fondamentaux comme la liberté d'expression ou encore la liberté individuelle ou les droits de la défense.

> *« De son côté, le Conseil constitutionnel s'est régulièrement fondé sur ce droit au respect de la vie privée pour examiner la constitutionnalité de dispositions législatives tendant à la création de fichiers : à titre d'exemple, l'encadrement législatif des fichiers de police judiciaire STIC et JUDEX*[65] *ou encore la création du dossier médical personnel*[66]*, ont été examinées sous l'angle du respect de la vie privée et de la proportionnalité de la mesure au regard des objectifs poursuivis par la loi. »* [67]

61. *« Aussi relative s'affirme-t-e1le, la vie privée de chacun comporte en tout état de cause un noyau irréductible, une zone d'intimité qui appelle une protection absolue. »*[68] C'est ce noyau irréductible, cette intimité que

---

[64] *V. infra n°30.*

[65] Décision n° 2003-467 du 13 mars 2003 relative à la loi pour la sécurité intérieure.

[66] Décision n° 2004-504 du 12 août 2004 sur la loi relative à l'assurance maladie.

[67] Y. DETRAIGNE et A.-M. ESCOFFIER, rapport préc. p. 15.

[68] R. BADINTER, « Badinter, Le droit et l'écoute électronique en droit français », *Publications de la Faculté de droit et de sciences politiques et économiques d'Amiens*, n° 1, 1971-1972, p. 21, n° 9.

le législateur a estimé qu'il était particulièrement nécessaire de protéger contre les atteintes continuellement perfectionnées de la technique moderne.

62. **Les technologies de l'information et de la communication et le soin**. Les concepts de communication et d'information, contrairement à celui de technologie, ne présentent aucune difficulté. Le mot *communication* provient du latin *communicatio* dérivé du verbe *communicare* qui décrit l'action de communiquer, c'est à dire de transmettre de l'un à l'autre. En tenant compte de la notion d'*information* précédemment définie [69], les technologies de l'information et de la communication constituent donc un ensemble de procédés permettant la conservation et la transmission d'informations et de données.

63. Les TIC sont antérieurs à l'écriture cunéiforme élaborée en basse Mésopotamie en 3400 avant J.-C. Cependant, ce n'est qu'à compter du XIX[ème] siècle, que nous trouvons une trace de l'utilisation de ces technologies dans le domaine médical. Suite à l'invention du télégraphe par Samuel Morse, l'armée nordiste aurait utilisé, lors de la guerre de Sécession[70], la première ligne télégraphique, construite entre Washington et Baltimore en 1844, afin de demander le ravitaillement en médicament des forces situées sur le front et, de communiquer à l'état-major le nombre de militaires blessés et de pertes humaines [71]. Cette utilisation essentiellement à des fins de stratégie et de logistique militaire resta toutefois une pratique limitée en temps de guerre.

64. Si son utilisation peut aujourd'hui sembler commune, le second outil de communication exploité par la médecine fût inventé le 14 février

---

[69] *V. supra n°3.*

[70] Guerre civile américaine, survenue entre 1861 et 1865 entre l'Union, dirigée par Abraham Lincoln, et la Confédération, dirigée par Jefferson Davis, aboutissant à la création des Etats unis d'Amérique.

[71] M. LAILA. *La télémédecine et les technologies d'assistance pour la prise en charge des personnes âgées fragiles à domicile et en institution : modélisation du besoin, de la prescription et du suivi*, Thèse, Grenoble, 2009, p. 19.

1876 par Alexander Graham Bell. Il s'agit du téléphone. Relevant de l'expérience scientifique plus que d'un acte médical, la démarche menée par le physiologiste Néerlandais Willem Einthoven[72], le 22 mars 1905, consistait en la transmission, au moyen d'un câble téléphonique, puis à l'enregistrement de l'électrocardiogramme d'un patient hospitalisé, situé à un kilomètre cinq de son laboratoire. Ce faisant, les premières données de santé furent produites, communiquées, enregistrée et examinées au moyen des technologies de l'information et de la communication. Déjà à l'époque, des problèmes juridiques sont soulevés mais uniquement sous l'angle de la propriété industrielle[73].

65. En 1920, la première licence pour radio de service médical est délivrée à New York, elle est dédiée aux soins réalisés sur les bateaux. Au cours de la première moitié du vingtième siècle, d'autres expériences seront également menées aux États-Unis mais aussi en Europe[74]. Les dispositifs se diversifièrent et pénétrèrent le monde de la santé au gré des progrès techniques et scientifiques. À titre d'exemple, en 1959 une nouvelle technique de communication dans le domaine de la santé est exploitée. Il s'agit de la vidéo, cette technologie a été appliquée par un service de psychiatrie Américain afin de réaliser une consultation à distance.

---

[72] Physiologiste néerlandais et prix Nobel de physiologie et de médecine de 1924, Willem Einthoven est l'inventeur du galvanomètre à corde, ancêtre de l'électrocardiographe.

[73] Alexander Graham Bell aurait volé cette invention à Antonio Meucci qui intenta un procès. Celui-ci dura jusqu'en 1889, date à laquelle Antonio Meucci mourut, ce qui mit fin à la procédure sans que sa paternité à l'égard de l'invention du téléphone ne soit admise. Toutefois, celle-ci fut officiellement reconnue en 2002 par la Chambre des représentants des États-Unis. Voir notamment R. WALLSTEIN, « . «Télécommunications – Histoire », *Encyclopaedia Universalis*, 2014.

[74] P. SIMON, D. ACKER, *La place de la télémédecine dans l'organisation des soins*, DHOS, nov. 2008, p. 95.

66. Enfin en 2001, *l'opération Lindbergh*[75], opération de télé-chirurgie constitue non seulement un record de distance puisque 7000 kilomètres séparent la patiente situé à Strasbourg, de l'équipe chirurgicale située à New York, mais représente également un tournant dans le recours aux TIC dans le domaine de la santé puisque le début du XXIème siècle marque l'essor de ce procédé.

67. Jusqu'à la fin des années 70 l'utilisation des technologies de l'information et de la communication n'est pas réglementée. En l'absence de règles *ad hoc,* les atteintes à la vie privée pouvant résulter de l'usage de ces moyens de communication au cours de l'exercice de l'activité médicale est garantie par des mécanismes traditionnels[76].

68. L'adoption de la loi relative à l'informatique aux fichiers et aux libertés marque un tournant dans la protection et permet la création de nouveaux droits afin de limiter toute intrusion non consentie dans la sphère privée pouvant résulter de la mauvaise utilisation de ces technologies.

69. **L'informatisation, un risque pour les droits et libertés individuelles.** En France, il a fallu attendre le milieu des années 70 pour voir poindre une prise de conscience collective des problématiques liées à l'informatisation et aux risques d'atteintes aux droits et libertés individuelles ou publiques résultant de l'usage des technologies de l'information et de la communication.

70. Ces technologies disposent d'une définition juridique mais celle-ci est inintelligible. Ce nouveau vocable pose bien des difficultés tant la définition sémantique de *technologie* demeure floue. Afin de déterminer

---

[75] Nom donné en hommage à l'aviateur Charles Lindbergh qui, en 1927, effectua la première traversée de l'Atlantique sans escale entre New -York et Paris à bord de son avion surnommé le « Spirit of St. Louis ».

[76] C. ZORN, *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé,* avant-propos B. Py, préf. I. de Lamberterie, PUN., 20102009.

les contours de la notion de technologie, il convient de se référer à son étymologie. Technologie vient à la fois du grec *techné,* qui signifie art et de *logia*, terme dérivé de *logos* qui signifie « discours », « description ». La technologie serait donc la description d'un « art », d'une technique. Cependant, au XIXème siècle, un professeur de l'université de Harvard, John Bigelow, est venu complexifier les choses en posant une conception contemporaine du mot technologie, *la technique.* Le terme *technologie* regroupe donc aujourd'hui deux acceptions. Les technologies de l'information et de la communication constituent donc un ensemble de procédés permettant la conservation et la transmission d'informations et de données.

71. En 1973, le Ministre de l'Intérieur Raymond Marcellin a pour projet d'initier la constitution d'un système d'interconnexion de fichiers à partir du numéro d'inscription au répertoire national d'identification des personnes physiques (RNIPP ou NIR). Ce projet repose sur la capacité d'un ordinateur, l'IRIS 80, à gérer un programme informatique dénommé SAFARI, *Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus*. Ce système est capable de procéder à la mise en relation automatisée de plusieurs fichiers publics et privés comprenant notamment les fichiers des services de police, du ministère de la Justice, du ministère des Armées, de la sécurité sociale, des banques. Le projet est révélé le 21 mars 1974 par Monsieur Philippe Boucher dans un article intitulé « *SAFARI ou la chasse au Français* » publié dans le quotidien, *Le Monde,* et rédigé à partir des informations divulguées par des informaticiens du ministère de l'Intérieur soucieux des conséquences de ce projet. Hommes politiques, médias et citoyens prennent conscience des atteintes aux droits et libertés individuelles auxquelles peut conduire l'informatisation. L'opinion publique se mobilise et le Premier ministre de l'époque, Pierre Messmer met fin au projet. Il institue, auprès du Garde des sceaux, une Commission dite informatique et libertés. Présidée par Bernard Chenot cette Commission, est chargée de proposer une réglementation sur l'utilisation des moyens informatiques. Elle publie en

1975 un rapport Tricot qui servira de fondement à la loi Informatique et Libertés.

72. C'est donc dans ce climat de méfiance vis-à-vis de l'État et sur les recommandations du rapport Tricot que le gouvernant déposa auprès du Parlement un projet de loi destiné à la mise en œuvre de garde-fous contre les abus de l'informatique susceptibles de porter atteintes aux libertés publiques mais aussi au droit à la vie privée. Dans son rapport, rédigé au nom de la commission des Lois, le sénateur Jacques Thyraud, souligne que ce texte conduit à s'interroger *« sur le devenir des libertés individuelles et publiques dans la quête permanente à l'information »*[77].

73. Il fallut trois ans de discussion, mais après de nombreux débats et un passage en commission mixte paritaire témoignant des tensions régnant au sein de la société, le projet de loi fut adopté définitivement par l'Assemblée nationale et le Sénat le 21 décembre 1977. Le principe est posé dans l'article 1 du texte :

> *« L'informatique doit être au service de chaque citoyen. […] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »*[78]

74. Il crée de nouveaux droits au profit de la personne concernée par le traitement de ses données à caractère personnel et de nouvelles obligations pour les responsables des traitements de données personnelles.

---

[77] J. THYRAUD, *Rapport fait au nom de la Commission des lois sur le projet de loi relatif à l'informatique et aux libertés*, Sénat, n° 72, Session ordinaire 1977-1978.

[78] Loi n°78-17 du 6 janvier 1978 dite « Loi relative à l'informatique, aux fichiers et aux libertés. art. 1er.

75. **Une utilisation de la technologie à des fins médicales réglementée.** En 1997, l'Organisation mondiale de la Santé (OMS) est venue préciser la notion de télésanté :

76. *« la cybersanté consiste à utiliser, selon des modalités sûres et offrant un bon rapport coût/efficacité, les technologies de l'information et de la communication à l'appui de l'action de santé et dans des domaines connexes, dont les services de soins de santé, la surveillance sanitaire, la littérature sanitaire et l'éducation, le savoir et la recherche en matière de santé »*[79].

77. Il en résulte que la télésanté est un concept plus large que la télémédecine. En effet, si la télémédecine est la pratique de la médecine à distance, la télésanté qui ne dispose d'aucune définition légale peut, quant à elle, être définie, comme la promotion de la santé au moyen de TIC ou encore comme « *l'utilisation des outils de production, de transmission, de gestion et de partage d'informations numérisés au bénéfice des pratiques tant médicales que médicosociale »*[80]

78. La télémédecine a été définie par la loi du 21 juillet 2009 relative à la télémédecine[80]. Il s'agit d'une *« forme de pratique médicale à distance utilisant les technologies de l'information et de la communication. Elle met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de santé, parmi lesquels figure nécessairement un professionnel médical et, le cas échéant, d'autres professionnels apportant leurs soins au*

[79] Organisation mondiale de la santé, Résolution sur la cybersanté, WHA58.28, mai 2005 79 R.

[80] Lasbordes. Rapport. La télésanté un nouvel atout au service de notre bien-être. nov. 2009 80 Loi n° 2009-879 du 21 juillet 2009 relative à la télémédecine.

patient » [81]. Le décret n°2010-1229 du 19 octobre 2010 relatif à la télémédecine, est venu circonscrire cette pratique médicale à l'article R. 6316-1 du Code de la santé publique la télémédecine en précisant qu'elle était constituée d'actes médicaux, *« réalisés à distance, au moyen d'un dispositif utilisant les technologies de l'information et de la communication »*.. La formule *« dispositif utilisant les technologies de l'information et de la communication »* permet d'opter pour le concept de technique puisque le terme technologie est utilisé par les textes afin de qualifier l'ensemble des procédés mis en œuvre par les outils de la télémédecine recensés à l'article R. 6316-1 du Code de la santé publique.

79. **Un système de soin organisé autour de la donnée.** La loi de 1978 relative à l'informatique, aux fichiers et aux libertés, a été constituée initialement comme une mesure réactive afin d'établir la confiance des citoyens face à l'outil informatique. Ce texte concède des droits nouveaux aux citoyens afin de les prémunir contre les systèmes d'informations centralisés dont se dotaient initialement les administrations publiques. Il constitue la première pierre de l'édifice en ce qui concerne la reconnaissance d'un droit à la protection des personnes, contre les atteintes pouvant résulter du traitement de leurs données à caractère personnel.

80. Afin d'endiguer la prolifération des règlementations nationales en Europe qui risquait d'entraver la libre circulation des données personnelles, le Parlement et le Conseil de l'Union européenne ont adopté, le 24 octobre 1995, la Directive 95/46/CE 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. Ce texte créé, dans le cadre de la réalisation du marché intérieur, un socle commun à tous les pays de l'Union européenne en matière de protection des données à caractère personnel y compris en ce qui concerne les données sensibles, catégorie à laquelle appartient les données relatives à la santé.

[81] C. santé publ, art. L. 6316-1.

81. Cette directive favorise par la création de ce socle commun, le développement d'une véritable économie de la donnée au centre de laquelle et placée l'individu. De ce fait, *« l'intégration économique et sociale résultant du fonctionnement du marché intérieur a conduit à une augmentation substantielle des flux transfrontaliers de données à caractère personnel. Les échanges de données à caractère personnel entre acteurs publics et privés, y compris les personnes physiques, les associations et les entreprises, se sont intensifiés dans l'ensemble de l'Union.*[82] *»*

82. La société Française n'a pas échappé au développement des usages des outils informatique et par conséquent à la contribution des systèmes d'information dans la performance des organisations et dans la qualité des services rendus au public y compris en matière de soins. Leur utilisation nécessitant la collecte, la captation, la transmission, l'exploitation, la conservation, l'archivage et la suppression de données, cet essor a entrainé un bouleversement économique et social et l'évolution du rapport que les individus entretiennent vis-à-vis de leur vie privée.

83. Le système de santé a évolué du fait de ce phénomène. Celui-ci a été bouleversé par l'arrivée de ces technologies ce qui a suscité et suscite encore de nombreuses problématiques, ne serait-ce que vis-à-vis du secret professionnel. Leur intégration au système de santé, dans un premier temps à des fins de simplification et de bonne gestion administrative puis comme outil de maitrise des dépenses de santé ont favorisé le développement de la circulation de l'information médico-administrative. Ces nouveaux outils concours désormais à la prise en charge thérapeutique faisant de la donnée à caractère personnel relative à la santé une ressource essentielle du système de santé.

[82] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, considérant (cons.) 5. JOUE n° L 119, 4 mai 2016.

84. La France dispose à l'heure actuelle de l'une des bases de données médico-administratives parmi les plus importantes au monde, le Système national d'information inter-régimes de l'assurance maladie (SNIIRAM). Cette base a été intégrée, depuis la loi de modernisation de notre système de santé[83] au Système national des données de santé (SNDS) nouvellement créé. Celui-ci comporte une majeure partie des données produites par les différents acteurs de soins [84]. Celles-ci constituent une richesse prodigieuse pour la santé publique, la veille sanitaire mais avant tout pour la recherche. L'accès et l'utilisation des données qu'il contient suscitent donc toutes les convoitises.

85. **Une appropriation de la santé et du bien-être.** De L'amélioration des capteurs, leur miniaturisation, le déploiement des smartphones et des dispositifs connectés ainsi que leur utilisation à des fins de bien être puis de santé ont conduit à une massification des données susceptibles de contenir des informations sur l'état de santé des personnes. Confronté à la mondialisation des flux et à l'absence de réglementation claire et unifiée, les risques pour les droits et libertés des personnes se sont accrues.

86. Le Règlement 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, a abrogé la directive de 1995. Il répond au développement de ces nouvelles technologies et à la transformation de l'économie et des rapports sociaux qui ont et vont faciliter le libre flux de données au sein de l'Union européenne ainsi qu'entre les États-membres

[83] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé

[84] Art. L. 161-29 du code de la sécurité sociale (C. sec. soc.) prévoit que les professionnels et les organismes ou établissements communiquent, sous forme nominative, aux organismes d'assurance maladie obligatoire, le code détaillé des actes, prestations et pathologies diagnostiquées, y compris lorsque ces prestations sont établies à partir des données mentionnées aux articles L. 6113-7 et L. 6113-8 C. santé publ.

de l'Union et les entreprises situées au-delà de ses frontières. Il s'agit de consolider les fondations établies par la Directive.

87. En effet le recours à la Directive requière de l'État membre de l'Union européenne, sa transposition dans son système juridique. Elle offre de la souplesse à l'Etat membre en instaurant une obligation de résultat tout en laissant le laissant libre quant aux moyens à prendre pour y parvenir. Ainsi, la Directive de 1995 ne permettait pas la création d'un cadre de protection des données *« solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles »*.

88. Le Règlement a pour finalité de répondre à ce besoin et par ce moyen de susciter la confiance qui permettra à l'économie numérique de se développer dans l'enceinte du marché intérieur. Il a, par conséquent, vocation à renforcer la sécurité juridique et pratique afin de permettre aux personnes physiques d'avoir le contrôle des données à caractère personnel les concernant et par ce moyen de susciter la confiance éliminant ainsi les dernières barrières qui divisent l'Europe. Le Règlement permettra à terme à l'économie numérique de se développer dans l'ensemble du marché intérieur.

89. **L'individu acteur de sa santé.** La médecine a donc évolué, au fur et à mesure de son histoire, d'une médecine de secret à une médecine de partage. La loi du 4 mars 2002, relative aux droits des malades et à la qualité du système de santé a placé le patient au centre du dispositif de soin. Au contact des technologies de l'information et de la communication et en raison de la transition épidémiologique, le soin s'est rapidement décloisonnée en premier lieu de la ville vers hôpital puis dans un second temps du secteur sanitaire vers le secteur social et médico-social. En raison de l'évolution de la technique et de l'appropriation des nouvelles technologies par le patient devenu acteur de sa propre santé, l'information de santé s'est totalement numérisée puis massifiée, au point de faire évoluer la médecine curative vers une médecine préventive, prédictive, personnalisée, participative.

90. Poursuivant le mouvement issu de la loi du 4 mars 2002[85], la loi du 26 janvier 2016[86]et, parallèlement, le Règlement 2016/679[87] (RGPD) font de l'individu qu'il soit patient, usager du système de santé ou simplement utilisateur d'un objet connecté[88], un véritable acteur de la production, de l'utilisation, de la protection mais aussi de la circulation des données à caractère personnel relatives à sa santé.

91. **Disponibilité de l'information de santé et droits de la personne : de nouveaux équilibres**. Pour permettre aux donnés de librement circuler sur le territoire de l'Union européenne, le Règlement général sur la protection des données, reconnait aux personnes concernées par le traitement de leurs données à caractère personnel, un véritable droit à l'autodétermination informationnelle. Ce droit, s'accompagne de mesures de nature à en garantir l'effectivité. Corrélativement, il responsabilise les autres acteurs du traitement et met à leur charge des obligations de nature à préserver la vie privée des personnes concernées par le traitement de leurs données.

---

[85] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé

[86] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé

[87] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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

[88] Dans le cadre de ses travaux Caroline Jay (C. Jay) se fonde sur l'analyse réalisée par P-J. ENGHOZI, S. BUREAU et F. MASSIT-FOLLÉA, pour définir les objets connectés comme *« des dispositifs électroniques capables de recueillir des données auprès de leurs propres utilisateurs ou de leur environnement, puis de les transmettre ensuite vers un autre objet connecté par l'intermédiaire d'un réseau dédié »*. Ainsi, des informations, taille, poids, âge, etc. sont, le plus souvent, renseignées par l'utilisateur à travers une interface qui peut être un smartphone, une tablette, une montre, etc. L'objet connecté, une balance, un tensiomètre, un podomètre, etc. va capter d'autres constantes, et transmettre l'information numérisée de manière automatique à cette interface, au moyen d'un réseau dédié. La donnée réceptionnée par cette interface, va être conservée soit en local, à titre d'exemple, sur le smartphone et/ ou va être transmise par celui-ci dans le cloud. L'application installée sur le smartphone, la tablette va également permettre à l'utilisateur de bénéficier de l'information dans un format compréhensible prenant généralement la forme d'un graphique, de pourcentages, etc.

92. Il en résulte que le droit à la protection des données à caractère personnel ne constitue pas un droit absolu.

93. Au regard de ce qui précède, l'objet de cette étude consiste à analyser s'il existe, concernant la circulation de la donnée à caractère personnel relative à la santé, un renversement de l'exception et du principe faisant de cette donnée un élément de connaissance disponible pour l'ensemble des acteurs intervenant dans le système de santé ou dans le traitement de cette donnée à des fins de bien-être.

94. La présente étude ne porte pas sur l'influence des technologies de l'information et de la communication sur la notion de secret professionnel dans le cadre de l'e-santé. Il envisage, à travers une analyse historique, la diversification des moyens de mise à disposition et de protection de l'information.

95. Notre étude ambitionne également à essayer de rendre intelligible la réglementation en proposant de la clarifier et de la simplifier. Il s'agit de proposer des mesures de nature à préserver la disponibilité sans pour autant porter atteinte à la confiance dans les systèmes d'information de santé et dans l'utilisation des technologies vis-à-vis des données à caractère personnel relatives à la santé.

96. À cette fin, seront donc successivement abordées :

97. **en première partie :** la circulation : une l'information relative à la santé comme une atteinte à l'intimité de la vie privée circonscrite.

98. **en seconde partie :** la circulation de la donnée à caractère personnel relative à la santé comme nouveau principe.

PREMIERE PARTIE LA CIRCULATION : UNE ATTEINTE À L'INTIMITÉ DE LA VIE PRIVÉE CIRCONSCRITE

« 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 aux libertés individuelles ou publiques. »[89]

101. **Un droit à la protection des données issue du droit à la vie privée.** La loi du 6 janvier 1978 avait initialement pour seule préoccupation de réguler le déploiement de l'informatique, et de protéger la vie privée et les libertés des citoyens face aux dangers de son utilisation. En conséquence, la protection des données à caractère personnel était, à sa genèse, étroitement liée à la notion de vie privée. La loi de 1970[90] a insérée au sein du Code civil un article 9 relatif à la vie privée. Celui-ci dispose que *« chacun a droit au respect de sa vie privée. »* En matière d'atteinte à la vie privée, la jurisprudence témoigne de la volonté des juridictions de conserver une certaine marge d'appréciation dans l'application de ce principe général. De la sorte, les juges se ménagent le moyen de tenir compte des évolutions sociétales et technologiques. Le droit à la protection des données à caractère personnel, a ainsi progressivement gagné en autonomie, [91] sans pour autant se détacher totalement du droit à la vie privée.

[89] Loi n°78-17 du 6 janvier 1978 dite « Loi relative à l'informatique, aux fichiers et aux libertés. art. 1er.

[90] Loi n°70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens 91 C. ZORN, Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé, avant-propos B. Py, préf. I. de Lamberterie, PUN, 2010, p. 35 et svt.

102. **Un droit nécessaire à la circulation maitrisée des données.** Dès l'année 1995, sous l'impulsion du droit communautaire, le rapport à la sauvegarde des droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel a évoluée. L'objectif formellement recherché au moyen de la directive du 24 octobre 1995 était d'éliminer les obstacles aux échanges de données nécessaires à la libre circulation *« des marchandises, des personnes, des services et des capitaux. »*.

103. Le Règlement de 27 avril 2016 poursuit le travail amorcé par la directive de 1995 en unifiant les législations nationales des Etats membres en un socle commun accordant un haut niveau de protection aux données à caractère personnel et en contrepartie en supprimant tout obstacle préalable à la circulation des données à caractère personnel.

104. S'agissant des données produites par le système de santé, le secret professionnel a vocation à s'appliquer à l'ensemble des professionnels intervenant dans ce système. Il permet à l'information de circuler de façon maitrisée dans l'intérêt de la personne prise en charge mais aussi à des fins de santé public, de recherche ou de pérennité du système de santé. Cette circulation est protéiforme, elle peut consister en l'échange ou le partage, mais aussi en l'accès aux informations.

105. S'agissant de l'information confiée aux acteurs du système de santé ou de la donnée produite par le système de santé, nous nous efforcerons de démontrer que bien que celles-ci soient amenées à circuler l'information mais aussi la donnée font l'objet d'une part, d'une protection exhaustive (Titre 1) et, d'autre part, d'une protection effective (Titre 2) de nature à préserver les droits de la personne.

TITRE I. UNE PROTECTION EXHAUSTIVE

« L'environnement numérique interroge le droit à la vie privée, le droit à la protection des données à caractère personnel, le droit au secret qui présentent des liens de connexités. Il existe un grand nombre de textes protecteurs de la vie privée. »[91]

107. **Une protection en fonction de la forme de l'information.** Selon qu'elle figure sur un support magnétique ou qu'elle prenne forme par le verbe, l'information ne va pas faire l'objet d'une protection juridique unique. Si dans le domaine du soin, le secret professionnel constitue, le moyen coutumier de protection de l'information (Chapitre 1), le droit ainsi que la sécurité des systèmes d'information apportent désormais, depuis la numérisation de l'information, des réponses complémentaires (Chapitre 2).

[91] C. BRETON-RAHALI, Le secret professionnel et l'action médico-sociale, Thèse, Nancy, 2014, p. 194

CHAPITRE 1. UNE PROTECTION DE LA PERSONNE PAR L'INFORMATION

109. **L'information de la personne un vecteur de confiance.** Compte tenu de la nature des informations relatives à sa santé et, de l'impérieuse nécessité de préserver sa confiance, l'information préalable de la personne prise en charge, permet aux professionnels de lui rappeler qu'elle a la maitrise des informations la concernant[92]. Elle peut ainsi, depuis la loi du 20 janvier 2016, selon les circonstances de l'espèce, consentir à leur partage entre des professionnels ne faisant pas partie de la même équipe de soins.

110. Elle peut également s'opposer à leur échange ou leur partage entre des professionnels faisant partie de la même équipe de soins. Elle constitue ainsi un vecteur de confiance vis-à-vis du système de soin.

111. **L'information de la personne un moyen d'émancipation.** L'obligation de délivrance de cette information fait, selon les circonstances, l'objet d'un renforcement. Ainsi, le décret n°2016-994[93] précise, qu'elle doit être réalisée, de manière systèmatique et, au cas par cas, lorsque l'équipe de soins est composée de professionnels n'appartenant pas tous à la catégorie des professionnels de santé[95]. Dans ces circonstances, pour que le professionnel soit tenu par cette obligation, le partage de l'information doit être réalisé de manière intra-catégorielle. *A contrario*, l'information sur le droit d'opposition est donnée préalablement mais sans qu'il soit nécessaire pour les professionnels de procéder à la délivrance d'une nouvelle information pour chaque opération de partage.

---

[92] Règl. (UE). PE et Cons. UE préc. art. 13.

[93] Décret n° 2016-994 du 20 juillet 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel 95 C. santé publ. art. R. 1110-2.

112. Ce droit à l'information résulte de la modification des modes de prise en charge de la personne et de l'utilisation des technologies de l'information et de la communication à leur appui. Il participe de l'autodétermination informationnelle et permet ainsi de protéger la personne en lui donnant par cette information le pouvoir de décider de l'utilisation des informations concernant sa santé. Cependant, la protection de la personne par l'information ne peut se réduire à son information. Les atteintes à sa vie privée et à ses droits pouvant exister en dehors du secret partagé, il convient de considérer la protection de l'information à caractère personnel relative à la santé de la personne.

113. **La confiance motrice de la confidence et du partage.** La donnée et l'information constituent des éléments de connaissance. Les informations à caractère personnel, qui sont confiées au professionnel du soin ainsi que les informations auxquelles les professionnels intervenant dans le système de santé peuvent avoir accès sont, en raison de leur objet, d'une nature sensible. Leur divulgation est susceptible de porter atteinte à l'intimité de la personne. L'information révélée peut également lui porter préjudice si elle est susceptible de permettre à un tiers, de lui opposer un refus au bénéfice d'un droit ou d'une prestation.

114. Il convient donc, à la fois, pour des motifs d'intérêt privé mais aussi pour des motifs d'intérêt général que les personnes accordent leur confiance aux professionnels qui participent à leur prise en charge. Cette confiance est indispensable pour que la personne consente à confier aux acteurs de soins une information sur sa santé ou sur sa situation sociale (Section 1). Elle est également indispensable pour que les professionnels puissent, dans l'intérêt de la personne, échanger et partager des informations la concernant. Cette confiance repose sur la protection du contenu informationnel (Section 2) autrement dit, sur des éléments liés à son état de santé et de manière générale à sa vie privée.

Section 1. Une information confiée aux acteurs de soin

« Le principe est que le secret professionnel est fait pour ceux dont la fonction ou profession provoque et exige la confiance du public de telle sorte que la loi imprime implicitement à leurs actes le caractère confidentiel dès lors qu'elle impose ou simplement recommande cette fonction ou profession à la confiance du public. »[94]

116. **Des secrets au secret.** L'article 226-13 du Code pénal, constitue le piédestal du secret professionnel. L'ensemble des professions de santé listées au sein de la quatrième partie du Code de la santé publique sont et, ont été, astreintes sur ces dispositions, au secret par profession. En ce qui concerne, les champs de l'action sociale et médico-sociale, compte-tenu de la diversité des statuts et professions qui les composent, ceux-ci pouvaient être astreints au silence par état ou par profession, par fonction ou mission temporaire. Il existait, de la sorte, une diversité des secrets applicables aux professionnels de l'action sociale et médico-sociale[95]. Selon les circonstances, les représentants d'une même profession pouvaient se trouver assujetties ou non au secret.

117. Cet environnement n'était pas propice à la confiance et, par conséquent, à l'échange et au partage entre les professionnels du soin. La simplification et l'amélioration de la qualité du droit, s'agissant du secret professionnel, résulte de l'homogénéisation des règles en matière de secret, procédant de l'inclusion des professionnels des champs social et médico-social dans la sphère d'échange et de partage (§1). Celle-ci trouve

[94] S. HENNION, *La responsabilité des travailleurs sociaux,* éd. ASH, 2e éd., 2012, p. 129.

[95] B. Py, *« Secret professionnel : Le syndrome des assignats »*, AJ Pénal, 2004, p. 133. Voir également C. BRETON-RAHALI, *Le secret professionnel et l'action médico-sociale,* Thèse, Nancy, 2014, p. 47

son origine dans la modification des modes de prise en charge de la personne désormais construits autour de parcours. Ainsi certaines prises en charge désormais longitudinale contribuent à l'attractivité du secteur sanitaire à l'égard des professionnels des champs social et médico-social (§2).

§ 1. L'inclusion du champ social et médico-social

« L'action médico-sociale est une création récente. (…) La notion est tout d'abord apparue dans le monde médical avant de s'étendre aux travailleurs sociaux.

Le secret professionnel est devenu un secret 'missionnel'. Les règles sont multiples et dispersées selon un processus de codification distinct. »[96]

118. **Une distinction originelle entre le sanitaire et le médico-social.** Alors qu'il ne s'agissait antérieurement que d'une simple obligation morale ou déontologique, l'année 1810 voit poindre la création d'un Code pénal qui apporte pour la première fois une consécration légale au secret. Par ces dispositions, l'article fait désormais de la violation du secret un délit pénal.

119. Dans la continuité de ce processus historique, la première catégorie de professionnels qui sont astreints au secret par les dispositions de l'article 378 du Code pénal regroupe les médecins et autres officiers de santé. Aucune mention ne figure concernant l'un quelconque des professionnels du secteur social. Toutefois, l'article s'inscrit dans une logique séparatiste, puisqu'après avoir identifié les professionnels de santé, il fait référence aux *autres dépositaires*. Autrement dit, le législateur semblait ordonnancer une hiérarchie vis-à-vis *des secrets détenus* en fonction du statut juridique du dépositaire. À côté des professions *nobles* essentiellement composées de professions libérales *« qui conduisent normalement à une organisation assurant à leurs membres une entière*

[96] C. BRETON-RAHALI, *Le secret professionnel et l'action médico-sociale*, Thèse, Nancy, 2014, p. 45.

indépendance »[97] et qui devaient nécessairement jouir de la confiance, demeurait des fonctions de *second ordre*. Ainsi, concernant les professions du champ social et plus particulièrement l'exercice de la profession d'assistant de service social, l'exercice libéral est totalement inexistant. Il en résulte que, bien que les professions de santé et les professions de l'action sociale soient concernées par le même article, il semble exister *ab initio* une distinction de traitement entre ces deux acteurs.

120. Rappelons à ce titre que les professions du champ social sont de création récente.

121. Elles sont, par conséquent, apparues postérieurement à la promulgation de l'article 378 de l'ancien Code pénal. Il en résulte que l'apparition du secret dans l'action sociale est, par définition, plus récente que dans le secteur sanitaire. Malgré cela, sous l'égide de l'ancien Code pénal, concernant le secteur social, le métier d'assistant de service social a bénéficié des dispositions relatives au secret professionnel reconnu par l'ancien article 378 du Code pénal.

> « *La première profession du social assujettie au secret est la plus ancienne historiquement. La profession d'assistante sociale reste canonique par rapport aux autres métiers du travail social et constitue le cadre de référence de l'ensemble des professions du social* »[98].

122. **La violation du secret professionnel uniformément sanctionnée.** Ce n'est qu'en 1992 que la loi introduit au sein du Code pénal à l'article 226-13 une infraction plus générale sanctionnant la violation du

---

[97] J. SAVATIER, *La profession libérale – Etude juridique et pratique*, LGDJ, 1947, p. 63. Université Mémoire, Paris II, 2015

[98] BRETON-RAHALI, C.,. Breton-Rahali, *op. cit*. p. 78.

secret professionnel commise par tous les professionnels [99]. Par ces nouvelles dispositions, la loi ne dresse plus de liste des professions soumises au secret mais astreint au secret les professionnel soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire. Elle oblige, dans un premier temps, à rechercher s'il existe, dans les textes, une disposition assujettissant la profession concernée à l'obligation de se taire. Dans l'hypothèse du contraire, il convient d'apprécier, *in concreto*, la situation pour déterminer si le professionnels considéré et soumis au regard du cadre de son intervention au secret en raison d'une fonction ou d'une mission. Dans le cadre d'une prise en charge thérapeutique, cette situation n'était pas propice à la fluidité et à la qualité de la prise en charge ainsi qu'à l'instauration d'un climat de confiance d'une part, entre le patient, l'usager et les professionnels participant à sa prise en charge et, d'autre part, entre les professionnels eux même puisque ceux-ci se trouvaient dans une situation d'incertitude vis-à-vis de leurs interlocuteurs en ce qui concerne leur obligation de se taire. L'article 226-13 abandonne également la distinction littérale initialement opérée et place l'ensemble des professionnels dépositaires sur un pied d'égalité. Qu'ils soient médecins ou assistants des services sociaux, les professionnels visés par une disposition législative sont exactement soumis à la même obligation, dont le manquement est pénalement réprimé.[100]

123. **Un nouveau secteur résultant d'un mariage de raison.** Le secteur médico-social, tel que nous le connaissons actuellement, résulte de la conjugaison improbable du secteur sanitaire extrêmement réglementé et du secteur social qui, jusque dans les années 70, était peu normalisé. La loi

[99] 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.

[100] CASF, art. L. 411-3 : *« Les assistants de service social et les étudiants des écoles se préparant à l'exercice de cette profession sont tenus au secret professionnel dans les conditions et sous les réserves énoncées aux articles 226-13 et 226-14 du code pénal./La communication par ces personnes à l'autorité judiciaire ou aux services administratifs chargés de la protection de l'enfance, en vue de ladite protection, d'indications concernant des mineurs dont la santé, la sécurité, la moralité ou l'éducation sont compromises n'expose pas, de ce fait, les intéressés aux peines fixées par l'article 226-13 du code pénal. »*

du 30 juin 1975 n°75-535 relative aux institutions sociales et médico-sociales organise ces secteurs. Il s'agit à la fois d'une loi de rupture et d'unification. En effet, elle rompt avec une organisation spontanée résultant d'un processus historique et reposant sur des initiatives essentiellement religieuses et/ou privées. Ensuite, elle opère une unification puisqu'elle envisage les deux secteurs comme un ensemble homogène soumis à un corps de règles communes figurant pour la plupart dans un même Code, à savoir, le Code de l'action sociale et des familles, anciennement Code de la famille et de l'aide sociale.

124. Cette situation ne s'oppose pas à ce que les établissements sociaux proposent des prestations de soins ou encore à ce que les personnes physiques ou morales appartenant au secteur de la santé se préoccupent de questions d'ordre social. Le secteur sanitaire n'est d'ailleurs pas totalement déconnecté du social car l'activité du médecin comporte une dimension sociale. Le médecin a toujours été au plus près des préoccupations quotidiennes de ses patients. C'est là un des aspects inhérents à sa profession, notamment à travers les éléments qui peuvent être portés à sa connaissance lors de consultations à domicile ou encore des informations qu'il peut obtenir lors de l'anamnèse. Cependant, contrairement à la médecine dite « ordinaire », la « médecine sociale » ne prend pas uniquement en considération la biologie humaine. Elle tient également compte de la population, tant du point de vue du contexte social que des conditions sanitaires. Ainsi, les secteurs sanitaire et médico-social, se sont construits au regard des besoins des personnes dont ils assurent la prise en charge.

125. Cela a finalement abouti à ce que le droit sanitaire s'attache aux droits des personnes dont la santé est menacée ou atteinte, tandis que le droit médico-social a envisagé l'état de santé comme constituant un élément parmi d'autres difficultés sociales rencontrées par la personne. De la sorte, jusqu'au début des années 2000, la séparation des deux secteurs s'est progressivement accentuée du fait du droit. Ils se sont démarqués par des systèmes distincts avec une spécialisation des structures les

composants, l'existence de professions et de conditions d'exercice particulières, deux codes mais aussi, des lois spécifiques[101].

126. **Une convergence de la prise en charge.** Bien que des différences considérables subsistent, il est possible d'observer une tendance au rapprochement de ces deux secteurs au cours des dernières années. Les mutations entreprises ont eu pour but de faciliter l'aménagement des parcours de soins entre les professionnels, les établissements de santé et les établissements médico-sociaux. Aussi, à l'aune des difficultés économiques rencontrées dans le secteur sanitaire, elles ont également permis de réduire les dépenses de fonctionnement. Le rapprochement s'est matérialisé par l'adoption de structures[102] et de modes de fonctionnement similaires[105] (y compris au niveau institutionnel[103]) ainsi que par une réforme nécessaire de la réglementation afin de faciliter la continuité de la prise en charge et *de facto*, le travail coordonné, en équipe pluridisciplinaire. De la même manière, ces facteurs ont induit, au sein du Code de la santé publique et du Code de l'action sociale et des familles l'apparition de dispositions semblables, relatives aux droits des usagers et patients ainsi qu'aux obligations des professionnels de ces secteurs.

127. Par conséquent, ces deux secteurs ont notamment pour point commun d'exiger la constitution, pour chaque patient et usager, d'un dossier de suivi. Dans le secteur sanitaire, pour les médecins libéraux, cette obligation est complétée par l'impératif de tenir en *sus « du dossier médical prévu par la loi, (…) une fiche d'observation »*[104]. Pour les

[101] Par exemple, la Loi n° 70-1318 du 31 décembre 1970 portant réforme hospitalière ainsi que la Loi n° 75-535 du 30 juin 1975 relative aux institutions sociales et médico-sociales.

[102] Loi n° 2009-879 du 21 juillet 2009, ayant refondu les groupements de coopération sanitaire, contrats pluriannuels d'objectifs et de moyens, pilotés par régionalesles agences régionales de santé. 105 Les Groupements de coopération.

[103] Par exemple, la Loi n° 70-1318 du portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

[104] C. santé publ, art. R. 4127-45

établissements de soins, elle prend la forme d'une obligation de constituer un dossier médical *« pour chaque patient hospitalisé dans un établissement de santé public ou privé »*[105]. Pour le secteur social et médico-social, le dossier de suivi peut être réalisé sous deux aspects différents. Il peut s'agir d'un projet d'accompagnement personnalisé mais aussi, depuis la loi du 2 janvier 2002 rénovant le Code de l'action sociale et des familles (CASF), le dossier unique de l'usager qui comporte l'ensemble des informations le concernant.

128. **Une conception missionnelle du secret.** En matière de protection de la vie privée, dans le champ sanitaire, suite à l'entrée en vigueur de la loi relative aux droits des malades et à la qualité du système de santé[106], les professionnels de santé, les personnels des établissements et organismes participant à la prévention et aux soins ainsi que tous les professionnels intervenant dans le système de santé se sont retrouvés assujetties à une obligation générale de secret sur le fondement de l'article L. 1110-4 du Code de la santé publique :

> *« 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. »*[107]

129. Par ces dispositions, les éducateurs spécialisés, les psychologues, ainsi que les éducateurs de jeunes enfants pouvaient ponctuellement se retrouver astreint au secret s'ils intervenaient dans le cadre de leurs

[105] C. santé publ, art. R. 1112-2.

[106] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

[107] C. santé publ art. L. 1110-4 dans sa version initiale issue de la Loi n° 2002-303 du 4 mars 2002.

missions auprès d'une personne prise en charge par « *un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins* ».

130. *A contrario,* dans le champ social, la loi rénovant l'action sociale et médicosociale, n'instaura pas de dispositions équivalentes, si ce n'est vis-à-vis de l'usager pris en charge par les établissements, services sociaux et médico-sociaux. Une obligation générale de respect *« des droits et libertés individuels »*[108] comprenant le droit au respect de la vie privée et à la confidentialité des informations est imposée aux professionnels exerçant dans ces structures.

131. Par conséquent, en l'absence de dispositions législatives explicites et en application du principe de légalité criminelle, les informations confiées aux travailleurs sociaux en dehors du secteur sanitaire n'étaient pas nécessairement soumises au secret professionnel, que ce soit d'un point de vue fonctionnel ou missionnel. Par ailleurs, les travailleurs sociaux faisaient l'objet d'une jurisprudence peu encline à admettre qu'ils puissent être soumis au secret professionnel au visa des articles 226-13 et 226-14 du Code pénal**.**

> *« La construction sédimentaire du secret dans l'action sociale accentue la perception de nombreux professionnels selon laquelle le secret professionnel détenu par les professionnels du champ social est plus relatif. Le statut juridique du dépositaire ne constitue pas une hiérarchie entre les secrets détenus, le secret médical n'est pas supérieur aux autres secrets. L'article 226-13 du Code pénal*

[108] CASF, rt.311-3 , artart. L. 311-3dans sa rédaction issue de la Loi n°2002-2 du 2 janvier 2002 rénovant l'action sociale et médico-sociale.

s'applique de la même façon pour tous les professionnels concernés par l'obligation. » [109]

132. Compte tenu de l'importance que représente, pour les personnes prises en charge, la garantie que l'intimité de leur vie privée ne sera pas révélée, les informations recueillies, apprises, comprises ou devinées par les professionnels du secteur sanitaire, médico-social ou social, ont toujours revêtues un caractère secret. Ainsi, C. BRETONRAHALI considère qu'il convient, pour l'instauration d'une véritable relation de confiance avec l'usager, sans laquelle il ne peut être envisagé de soins et d'aide, d'élargir le cercle des professionnels soumis au secret, notamment à l'ensemble des travailleurs sociaux des établissements et services sociaux et médico-sociaux[110]. Elle appelle à une unification de la mosaïque du secteur social par l'harmonisation des dispositions relatives au secret professionnel, à l'image des dispositions de l'article L. 1110-4 du Code de la santé publique. Pour ce faire, elle préconise l'abandon des critères *« de l'assujettissement classique – profession, fonction (…) au profit d'un seul critère polyvalent : la mission »*[111].

133. **Une harmonisation du secret dans le cadre de l'échange et du partage.** Par souci de cohérence entre les différents secteurs et dans le but de permettre l'échange et le partage d'informations entre les professionnels concourant à la prise en charge de la personne, la loi du 26 janvier 2016[112] unifie textuellement et harmonise les dispositions relatives au secret professionnel dans le cadre de l'échange et du partage

---

[109] BRETON-RAHALI,,*op. cit*. p. 99.

[110] La composition des établissements et services sociaux et médico-sociaux est définie à l'art. 312-1

CASF

[111] *Ibid.*

[112] *Ibid.*

d'informations entre les professionnels des secteurs sanitaire, social et médico-social. Il en résulte que :

> *« Toute personne prise en charge par un professionnel […] du secteur médicosocial 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 a droit au respect de sa vie privée et du secret des informations la concernant. Excepté dans les cas de dérogation expressément prévus par la loi, 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. »*[113]

134. Par ce renvoi aux dispositions du I de l'article L. 312-1 du CASF la loi de 2016, poursuit ce travail d'harmonisation et d'unification des secteurs et permet de couvrir un large panel de structures qu'elles soient en charge de l'enfance, des personnes handicapées mais aussi des personnes âgées. Les professionnels concernés sont également bénéficiaires de ces dispositions, puisque ces dispositions comprennent désormais les professionnels du champ sanitaire ou du champ social qui participent à la prise en charge du patient.

135. L'échange et le partage demeurent, par conséquent, subordonnés à la condition que les professionnels soient soumis au secret professionnel et qu'ils participent tous à la prise en charge de la personne. Le principe de proportionnalité existant également au sein de Règlement 2016-679[114] est repris mais deux conditions supplémentaires sont introduites. La

[113] C. santé publ. art. L. 1110-4 al. 1 et al. 2.

[114] Règl. (UE). PE et Cons. UE préc. art. 5.

première emprunte au droit à a protection des données à caractère personnel le principe de finalité[115], en subordonnant la licéité de l'échange et du partage à la communication des informations strictement nécessaires à la coordination ou à la continuité des soins, à la prévention ou à son suivi médico-social et social. La seconde résulte également de la modification des dispositions de l'article L. 1110-4 du Code de la santé publique la loi de 2016.

136. Elle emprunte à l'ancien article 378 du Code pénal l'utilisation d'une liste limitative recensant les professionnels du secteur social et médico-social soumis au secret professionnel et autorisés à échanger et partager de l'information. Par ce truchement, les professions du secteur social et médico-social se trouvent à l'aune des professions de santé, légalement définies. Cette évolution si elle n'introduit pas *stricto sensu* une véritable égalité entre les professions de santé et les autres professions, instaure, au profit de l'usager et du patient, un véritable *« secret collectif, d'équipe lui permettant de comprendre que l'information qu'il communique est confiée à une équipe et non au seul professionnel qui reçoit la confidence »*[116]. Ainsi, la qualité de la prise en charge de la personne et son parcours s'en trouvent améliorer.

137. Bien que l'article figure dans le Code de la santé publique, ces nouvelles dispositions concernent également le champ social et médico-social. Elles rompent avec les inégalités antérieures fondées sur les secteurs professionnels d'intervention et qui concernaient essentiellement les professionnels des établissements et services sociaux et médico-sociaux qui ne relevaient pas de la protection de l'enfance[117].

---

[115] Règl. (UE). PE et Cons. UE préc. art. 5. §1,b)

[116] C. BRETON-RAHALI, *op. cit*, p. 104.

[117] J.-P. ROSENCZVEIG, *Le secret professionnel en travail social et médico-social*, 6e éd., Dunod, 2016, p. 39.

§ 2. Attractivité du secteur sanitaire

140. **Le parcours de santé de la personne et le secret professionnel.** L'harmonisation des dispositions relatives au secret professionnel tient à la confusion de plus en plus importante entre la prise en charge médicale et la prise en charge médicosociale et sociale. Si ce rapprochement est d'abord sensible en ce qui concerne les droits des personnes[118], il l'est également sur le plan institutionnel[119]. Toutefois, l'harmonisation des deux droits – de la santé et du social ou médico-social – n'est que parcellaire. A titre d'exemple, s'agissant de la responsabilité, D. Trucher souligne :

> *« Le domaine de la santé publique et celui de l'action et de l'aide sociales demeurent des domaines d'étude juridique bien distincts, disposant chacun de sa logique propre, bien au-delà du seul domaine de la responsabilité. »*[120]

141. Le constat n'est pas identique concernant le secret professionnel. L'article L. 1110-4 du Code de la santé publique, qui ne prévoyait la soumission au secret professionnel et le partage d'information que dans le

---

[118] D. Truchet, *« La genèse de la construction des droits sanitaire et médico-social »*, RDSS 2014, p. 495. L'uniformisation est particulièrement visible en ce qui concerne la participation des individus dans la prise en charge. Sur ce point v. D. Cristol, *« Le droit à la participation dans les lois des 2 janvier et 4 mars 2002 », RDSS* 2012, p. 453. +

[119] Avec, notamment, la création des agences régionales de santé par la loi dites « HPST » (Loi n° 2009879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires) ; *Ibid.*

[120] C .-A. Dubreuil, *« Les responsabilités sanitaire et sociale, convergences et divergences », RDSS* 2015, p. 75 ; S'agissant des droits des personnes certains auteurs soulignent également une convergence en demiteinte par exemple dans la prise en charge du vieillissement : B. Apollis et G. Duthil, *« Le vieillissement un enjeu de santé publique : à quand une réelle convergence des droits sanitaire et médico-social ? », RDSS* 2018, p. 538.

seul cadre sanitaire[121], a connu, comme nous l'avons précédemment mentionné[122], une refonte lors de la loi du n°201641 du 26 janvier 2016[123]. Au travers de ce texte législatif ce n'est plus uniquement le parcours de soin qui constitue le mode unique de prise en charge de la personne, il est désormais question du parcours de santé, voire, de vie. Ces notions ne sont pas définies par les textes législatifs ou règlementaires, il s'agit de jalons pour une gouvernance efficace de l'action des acteurs des systèmes de soins et du système social et médicosocial. C'est en effet, les lignes des politiques gouvernementales qu'il faut chercher un éclaircissement. Le ministère de la santé affirme depuis la loi « HPST » de la volonté d'adopter une approche globale de la santé des personnes en associant parcours de soin, parcours de santé et parcours de vie[124]. Cette volonté trouve une expression forte dans les travaux préparatoires de la loi du 26 janvier 2016[125], le « comité des sages » désigné pour formuler des

---

[121] M.-F Callu constatait alors la nécessité d'harmoniser les législations : *« Toutefois, il peut se trouver des situations professionnelles, non couvertes par les textes précités, dans lesquelles une prise en charge particulière nécessite que d'autres acteurs disposent d'un minimum d'informations, par exemple à caractère médical, pour adapter l'action à la vulnérabilité réelle de la personne suivie »* (M.-F. Callu, *« État des lieux juridique et pratique. D'un point de vue juridique, secret professionnel et partage d'informations sont appréhendés différemment selon qu'ils s'exercent dans le secteur sanitaire ou dans celui du médico-social. Or, en pratique, ces deux secteurs sont complémentaires et ne peuvent être imperméables aux échanges pour le bien-être des personnes prises en charge »*, *JA* 2013, n° 474, p. 19, v. *supra* n° 68 et svt.

[122] V. *supra* n° 76.

[123] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé

[124] Le ministère de la santé donne la définition de ces notions : « Les parcours de santé, qui articulent les soins avec, en amont, la prévention en santé et sociale et, en aval, l'accompagnement médico-social et social, le maintien et le retour à domicile. Les parcours de soins, qui permettent l'accès aux consultations de 1er recours et, quand cela est nécessaire, aux autres lieux de soins : hospitalisation programmée ou non (urgences), hospitalisation à domicile (HAD), soins de suite et de réadaptation (SSR), unité de soins de longue durée (USLD) et établissements d'hébergement pour personnes âgées dépendantes (EHPAD). Les parcours de vie, qui envisagent la personne dans son environnement : famille et entourage, scolarisation, prévention de la désinsertion professionnelle, réinsertion, logement… » (disponible sur : <https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/parcours-des-patients-et-desusagers/article/parcours-de-sante-de-soins-et-de-vie>.

[125] V. notamment : L. Véran, B. Laclais, J.-L. Touraine, H. Goeffroy, R. Ferrand, *Rapport fait au nom de la commission des affaires sociales sur le projet de loi relatif à la santé*, n° 2673.

recommandations en amont de la proposition de loi avait par ailleurs mis en exergue la nécessité du décloisonnement[126]. Pour que cette prise en charge globale soit possible tout en assurant le respect de la vie privée des personnes, il était nécessaire de généraliser le secret professionnel.

142. **Condition préalable de l'infraction et personnes soumises au secret.** Ainsi, que nous l'avons esquissé en amont[127], l'infraction punissant la violation du secret professionnel suppose, en outre de la réunion des éléments traditionnels de l'infraction, l'existence de conditions préalables. Celles-ci consistent en des éléments préexistants, en ce qu'elles sont « *nécessairement visées par les textes d'incrimination mais qu'elles ne font pas véritablement partie du comportement à sanctionner* »[128], elles sont « *l'interface entre le droit pénal et le droit extrapénal, entre la règle pénale et le commandement extrapénal dont celle-ci sanctionne la violation. Elle sont dans la loi pénale le témoignage de la règle sanctionnée* »[129]. Ainsi, les conditions préalables sont à la fois préexistantes et dénuées de coloration pénale. Concernant l'infraction de violation du secret professionnel elle exige que la révélation de l'information soit le fait d'« *une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire* »[130]. C'est donc à l'extérieur du Code pénal qu'il faut rechercher les personnes astreintes au secret.

143. **Les personnes intervenant dans le système de santé.** Si les dispositions du Code de l'action social et des familles permettent d'affirmer qu'il existe toujours une distinction au regard des missions et

---

[126] Comité des « sages », *Un projet global pour la stratégie nationale de santé, 19 Recommandations du comité des « sages »*, juin 2013, (disponible en ligne sur <https://solidarites-sante.gouv.fr/IMG/pdf/rapportcordier-SNS-sages.pdf>).

[127] V. *supra*

[128] E. DREYER, *Droit pénal général*, LexiNexis, 2013, n° 216.

[129] L. ROUSVOAL, *L'infraction composite, essaie sur la complexité en droit pénal*, thèse Rennes I, 2011, n° 162.

[130] C. pén. art. 226-13.

des fonctions des professionnels de l'action sociale et médico-sociale. Les dispositions du Code de la santé publique permettent d'affirmer une relative harmonisation dans le cadre du système de santé. Dans sa version issue de la loi du 4 mars 2002, l'article L. 1110-4 du Code de la santé publique, dispose que ce secret *« […] s'impose à tout professionnel de santé, ainsi qu'à tous les professionnels intervenant dans le système de santé »*. La mention des professionnels de santé disparait à l'occasion de la loi du 26 janvier 2016, ainsi : *« Il s'impose à tous les professionnels intervenant dans le système de santé »*. Cette mention était en effet surabondante, par ailleurs, la disposition n'opère aucune différenciation entre professionnel de santé et professionnel de l'action sociale ou médico-sociale. En effet, le système de santé est *attractif.* Cette attractivité s'explique par le fait que certaines prises en charge, uniquement médicales à l'origine, se révèle réduite dans leur efficacité si elle ne s'accompagne pas d'un suivi social et médico-social. Les travaux préparatoires de la loi du 26 janvier 2016 mettent en exergue les spécificités de ces prises en charges complexes. Il en est ainsi de la prise en charge des personnes âgées, au travers du dispositif PAERPA[131], dont le rapport fait au nom de la commission des affaires sociale fait mention en précisant :

144. *« De nombreux patients se retrouvent dans une situation complexe à la fois médicale et psychosociale. L'association de plusieurs pathologies, leur degré de sévérité ou le recours à des hospitalisations répétées d'une part, l'isolement ou la vulnérabilité sociale, la situation de dépendance d'autre part justifient l'organisation d'un parcours adapté et centré sur le patient.»*[132]

[131] Programme des Personnes Agées En Risque de Perte d'Autonomie, fondé sur l'article 48 de la Loi de financement de la sécurité sociale (LFSS) pour 2013, et s'inscrivant dans le cadre de la Stratégie Nationale de Santé.

[132] L. Véran, B. Laclais, J.-L. Touraine, H. Goeffroy, R. Ferrand, *Rapport fait au nom de la commission des affaires sociales sur le projet de loi relatif à la santé*, n° 2673, p. 36.

145. Il est encore précisé que les prises en charge complexe concernent aussi les hospitalisations à domicile et la prise en charge du handicap[133]. Si le patient est au centre de la prise en charge, le médecin traitant en est le pivot organisationnel[134], aussi c'est en quelque sorte la prise en charge sanitaire qui absorbe, du point de vue juridique, les autres modes de prise en charge.

146. **L'indifférence quant à la profession ou à la fonction.** Il appert que l'extension du champ d'application du secret professionnel s'appréhende eu regard à l'intervention dans le système de santé. Cette intervention est liée à un mode de prise en charge dont la pluridisciplinarité est extensive. Les professionnels, qu'importe qu'ils s'agissent de professionnels relevant du secteur social ou médico-social, sont soumis au secret dès lors qu'ils interviennent dans la prise en charge global du patient. En ce sens, notre affirmation selon laquelle les préconisations de certains auteurs sont dépassées, se trouve vérifiée. Tandis que les motivations qui exigeaient une soumission au secret professionnel relevaient de considérations propres à la profession[135] ou aux fonctions, c'est au grès des missions dans le système de santé par le biais de la prise en charge du patient qu'il faut désormais analyser cette question.

Section 2. Un contenu informationnel protégé

[133] *Ibid.* p. 37.

[134] *Ibid.* p. 32

[135] Sur ce point v. notamment M. COUTURIER, *Pour une analyse fonctionnelle du secret professionnel*, thèse Lille II, 2004, n° 85 et svt.

147. **Une protection de l'information adaptée et permissive**. Le nombre de professionnels assujettis au secret professionnel n'a cessé d'augmenter depuis la loi du 4 mars 2002. Dans le cadre de l'activité de soin, il intègre désormais des professionnels ne concourant pas dans la réalisation d'un acte thérapeutique mais qui participent au système de santé. En raison de sa portée générale, il convient de s'interroger l'infraction de secret professionnel constitue l'une des réponses les plus adaptée à la divulgation illicite d'informations à caractère secret (paragraphe 1). Le droit s'il sanctionne la révélation illicite d'informations couvertes par le secret professionnel, ménage des hypothèses dans lesquelles la révélation est permise (paragraphe 2).

149. § 1. Une divulgation sanctionnée

« Il y a plus de peine à garder un secret qu'à tenir un charbon ardent dans sa bouche »

150. Socrate

151. **Une approche traditionnelle.** Nous ne pouvions considérer la circulation et la protection de l'information sans envisager la sanction de sa divulgation. Ces développements sont nécessaires à notre démonstration, ils ne peuvent, pour autant, être novateurs. Que l'information à caractère secret soit révélée par le *logos*, c'est-à-dire par la parole, ou en ayant recours à un quelconque outil numérique, vis-à-vis du secret professionnel, les éléments constitutifs de l'infraction ainsi que la réponse pénale ne dérogent pas au droit commun. Nous ne soustrayons donc pas à un rappel des conditions de la divulgation d'une information à caractère secret. Nous invitons cependant le lecteur, à se référer, en complément de nos développements aux travaux de M. COUTURIER[136], B. PY[137], C. ZORN[138] en ce qu'ils concernent également la distinction entre le secret professionnel et d'autres divulgations sanctionnées au titre de la confidentialité, et du devoir de réserve. Nous invitons également le lecteur à consulter les travaux de C. BRETON-RAHALI[139], A. NIETO[140].

[136] M. COUTURIER, Pour une analyse du secret fonctionnel, Thèse Lille, 2004.

[137] B. PY, Le secret professionnel, L'Harmattan, coll. « La justice au quotidien », Paris, 2005.

[138] C. ZORN, Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé, avant-propos B. Py, préf. I. de Lamberterie, PUN, 2010, p. 35 et svt.

[139] C. BRETON-RAHALI, Le secret professionnel et l'action médico-sociale, Thèse, Nancy, 2014.

[140] A. NIETO, La vie privée à l'épreuve de la relation de soin. Thèse, Montpellier, 2017. 144 C. santé publ. R. 4127-4.

152. Nous l'avons exposé en introduction de nos travaux, le secret professionnel était *ab initio* une obligation déontologique élémentaire.

> *« Le secret professionnel institué dans l'intérêt des patients s'impose à tout médecin dans les conditions établies par la loi. 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 »*[144]

153. Il constitue également depuis 1810 une infraction pénale, dont la violation sanctionne depuis la révélation illicite d'une information à caractère secret. Dans le domaine de la santé, cette sanction a pour objet de préserver la confiance en l'institution de la médecine[141] et par ce moyen, l'intimité de la vie privée, afin de garantir la pérennité de notre système de santé et donc la santé publique entendue comme la bonne santé de la population.

154. **Les professionnels de la technique également assujettis**. Avec l'assimilation du numérique par le système de soin, le secret n'est plus, depuis la loi de 4 mars 2002, exclusivement confiné à la relation thérapeutique. Il couvre désormais, *« l'ensemble des informations concernant la personne venues à la connaissance du professionnel, de tout membre du personnels de ces établissement, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tous les professionnels intervenant dans le système de santé. »*[142]

155. De ce fait, à l'ensemble des professionnels précédemment évoqués, s'adjoignent les professionnels intervenant dans la gestion technique de l'information. Ainsi, indépendamment de la forme de

---

[141] B. PY, *« Le secret professionnel et le signalement de la maltraitance sexuelle. L'option de conscience : un choix éthique », Archive de politique criminelle* 2012/1, n°34, p. 75.

[142] C. santé publ. art. L. 1110-4 §1, al. 2.

l'information, sont également soumis au secret professionnel, lorsque l'hébergement de données à caractère personnel est externalisé, les hébergeurs de données de santé à caractère personnel certifiés ou agréés et les personnes placées sous leur autorité qui ont accès aux données déposées, article L. 11118, V. al. 2 du Code de la santé publique. De la même manière, depuis la loi du 31 juillet 1991[143], les établissements de santé qu'ils soient de droit privé ou public, doivent, dans le cadre du programme de médicalisation des systèmes d'information (PMSI)[144], procéder à l'analyse de leur activité médicale et transmettre *« les informations relatives à leurs moyens de fonctionnement et à leur activité »* aux services de l' État et de l'Assurance maladie. Concernant l'activité de médecine, chirurgie, obstétrique (MCO) mais aussi l'odontologie, cette analyse est fondée sur le recueil systématique des informations administratives et médicales, qui constituent le résumé de sortie standardisé. Le traitement de ces informations n'échappe pas au secret professionnel. Ainsi, les données figurant dans le dossier médical[145] qui sont, à cette occasion, recueillies pour chaque patient, par des professionnels soumis au secret, sont transmises au médecin responsable de l'information médicale (DIM) afin qu'il soit procédé à l'analyse de l'activité médicale de ces établissements. Celui-ci est soumis au secret professionnel[146]. Il en est de même des personnels placés ou détachés auprès de lui et qui travaillent à l'exploitation de données nominatives, sous son autorité. De la même manière, les personnels qui relèvent de la direction des systèmes d'information (DSI) ainsi tous membres du personnel et les tiers, intervenant sur le matériel, les logiciels utilisés pour le traitement des données sont également soumis au secret professionnel.

[143] Loi n° 91-748 du 31 juillet 1991 portant réforme hospitalière.

[144] C. santé publ. art. L. 6113-7 et L. 6113-8.

[145] La composition du dossier médical est mentionné à l'article L. 1113-1 du Code de la santé publique.

[146] C. santé publ. R. 6113-5 et R. 6113-7.

156. **Les conditions constitutives de l'infraction.** L'obligation de secret professionnel repose sur la divulgation d'une information à caractère secret. Les éléments matériels constitutifs de l'infraction de violation du secret professionnel n'ont pas évoluées. Ce sont les mêmes que sous la rédaction de l'article 378 du Code pénal. Cette révélation illicite peut prendre différentes formes, auxquelles le droit réagit désormais, au titre de l'article 226-13 du Code pénal, indifféremment. Il peut s'agir, à titre d'exemple, d'une publication dans une revue scientifique ou encore dans une revue destinée au grand public. La révélation peut également prendre la forme d'une confidence ou d'une dénonciation. En ce qui concerne l'élément moral, il s'agit d'un dol général ainsi, il n'est pas exigé que cette révélation soit motivée par une intention de nuire, il est fondamental qu'elle ne résulte pas d'une simple imprudence ou négligence. Ainsi, l'individu fautif doit avoir conscience de révéler un secret et de ne pas s'être trouvé dans une situation pour laquelle il existe un fait justificatif relevant de l'ordre ou de l'autorisation de la loi. Enfin, pour que l'acte soit préjudiciable, les éléments révélés doivent être suffisamment précis et de nature à permettre l'identification de la personne.

157. Si tous les éléments constitutifs de l'infraction sont réunis, la responsabilité pénale du dépositaire du secret peut être engagée sur le fondement de l'article 226-13 du Code pénal. En revanche, si l'infraction de violation du secret professionnel n'est pas constituée, le transgresseur n'échappe pas nécessairement à ses responsabilités. Il peut, en effet, voir sa responsabilité civile engagée. A ce titre, un médecin spécialisé en biologie médicale ou médecine de laboratoire pourrait voir sa responsabilité engagée s'il communiquait à une autre personne que le médecin traitant ou son patient, les résultats d'un prélèvement.

§ 2. Des révélations permises

159. M. Bénéjat-Guerlin l'illustre au sein de ses travaux relatifs à la protection pénale du secret professionnel dans le domaine de la santé, *« c'est au travers des hypothèses de révélations non punissables que l'on peut jauger la protection pénale propre au secret médical »*[147].

160. Sur le plan supranational et communautaire, la Convention européenne des droits de l'Homme (Conv. EDH), ratifiée par la France depuis 1973[148] dispose en son article8 relatif au droit au respect de la vie privée et familiale :

> *« 1.Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*
> *2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sureté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »*[149]

161. Rappelons que c'est dans un premier temps, la Cour de justice des Communautés Européennes (CJCE) dans son arrêt *X. c/ Commission* du 5

---

[147] BENEJAT-GUERLIN. *« Que reste-t-il de la protection pénale du secret médical ? », AJ Pénal* 2017, p. 368.

[148] Loi n° 73-1227 du 31 décembre 1973 autorisant la ratification de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et de ses protocoles additionnels n° 1, 3, 4 et 5. Voir également, F. VILLEVIEILLE... Voir également, F. Ville, *« La ratification par la France de la Convention européenne des Droits de l'homme* »,». Annuaire Français de Droit International, 1973 p. 922.

[149] Convention européenne des droits de l'Homme (Conv. EDH), art. 8.

octobre 1994[150] qui a affirmé, en se fondant sur les dispositions de l'article 8 précité, que le droit pour tout individu de tenir secret son état de santé constituait une composante du droit au respect de sa vie privée[151].

162. **Une conception relativiste du secret.** La Cour européenne des droits de l'Homme (CEDH) a, sur le fondement du paragraphe 2 du même article, affirmé le caractère relatif du droit au respect de la vie privée et, du secret professionnel. D'un autre côté, elle a également développé, au regard du même paragraphe, une jurisprudence opérant un *« contrôle strict (…) sur les ingérences au regard du droit à la vie privée »*. La CEDH a donc eu à connaitre dans le cadre de plusieurs affaires relatives à la protection de la vie privée, de l'articulation entre la protection des **données** à caractère personnel relatives à la santé et de la relativité du secret professionnel[152].

163. **Un contrôle strict des ingérences.** La première de ces affaires, Z. c/ Finlande [153] concernait la révélation de la séropositivité d'une requérante dans le cadre d'une procédure pénale engagée à l'encontre de son époux. En l'espèce, celui-ci était poursuivi pour plusieurs viols, à la suite desquels il avait transmis délibérément le VIH à ses victimes. Il était nécessaire de démontrer, pour retenir sa culpabilité, que sa femme était séropositive et l'avait contaminé. L'épouse ayant refusé de témoigner contre son mari, ses médecins furent, conformément au droit Finlandais, contraints par ordonnances, de témoigner de l'infection de celle-ci par ce virus. Dans ce cadre, les dossiers médicaux la concernant avaient également été saisis à l'hôpital où elle était suivie. Ces éléments avaient été

[150] CJCE, 5 octobre 1994, X. c/ Commission, aff. C-404/92 P, Rec. I-128, *D.* 1995, p. 421, note J.-L. CLERGERIE.

[151] 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 A. LECA (dir.),*»*. Le secret médical, CDSH , n° 15, LEH, 2012, pp. 51-66.

[152] I. LAURENT-MERLE, *« Le secret des données médicales et la protection de la vie privée : un secret de polichinelle ? »*, *D.»*. 2000, p. 521.

[153] Cour EDH 25 février 1997, Z. c/ Finlande, 22009/93.

joints en intégralité au dossier d'enquête. Au cours de cette procédure pénale, l'identité de la requérante avait été divulguée et les données de santé concernant sa séropositivité figuraient dans l'arrêt de la cour d'appel[154].Dans le cas d'espèce, s'agissant de la divulgation de données à caractère personnel relatives à la santé, la Cour avait conclu sur le fondement du paragraphe 1 de l'article 8 [155] de la Convention à une ingérence dans le droit au respect de la vie privée et familiale. Selon la Cour, *« le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique de toutes les Parties contractantes à la Convention. Il est capital non seulement pour protéger la vie privée des malades mais également pour préserver leur confiance dans le corps médical et les services de santé en général...»*

164. À travers cette décision, la CEDH est allée plus loin dans la construction de sa jurisprudence relative à la protection des données de santé[156]. Elle a ainsi articulé « *sa jurisprudence sur la protection des données de santé autour de ce principe [de sacrosaint secret professionnel] en s'appliquant à en rappeler l'essence »*. Rappelons, à cette occasion, que la protection des données à caractère personnel relatives à la santé, excède la simple divulgation d'une information à caractère secret et ainsi le droit à la vie privée puisqu'elle comprend également les autres droits et libertés de la personne[157], à titre d'exemple, le droit à la non-discrimination reposant sur des données à caractère personnel. Toutefois, la Cour a parallèlement admis au cours de la même

---

[154] *Ibid.*

[155] *« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. »* Notons que la Convention ne fait pas expressément de distinction entre la notion de secret professionnel ou de confidentialité, elle renvoie simplement au respect de la vie privée.

[156] S. GAMBARDELLA, *« Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé* »,». RDSS 2016, p. 271.

[157] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, art. 70-18 à 70-24.

affaire « *que la protection de la confidentialité des données médicales (…) peut parfois s'effacer devant la nécessité d'enquêter sur des infractions pénales, d'en poursuivre les auteurs et de protéger la publicité des procédures judiciaires (…), lorsqu'il est prouvé que ces derniers intérêts revêtent une importance encore plus grande »*[158]**.**

165. À ce titre, elle a apprécié si *« l'atteinte à la vie privée et familiale de la requérante provoquée par les mesures incriminées était (…) soumise à d'importantes restrictions et assortie de garanties effectives et suffisantes contre les abus »*[159].La Cour en a finalement conclu que si « *la saisie des dossiers médicaux de la requérante et leur adjonction au dossier d'enquête ne constituait pas une violation des dispositions de l'article [8 de la Convention] »*, la divulgation de son identité et de l'état de santé de la requérant avait violé ces mêmes dispositions.

166. **L'exclusion de révélations guidées par un intérêt privé.** Dans un second arrêt, *M. S c/ Suède*[160], une requérante contestait, à la suite d'une demande portant sur le versement d'une prestation sociale, la divulgation de données à caractère personnel relatives à santé. Cette révélation résultait de la transmission de son dossier médical, par un service de gynécologie, à la Caisse de sécurité sociale Suédoise. La communication de ces données à caractère personnel relatives à sa santé était nécessaire à la Caisse pour apprécier la recevabilité de la demande de pension d'invalidité consécutivement à un accident professionnel lui ayant occasionné une blessure au dos. Les données contenues dans le dossier excédaient la demande de la Caisse puisqu'elles portaient également sur un avortement subi antérieurement par la requérante. Cette information démontrant

[158] Cour EDH 25 février 1997, Z. c/ Finlande, préc. § 97.

[159] Cour EDH 6 septembre 1978, Klass et autres c/ Allemagne, 5029/71. Allemagne.

[160] Cour EDH, 27 août 1997, M. S. c/ Suède, 20837/92.

l'ancienneté des problèmes de dos de la requérante avait conduit au rejet de sa demande.

167. Dans le cadre de cet arrêt, la Cour rappelle que la confidentialité des données à caractère personnel et, *in casu,* des données relatives à la santé, revêtent, au regard de l'article 8 de la Convention Européenne des Droits de l'Homme, une importance fondamentale vis-à-vis du droit au respect de la vie privée mais aussi à l'égard de la préservation de la confiance des personnes dans le corps médical et d'une manière générale dans le système de santé. Bien que *« le secret n'empêche pas […] la divulgation d'informations à une autorité publique, si cette divulgation est obligatoire en vertu d'une loi ou d'un décret »,* la Cour conclut à la violation de l'article 8 de la Convention, considérant que le droit Suédois ne définissait pas en des termes suffisamment précis et intelligibles l'étendue et les modalités d'exercice du pouvoir d'appréciation accordé aux autorités compétentes.

168. En l'espèce, si l'on se réfère aux dispositions de l'article 6 du Règlement générale sur la protection des données et à son considérant 43, la requérante n'avait pas consentie au traitement de ses données à caractère personnel relatives à sa santé à cette fin. Il en résulte que la protection pénale semble s'amenuiser. Cependant, celle-ci ne faiblira jamais au point d'admettre des révélations dans le seul intérêt privé. De ce point de vue, le secret médical demeure une règle déontologique et une infraction pénale instaurée *« non seulement pour protéger la vie privée des malades mais également pour préserver leur confiance dans le corps médical et les services de santé en général »*, selon la formule constante de la CEDH[161].

169. **Un nombre considérable de dérogations.** Notre droit national, connais un nombre considérable de dérogations au secret professionnel de l'ordre de l'ordre et de l'autorisation de la loi. Rappelons à cette occasion,

[161] *Ibid.*

que l'autorisation de la loi admet la révélation ou le partage d'informations couvertes par le secret professionnel sans pour autant être systématiquement obligatoire. L'échange et le partage d'informations à caractère personnel relatives à la santé, lorsqu'ils sont réalisés dans les conditions définies à l'article L. 1110-4 du Code de la santé publique entre dans le champ des révélations autorisées. Ce partage existait antérieurement à sa codification au sein du Code de la santé publique mais en l'absence de dispositions légales, celui-ci était illicite.

170. Ce n'est que suite à l'adoption de la loi du 4 mars 2002, que deux ou plusieurs professionnels de santé ont pu 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. »*[162] Nous l'avons précédent précisé, cette révélation est désormais autorisée entre tous les professionnels assujettis au secret dans le respect des nouvelles conditions définies codifiées par la loi de 2016[163] au même article L. 1110-4.

> *« 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. »*

[162] C. santé publ. art. L. 1110-4 dans sa rédaction issue de la Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

[163] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé 168 C. civ., art. 55.

171. Le droit français comporte d'autres dérogations relevant de l'ordre ou de l'autorisation de la loi. A titre d'exemple, les déclarations obligatoires composées des certificats médicaux ainsi que des déclarations telles que les naissances[168] et décès[164].

172. Figure également parmi ces déclarations obligatoires le signalement de maladies infectieuses qui font l'objet d'une transmission de données individuelles à l'autorité sanitaire par les médecins et les responsables des services et laboratoires de biologie médicale publics et privés. Ces transmissions, sont réalisées lorsqu'elles nécessitent une intervention urgente locale, nationale ou internationale ou si leur surveillance est nécessaire à la conduite et à l'évaluation de la politique de santé publique[165]. Le nombre de ces maladies a été récemment élargi puisqu'il comporte désormais[166] la déclaration obligatoire des cas de Zika portant ainsi la liste des affections visées par l'article D. 3113-6 du Code de la santé publique à D. 3113[167].

173. Entre dans le champ de l'autorisation de la loi, l'analyse de l'activité et de la facturation des établissements de santé, qu'ils soient publics ou privés. Les praticiens exerçant au sein de ces établissements transmettent au médecin responsable de l'information médicale, les données de santé nominatives nécessaires à cette analyse[173]. Dans ce cadre, le médecin ainsi que les personnels du service ou département de l'information médicale placés sous son autorité qui organisent le recueil, la circulation et le traitement des données nominatives, sont soumis au

---

[164] C. civ., art. 78.

[165] C. santé publ, art. L. 3113-1.C. santé publ.

[166] *Ibid.*

[167] La liste des maladies infectieuses dont la déclaration est obligatoire est disponible à partir du site de l'Institut national de veille sanitaire (InVS), accessible à l'adresse suivante : invs.santepubliquefrance.fr. 173 C. santé publ, art. L. 6113-7 al. 1. En ce qui concerne les Groupements hospitaliers de territoire (GHT) et l'obligation, pour les établissements qui en font partie, de transmettre au département de l'information médicale de territoire leurs données d'activité, se référer aux dispositions des articles R. 6113-11-1 C. santé publ.

secret professionnel[168]. Cette dérogation compte également les traitements à des fins de recherche dans le domaine de la santé[169], sur lequel nous reviendrons plus tard dans le cadre de nos développements.

174. En ce qui concerne, l'article 226-14 du Code pénal, celui-ci a, depuis 1994, connu plusieurs réformes. On ne compte pas moins de huit modifications qui ont étendu les atteintes admises au principe du secret professionnel. Ces modifications concernaient notamment l'ajout, par la loi de 1998[170], à l'alinéa 1 de l'article précité, de dispositions générales visant l'ensemble des professionnels soumis par état ou par profession, par fonction ou mission au secret professionnel et qui étaient susceptibles d'être amenées à constater des atteintes sexuelles commises sur des mineurs ou des personnes vulnérables. Enfin, la loi sur la sécurité intérieure [171] a en 2003, intégré à l'article 22614 du Code pénal un troisièmement permettant aux professionnels de la santé ou de l'action sociale de signaler à l'autorité administrative le caractère dangereux de personnes qui détiennent une arme ou qui ont manifesté l'intention d'en acquérir une. Compte tenu du nombre de dérogations introduites successivement au principe de secret professionnel, on est en droit de constater qu'*« en systématisant les exceptions et dérogations, le secret professionnel est aujourd'hui dévalorisé »*[172].

[168] C. santé publ, art. R. 6113-5.

[169] Décret n° 2018-342 du 7 mai 2018 complétant la liste des maladies faisant l'objet d'une transmission obligatoire de données individuelles à l'autorité sanitaire.

[170] Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs.

[171] Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.

[172] B. PY*« Le secret professionnel* ». Harmattan, coll. « La justice au quotidien. » Paris, 2005, p. 9.

CONCLUSION DU CHAPITRE 1

176. **Une protection par l'information**. Dans le cadre la prise en charge au sein du système de santé les informations concernant la personne sont protégées, en application de l'article L. 1110-4 alinéa 1 du Code de la santé publique, par le secret professionnel de l'article 226-13.

> « *Toute personne prise en charge par un professionnel de santé, [...] 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 a droit au respect de sa vie privée et du secret des informations la concernant.* »

177. Ce partage étant restreint à un nombre limité de professionnels, dans le cadre des anciennes dispositions résultant de la loi du 4 mars 2002, la réforme réalisée par loi de modernisation de notre système de santé, a permis, d'étendre le secret partagé décris aux dispositions du II et du III de l'article L. 1110-4 en ayant recours au secret professionnel.

178. La combinaison de ces dispositions permet le partage d'informations à caractère personnel de manière maitrisée avec un ou plusieurs professionnels identifiés participant à la prise en charge d'une même personne, à condition 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.

179. En l'absence d'échange et de partage ou lorsque l'échange et le partage ont été réalisé sans respecter les dispositions précités le secret professionnel, vient sanctionner la divulgation de l'information à caractère secret. Cette divulgation sanctionnée résulte de la révélation d'un élément de connaissance mémorisé par la personne tenue au secret que cette

mémorisation proviennent de ce qu'elle a entendu, lu ou vu y compris lors de la consultation d'un fichier.

180. Le secret professionnel comme moyen traditionnel de protection de l'information permet donc une protection exhaustive qui ne s'efface qu'en présence d'une valeur sociale protégée jugée supérieur et reconnue par une disposition légale.

181. Le secret professionnel dépasse désormais le cadre de la relation de soin. Il considère les professionnels de la technique, qui sont susceptible de connaitre de l'information de santé dans le cadre de la manipulation des données ou de leur intervention sur l'outil numérique. La divulgation d'une information à caractère secret pénalement sanctionnée voie donc son périmètre élargie et permet ainsi de de circonscrire les atteintes à la vie privé en sanctionnant les révélations illicites. Il existe traditionnellement, une liste considérable de dérogations au secret professionnel instituées par la loi, dans la nécessité d'établir une communication maîtrisée de l'information protégée. Il en résulte que la protection pénale semble s'amenuiser.

182. Cependant, si nous pouvons toutefois regretter qu'elles constituent une systématisation des exceptions et dérogation au secret professionnel. Ces dérogations sont justifiées, par des motifs d'intérêt public et autorisent la circulation de l'information en raison de valeurs sociales protégées jugées supérieures. Le secret partagé entre dans le champ de ces révélations permises. Bien qu'il puisse de prime abord, paraître d'intérêt privé car consentie dans l'intérêt du patient, cette dérogation constitue au même titre que les autres une réponse à la protection d'une valeur sociale jugée supérieur, en l'occurrence, la santé de la population, la qualité des soins et l'efficience de la prise en charge.

183. La donnée à caractère personnel est définie à l'article 4 §1 du Règlement du 27 avril 2016 comme *« toute information se rapportant à une personne physique identifiée ou identifiable […]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 ». Pour les droits et libertés de la personne comprenant le droit à la protection de ses données ainsi que le droit au respect de sa vie privée soient respectés, il est indispensable et déterminant que les données concernée ou leur traitement puissent permettent directement ou indirectement de l'identifier.

184. Le droit à la protection des données à caractère personnel est issu du droit à la vie privée, il s'est progressivement émancipé. Cependant, la donnée demeure une information ayant acquis une valeur ajoutée d'ordre technologique. Celle-ci rend plus aisée sa circulation mais la donnée n'en demeure pas moins une information. Elle peut donc être protégée, par le droit, en ayant recours aux moyens traditionnels de protection de la vie privée auquel le secret professionnel appartient.

185. Il existe, en raison de valeurs sociales protégées jugées supérieures, un nombre considérable de révélations permises. Le secret partagé relève de ces exceptions au principe du secret En raison de l'attractivité du secteur sanitaire, le secret professionnel constitue désormais un moyen facilitant l'échange et le partage maitrisé de l'information par l'assujettissant harmonisé des professions des champs social, médico-social et sanitaire.[173] Il contribue également à la pérennité du système de santé en permettant la circulation de la donnée du professionnel ayant recueillie l'information à des fins thérapeutiques aux professionnels du département de l'information médicale afin que celui-ci puisse l'exploiter et la transmettre à des fins d'analyse de l'activité médicale[174].

[173] C. santé publ. art. L. 1110-4.

[174] C. santé publ. art. L. 6113-7 et L. 6113-8.

186. Le délit de violation du secret professionnel constitue donc, en raison de ses éléments caractéristiques, une réponse adaptée permettant de sanctionner la divulgation d'une information à caractère secret quelle que soit la forme de cette divulgation.

CHAPITRE 2. UNE PROTECTION DE LA PERSONNE PAR LA DONNEE

188. **Une protection de la personne proportionnelle aux risques pour sa vie privée.** Le Règlement général à la protection des données a pour objet de créer un environnement favorable à la libre circulation des données à caractère personnel. Le principal obstacle à cette circulation à l'échelle de l'Union européenne, résultait de la multiplication des règlementations nationales. Les institutions législatives de l'Union européenne ont entendues mettre fin à cette situation en unifiant la protection des données à caractère personnel selon un paradigme à somme positive, c'est à dire dépourvue de compromis inutiles. Cette protection intégrée de la vie privée évite, par exemple, la dichotomie entre la protection de la vie privée et la sécurité ou encore entre la vie privée et la disponibilité de l'information en démontrant qu'il est vraisemblable de concilier ces objectifs.

189. Le rattachement du régime de protection de la donnée aux droits de la personnalité, conduit à subordonner l'application des dispositions du Règlement de 2016 et de la loi Informatiques et Libertés, au caractère personnel de la donnée (Section 1). Les données à caractère personnel relatives à la santé font, en raison de leur sensibilité, l'objet d'un régime spécifique consistant en l'interdiction, par principe, de leur traitement. Ce régime est assorti d'exceptions permettant le traitement de la donnée, autrement dit, sa circulation. L'application de ce régime dérogatoire est subordonnée à la qualification de l'information directement ou indirectement identifiante en donnée de santé (Section 2).

Section 1. Une donnée identifiante

« Quand l'objet des données est un sujet de droit, l'information est un attribut de la personnalité »[175]

191. **L'identification comme condition essentielles et déterminante de la protection.** Le droit à la protection des données à caractère personnel appartient aux droits de la personnalité. Par suite, la loi relative à l'informatique, aux fichiers et aux libertés[176], ainsi que le Règlement général à la protection des données[177] protègent à travers la donnée, la personne concernée par le traitement, son individualité, son intégrité morale, c'est à dire sa vie privée, sa dignité, son image, etc. Ces textes reconnaissent à cette fin des droits à la personne, qui sont destinés à lui permettre de conserver un lien avec ces fragments de sa personnalité et la maitrise des informations la concernant.

192. Ce lien avec la personne, constitue une condition indispensable à la protection de la donnée (paragraphe 1). Dans notre société fondée sur l'utilisation des technologies de l'information et de la communication le lien avec la personne peut, compte tenu de la masse de données traitées ou des technologies susceptibles d'être utilisées, être distendu. Ce contexte conduit les acteurs du traitement mais aussi de la protection des données à éprouver des difficultés quant à l'appréciation du caractère indirectement identifiant d'une information (paragraphe 2).

---

[175] P. Catala. *Le Droit à l'épreuve du numérique: Jus ex machina,* PUN, 1998

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

[177] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libr1e circulation de ces données.

§ 1. Une condition indispensable

193. **Une information nominative.** L'article 4 de la loi Informatique et Libertés dans sa rédaction initiale, employait le terme d'informations nominatives dont il donnait une définition fonctionnelle. Étaient considérées comme des informations nominatives toutes *« informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale »*. Bien que la notion de *« donnée à caractère personnel »*[178] puisse, de prime abord, comprendre une catégorie plus importante de données, la CNIL a toujours adoptée une interprétation lato sensu de la notion d'information nominative.

194. Cependant, *« cette définition se limitait (…) à des éléments d'identifications essentiellement physiques, physiologiques, économiques ou [encore] culturels »*. C'est pourquoi, elle s'est rapidement trouvée inadaptée[179]. En effet, la numérisation de la société et les progrès technologiques, notamment en ce qui concerne les moyens, méthodes et techniques d'identification directe et indirecte, de traçabilité, de pistage ou de profilage, ont conduit à accentuer l'écart entre la lettre et l'esprit de la loi tel qu'il résulte de l'interprétation réalisée par les juridictions[180]. Ainsi, le qualificatif d'information nominative excluait, *in fine*, la captation

[178] Notion substituée par la loi du 6 août 2004 transposant la directive n° 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, *JOCE* n° L 281, 23 nov. 1995, p. 31.

[179] M. VIVANT, « Qu'entend-on par « données à caractère personnel » ? », Lamy droit du numérique 2015, étude 4276.

[180] *« Eu égard à sa nature, à sa composition et à ses attributions [la CNIL] peut être qualifié[e] de tribunal au sens de l'article 6-1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentale »* (CE, 19 fév. 2008, Profil France, n° 311974, Inédit), inédit

d'images, de traces numériques, l'utilisation de numéros d'identifications de la personne ainsi que la protection de données de la personnalité[181].

195. **Une donnée à caractère personnel.** La protection des informations nominatives à caractère personnel, relevant du droit de la personnalité, il est indispensable pour qu'elle soit protégée par les dispositions de la loi relative à l'informatique, aux fichiers et aux libertés ainsi que par le Règlement général sur la protection des données, qu'elle puisse être rattachée à la personne sur laquelle l'élément de connaissance qu'elle contient porte. La loi n° 2004-801 du 6 août 2004 a étendu *« le champ de la protection aux domaines de la voix et de l'image*[182] *[en prenant en compte les progrès] des techniques d'identification (moteurs de recherche, logiciels de reconnaissance vocale ou morphologique) »*[183]. La notion de données à caractère personnel n'exclue toutefois pas l'information nominative. Ainsi, le nom, le prénom et la date de naissance constituent des données nominatives qui permettent de procéder directement à l'identification d'une personne sans qu'il soit nécessaire de s'interroger si le traitement d'informations nominatives, entre dans le champ d'application *ratione materiae* de la loi relative à l'informatique, aux fichiers et aux libertés.

196. La complexité de modalités techniques mais aussi organisationnelles, de mises en œuvre d'un traitement ainsi que les progrès techniques peuvent conduire le responsable de traitement à éprouver des difficultés quant à la qualification de ce dernier. Ainsi, si un traitement peut sembler a priori porter sur des données non identifiantes, il peut s'avérer *in fine* qu'il concerne des données à caractère personnel.

---

[181] M. DUPUIS, « La vie privée à l'épreuve des réseaux sociaux », *Revue Lamy de droit civil* 2013, n° , N°102.

[182] M. VIVANT, « Quelles différences entre « données à caractère personnel » et « informations nominatives » ? »,?, Lamy droit du numérique 2015, étude 4278.

[183] A. TÜRK, Rapport fait au nom de la commission des lois sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, n° 218, Sénat, Session ordinaire 2002-2003.

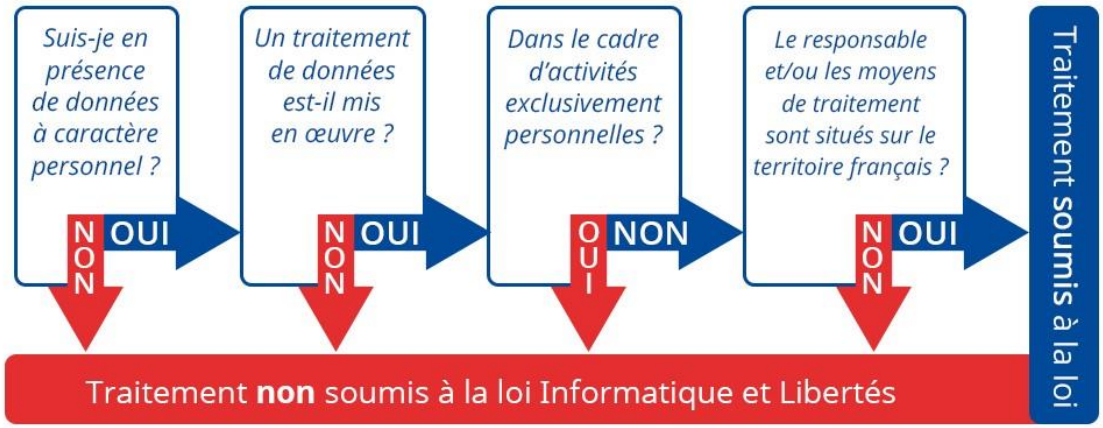
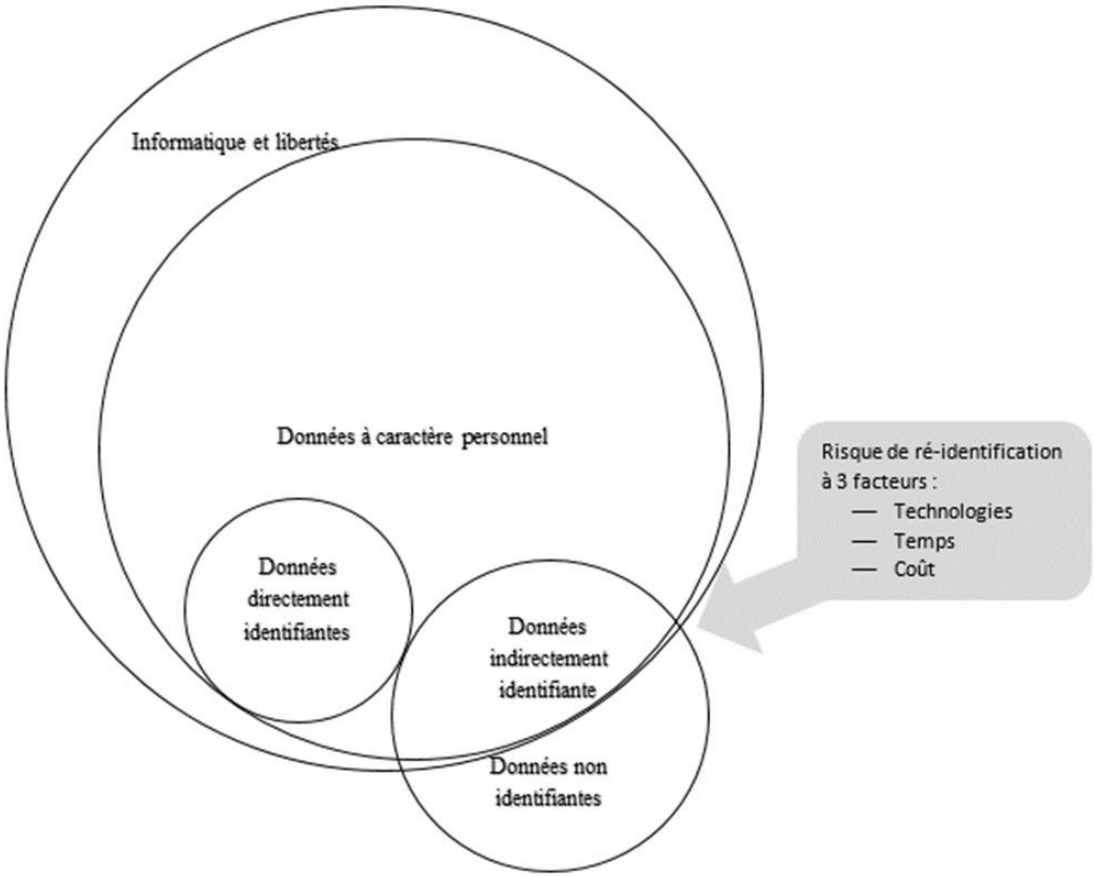


Figure 1 Schéma disponible à l'adresse suivante : https://www.cnil.fr/fr/informatique-et-libertes-suis-je-concerne

197. L'applicabilité de la loi dépend de la capacité du responsable du traitement ou des tiers à procéder à une identification de la personne concernée à partir des données traitées. Nous nous situons par conséquent à la frontière entre l'application du régime de protection et l'absence de réglementation du traitement. La mise en œuvre d'un tel traitement peut engendrer une atteinte aux droits et libertés de la personne concernée et un risque pénal pour le responsable du traitement. Cette menace est accrue lorsque la qualification du traitement s'avère *a posteriori* erronée et qu'il en résulte l'absence de mesures destinées à diminuer l'occurrence des risques.



198. Dans ce contexte, la CNIL a pu considérer qu'une représentation graphique de la personne humaine, découpée en zones selon les degrés de handicap afin de permettre un diagnostic quasi instantané, constituait un traitement de données à caractère personnel. En l'espèce, le traitement dressait une définition fine du profil ainsi que de la personnalité de la personne concernée et était, de ce fait, susceptible d'amener à une prise de décision sur son seul fondement en contradiction avec les dispositions de la loi Informatique et Libertés.[184]

[184] CNIL, 6e rapport d'activité du 1er janvier au 31 décembre 1985, p. 106 et s. et 7e rapport, p. 56..)...

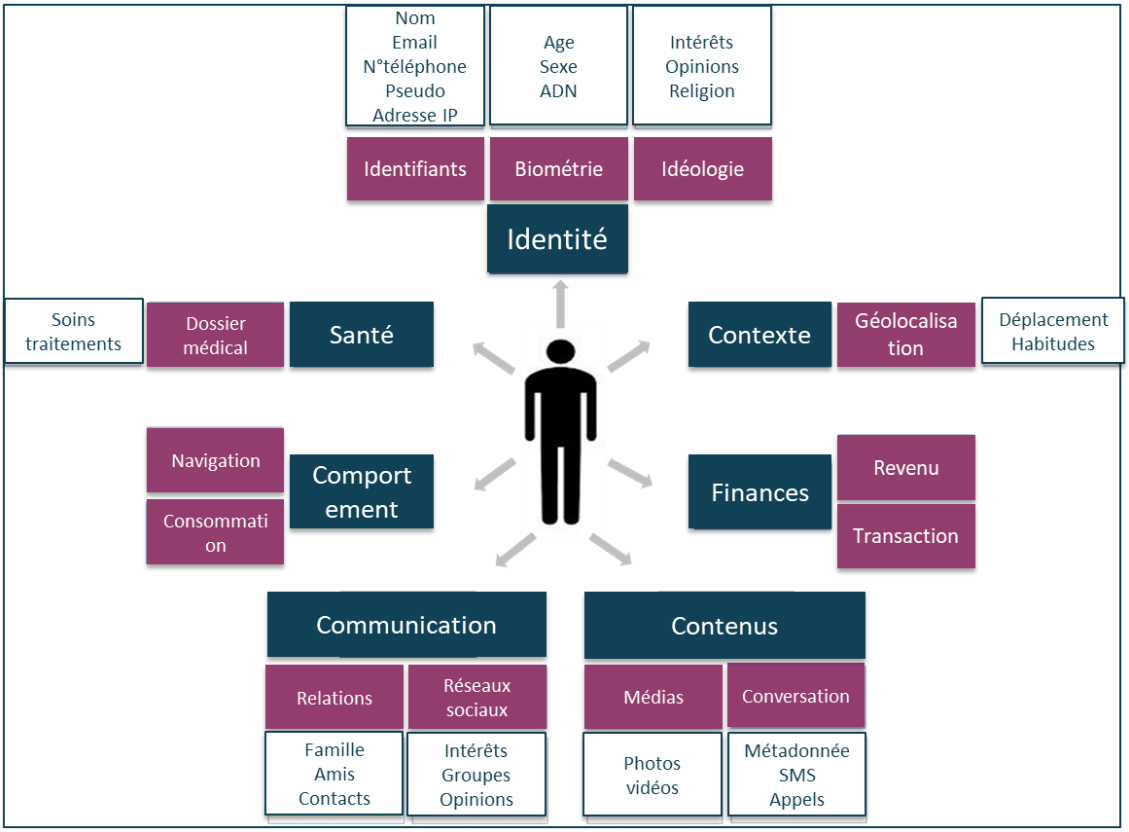


Figure 3Représentation graphique des informations constituant des données à caractère personnel

199. Cette représentation fine du profil de la personne permettait ainsi son identification.

§ 2. Une appréciation difficile

201. L'identification et la pseudonymisation comme moyen de protection. Le champ d'application *ratione materiae* du droit à la protection des données à caractère personnel, dépend de la capacité du responsable de traitement et des tiers à identifier la personne à partir des données qui sont traitées(A). Cette capacité d'identification doit être appréciée en tenant compte de multiples facteurs. Le caractère indirectement identifiant peut également résulter d'une action volontaire. Il peut s'agir de la mise en œuvre d'une mesure de sécurité consistant en la pseudonymisation des données. La ré-identification de la personne suppose alors la réalisation de traitements supplémentaires sur les données ou le recours à des informations complémentaires. Cette identification indirecte peut également résulter du recours à un identifiant. Dans le secteur de la santé l'utilisation d'un identifiant est guidée par la volonté de prévenir d'éventuels risques d'identitovigilance. Compte tenu des données concernées, l'identifiant choisi ne doit pas permettre de procéder au croisement ou au rapprochement de fichiers et constituer ainsi un risque pour la vie privée de la personne (B).

A. Une imputabilité incertaine

« Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de 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 ».[185]

[185] Règl. (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, considérant 26, Préambule, JOUE L 119, 4 mai 2016.

202. **L'identification des professionnels comme moyen de protection**. Il s'agit par l'identification de la personne de protéger les données la concernant mais il s'agit également, par l'identification des professionnels de protéger la personne contre les accès indus.

203. L'identification du professionnel un Le développement d'internet et des technologies de l'information et de la communication, ont fait évoluer considérablement les moyens d'échanger et de partager de l'information, blogs, bases de données de santé, dossiers médicaux partagés, messageries, etc. La plupart des échanges ont désormais lieu de manière instantanée et dématérialisée. Les solutions logicielles et systèmes d'informations utilisés doivent garantir la sécurité de l'information sur l'ensemble des critères fondamentaux (disponibilité, intégrité, confidentialité, traçabilité)[186]. L'objectif et de mettre en œuvre de mesures garantissant le respect des droits des personnes ainsi que la confiance de celle-ci dans le système d'information de santé.

204. En matière de confidentialité et de traçabilité, la confiance est préservée au moyen de l'identification et de l'authentification des professionnels souhaitant accéder à la donnée. L'authentification [187] permet d'accorder un accès aux données à caractère personnel relatives à la santé aux seules personnes autorisées. Elle permet également, conformément aux dispositions de l'article R. 1110-1 du Code de la santé publique, de maitriser et de conditionner les accès au système d'information en différenciant les possibilités d'accès aux données de

[186] C. santé publ, art. L. 1110-4-1.

[187] Référentiel Général de Sécurité, version 2.00, § 3.2.a.1 : *« L'authentification a pour but de vérifier l'identité dont se réclame une personne ou une machine*. » *S'identifier consiste à communiquer une identité préalablement enregistrée, s'authentifier consiste à apporter la preuve de cette identité. L'authentification est généralement précédée d'une identification*. 194 C. santé publ, art. L. 1110-4-1.

santé en fonction des droits attachés à l'identité de l'utilisateur (matrice d'habilitation).

205. La bonne utilisation des technologies de l'information et de la communication, c'est-à-dire une utilisation *« conforme [à la réglementation ainsi qu'] aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24 »*[194] et aux recommandations adoptés par la CNIL, représente une valeur ajoutée en matière de secret partagé. Elles permettent effectivement aux professionnels de santé, aux établissements et services de santé, aux hébergeurs de données de santé à caractère personnel et à tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social mais aussi, dans une certaine mesure, aux patients et usagés, de s'assurer que *« les professionnels participant à la prise en charge d'une même personne [puisse accéder aux] 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 [dans la limite du périmètre de leur missions] »*[188].

206. En ce sens, l'identification et l'authentification forte permettent également de contrôler, *a posteriori,* les actions réalisées au sein du système (imputabilité) par la production de traces intègres et, par conséquent, opposables (utilisées à des fins probatoires). De cette manière, il est possible de contrôler, pour chaque utilisateur, les actions qu'il a réalisé au sein du système et notamment, de connaître les données auxquelles il a eu accès, qu'il a partagé mais aussi modifié ou supprimé.

207. Lorsque le système est utilisé par des professionnels ne faisant pas partie d'une équipe de soins, les mesures mises en œuvre doivent, par ailleurs, préalablement être portées à la connaissance de la personne prise en charge.

[188] C. santé publ, art. R. 1110-1.

208. **Un lien difficile entre l'information et la personne.** La définition de la donnée à caractère personnel témoigne de la difficulté de déterminer plus finement cette notion a priori. L'applicabilité de la réglementation résultant de la qualification de la donnée, la notion de donnée indirectement identifiante a *de facto* vocation à protéger les droits et libertés de la personne en laissant au responsable du traitement et, a posteriori, au juge la charge d'en apprécier le caractère indirectement identifiant. Cette appréciation est réalisée au regard des risques que peut représenter le traitement litigieux ainsi que la capacité et des moyens qui sont nécessaires pour procéder à l'identification de la personne dont les données sont traitées En raison de la complexité que représente l'appréhension, par un néophyte, des moyens techniques permettant l'identification d'une personne, cette détermination au cas par cas s'avère souvent complexe. La question du caractère personnel de l'adresse Internet Protocol (adresse IP) matérialise cette difficulté et, a été l'objet d'une jurisprudence abondante et fluctuante. Afin de définir si ce numéro constitue une donnée à caractère personnel indirectement identifiante, il convient de déterminer son mode de fonctionnement ainsi que les modalités de son attribution pour enfin s'intéresser aux problématiques et enjeux de sa qualification.

209. **L'internet protocole un environnement fonctionnant sur une identification aléatoire.** Il y a lieu de rappeler que les appareils connectés en réseau (ordinateur de bureau, ordinateur portable, tablette, smartphone, imprimantes…) communiquent entre eux grâce à un protocole appelé *Internet Protocol*. Celui-ci repose sur l'utilisation de numéros d'identification uniques constituant de véritables adresses numériques, appelées adresses IP. Elles permettent l'identification et la localisation des appareils connectés au réseau et ainsi, l'envoi et la réception de paquets de données d'un appareil identifié à un autre. Les adresses IP sont également utilisées à d'autres fins tel que le *Web analytique* puisqu'elles peuvent notamment être collectées par les administrateurs de sites *Web* au moyen

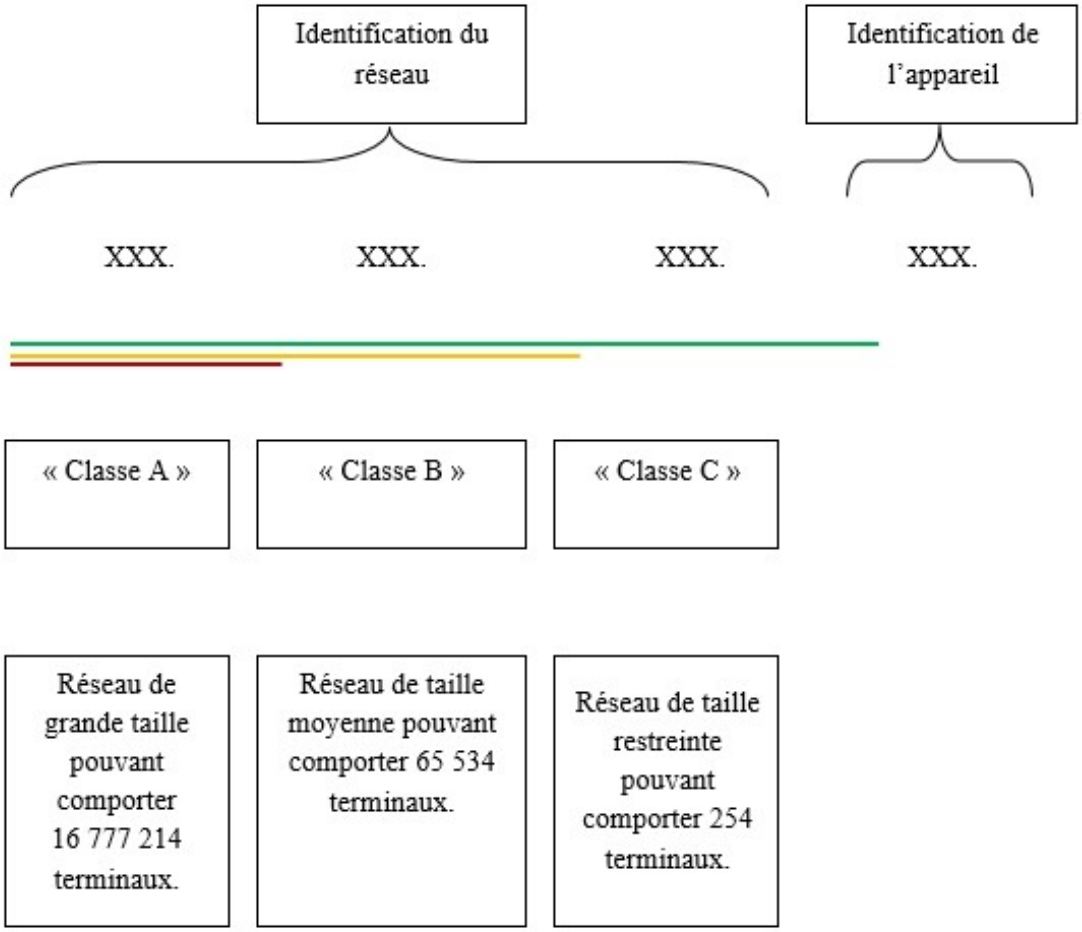
d'un fichier journal *(log file)* dans le but de connaitre la fréquentation des sites web.

210. L'*Internet Protocol* actuellement le plus utilisé correspond à la version 4 *(IPv4).* Cette adresse IP est constituée de 4 *octets*[189] autrement dit 4 fois 8 *bits* [190] soit 32 *bits* et, est exprimée sous la forme xxx.xxx.xxx.xxx. Chaque segment représente un octet, soit un nombre décimal compris entre 0 et 255. Cette adresse peut être décomposée en deux parties, les trois premiers nombres permettent d'identifier le réseau et le dernier nombre représente l'appareil connecté au réseau.

211. On distingue traditionnellement trois types de réseaux dont les réseaux locaux qui ont pour acronyme LAN issue de l'anglais Local area network, les réseaux urbains appelés MAN autrement dit Metropolitain Area Network, de taille intermédiaire ces réseaux publics concernent essentiellement le secteur bancaire, universitaire, médical, transport, (…) et permettent la transmission de données sur des distances importantes, les réseaux étendus appelés wide area network, (WAN).

[189] L'octet est une unité de mémoire informatique. un OCTET est un multiplet de 8 bits codant une information. Souce : Futura Tech. (https://www.futura-sciences.com/tech/definitions/informatique-octet585/)

[190] Il s'agit d'une contraction du mot *binary digit* (chiffre binaire). Elle constitue l'unité la plus simple dans un système de numération. Elle ne peut, par conséquent, prendre que deux valeurs, désignées le plus souvent par les chiffres 0 et 1. Source : JDN (https://www.journaldunet.fr/web-tech/dictionnaire-duwebmastering/1203567-bit-definition/)



212.

213. *Figure 4Représentation graphique d'une adresse IP*

214. Les adresses des terminaux directement connectés sur le réseau public internet sont attribuées par *l'Internet Corporation for Assigned Names and Numbers* (ICANN) au niveau mondial. Il délègue la gestion de ces adresses à des instances régionales, le *Réseaux IP européen Network Coordination Center* (RIPE NCC) pour la région Europe.

215. Les adresses IP octroyées par l'ICANN sont finalement allouées à l'utilisateur final qui en fait la demande à un *Local Internet Registry* (LIR)[191]. Sur le réseau local, l'identification des appareils connectés se fait

[191] Il s'agit le plus souvent de fournisseurs d'accès à internet (FAI) Pour connaître la liste des FAI français il convient de se rendre à l'adresse suivante https://www.ripe.net/membership/indices/FR.html

par l'attribution d'une adresse IP Lan. Cette adresse est donnée par un routeur. Le plus souvent, les adresses IP des appareils connectés sont attribuées de manière dynamique[192] par le fournisseur d'accès internet (FAI). Cependant, il arrive que certains FAI proposent une adresse IP statique, qui demeure identique à chaque reconnexion.

216. **Le caractère personnel de l'identifiant matériel.** Un patient peut, dans le cadre de sa prise en charge avoir recours à un espace numérique de santé lui permettant, par exemple, de consulter ses examens ou d'être mis en relation avec un professionnel. Ces services nécessitent, outre l'authentification forte[193] du patient, l'identification du matériel. Ainsi, la question de l'impact de l'attribution de l'adresse IP sur le caractère personnel directement ou indirectement identifiant, se pose. Le mode d'attribution de l'adresse IP à un impact sur la vraisemblance du risque d'identification de la personne. La Cour de justice de l'Union européenne, dans un arrêt du 19 octobre 2016[201] a eu à connaitre de l'appréciation du caractère personnel d'une adresse internet protocole dynamique. À ce titre, elle a considéré qu'une telle adresse, *« enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site Internet que ce fournisseur rend accessible au public constitue, à l'égard dudit fournisseur, une donnée à caractère personnel au sens de cette disposition, lorsqu'il dispose de*

---

[192] Le FAI attribut, le plus souvent, à son abonné une adresse IP différente à chaque connexion. Cette adresse est qualifiée de dynamique et peut par conséquent être réutilisée, dans le temps, par plusieurs appareils connectés. De cette manière, l'adresse est attribuée à un terminal le temps nécessaire à sa connexion au réseau. Cette connexion expirée, l'adresse IP dynamique est de nouveau disponible et peut être allouée à un autre terminal. Elle ne permet pas l'identification d'une machine ou de l'utilisateur d'une session à l'autre mais permet cependant la géolocalisation du point d'accès au réseau.

[193] *« L'authentification forte, ou authentification à deux facteurs, combine quelque chose que l'on sait*

(mot de passe, code PIN) avec une autre chose qui peut être un élément biométrique, un objet que l'on

possède ou une action que l'on sait faire. » Source Futura Tech (https://www.futurasciences.com/tech/definitions/securite-authentification-forte-15025/) 201 CJUE, 19 oct. 2016, Breyer, C-582/14.

moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet de cette personne. »[194]

217. Il en résulte, que les modalités d'attribution de l'adresse IP sont indifférentes. Quelle soit attribuée de manière statique ou dynamique, elle peut indirectement permettre l'identification du détenteur de la ligne et non l'utilisateur du terminal connecté au réseau. De la sorte, à partir du moment où il est possibilité pour un individu de déterminer l'identité du détenteur du terminal, cette information doit être considérée comme une donnée à caractère personnel indirectement identifiante. L'adresse IP peut être considérée comme une donnée à caractère personnel en ce qu'elle permet l'identification du titulaire de la ligne. Cependant, son exploitation ne permet pas toujours d'identifier l'utilisateur du terminal connecté au réseau. Le titulaire de la ligne n'étant pas nécessairement l'utilisateur du terminal, à défaut d'authentification forte de l'utilisateur du poste, l'appréciation du caractère personnel de l'adresse IP doit être distinguée de sa capacité à permettre l'identification de l'utilisateur d'un terminal déterminé. Ainsi, l'adresse IP constitue *in fine*, par sa constitution et, ses modalités d'attribution ainsi que les moyens techniques d'identification à disposition, une donnée à caractère personnel.

218. Cependant, la reconnaissance du caractère personnel de cette donnée devrait être destinée à protéger la personne concernée, tout au plus, à identifier le titulaire de la ligne ou le propriétaire du poste. L'utilisation de l'adresse IP comme moyen d'identification de l'auteur d'une infraction revient à reconnaitre une présomption de responsabilité pesant sur le propriétaire de la ligne ou du poste. Dans ce cadre, cette appréciation doit être menée *in concreto.*

219. **L'IP un moyen d'identification incertain.** Le recours à une adresse IP comme moyen d'identification du matériel ne constitue pas un

[194] *Ibid.*

procédé infaillible. Sur le réseau internet, les appareils connectés disposent d'une seule adresse IP publique permettant d'identifier le matériel connecté. Par ailleurs, il est possible de détourner une adresse IP en ayant recours à l'usurpation IP ou *IP spoofing.* Il s'agit d'une technique destinée à usurper l'identité d'un autre équipement pour masquer sa propre identité et bénéficier d'un service auquel le matériel a accès ou pour commettre une infraction.

220. Nous l'avons explicité ci-dessus, il est possible de procéder à une usurpation d'identité matérielle. Aussi, la question du caractère indirectement identifiant de l'adresse IP est à l'origine d'une jurisprudence abondante et fluctuante le plus souvent en opposition avec le résultat des travaux du G29[195] ainsi que la position de la CNIL.

221. Le groupe des *«CNIL européennes,* dans son document de travail du 21 novembre 2000, considère que l'adresse IP constitue « *un identificateur relativement faible »*[196]. Il précise dans ce même document de travail que cette adresse doit être considérée comme une donnée à caractère personnel indirectement identifiante compte tenu du fait qu'elle permet aux FAI ainsi qu'aux gestionnaires de réseaux locaux, d'identifier les utilisateurs Internet auxquels ils les ont attribué, notamment en utilisant des moyens raisonnables[197.]

222. En ce sens, le Tribunal de grande instance de Paris a également affirmé que l'adresse IP constituait une donnée à caractère personnel

---

[195] Le groupe de travail de l'article 29 (G29) sur la protection des données, encore appelé « Groupe des CNIL européennes », est un organe consultatif européen indépendant institué par l'article 29 de 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.

[196] Groupe de travail de l'article 29 (G29) sur la protection des données, Document de travail « Le respect de la vie privée sur internet – Une approche européenne intégrée sur la protection des données en ligne », Adopté le 21 novembre 2000, p. 18.

[197] Ibid., n° 16 p. 22.

permettant de procéder à l'identification des personnes. Pour ce faire, il retient une présomption simple. Le fournisseur d'accès internet détient les données nominatives de ses clients[198]. Compte tenu de l'état de l'art, il constate que les outils logiciels permettant de procéder à une usurpation d'adresse ne sont pas suffisamment déployés pour que l'adresse IP ne soit pas considérée comme représentant le seul moyen permettant de retrouver la personne physique à partir des données détenues par le fournisseur d'accès :

223. *« L'adresse IP est une donnée personnelle puisqu'elle (…) permet d'identifier rapidement à partir de services en ligne gratuits le fournisseur d'accès du responsable du contenu qui détient obligatoirement les données nominatives du responsable du contenu, (…). Au regard de la technique existante, cette adresse apparaît être le seul élément permettant de retrouver la personne physique (…). Si effectivement, cette adresse peut être usurpée grâce à des outils logiciels spécialement développés, ces détournements en nombre très limité à ce jour ne sauraient disqualifier cette adresse comme donnée permettant l'identification personnelle des fournisseurs de contenu. »*[199]

224. Pour la chambre criminelle de la Cour de cassation, l'adresse IP est également une donnée indirectement identifiante car elle constitue un moyen de procéder à l'identification de la personne mais en ayant recours

---

[198] Art. L. 34-1 C. P et T, « III.- Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales (…) et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du Code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information d'information mentionnée à l'article L. 2321-1 du Code de la défense, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. (…) ». Voir également art. R. 10-13, I (a) et (b) et (C.), (P) et (T), « (…) Les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales les informations permettant d'identifier l'utilisateur ; les données relatives aux équipements terminaux de communication utilisés (…) »

[199] TGI Paris, 3e ch., sect. 3, 24 juin 2009.

au faisceau d'indices *« sur [lesquels] le tribunal fonde sa conviction »*[200]. *A contrario*, les Cours d'appel de Paris et de Rennes ont considéré que le numéro IP ne constitue pas une donnée à caractère personnel dans la mesure où il *« ne se rapporte qu'à un ordinateur et non à l'utilisateur »*[201].

225. En conséquence, la question de l'appréciation du caractère personnel de l'adresse IP est le plus souvent soulevée lors de contentieux relatifs à l'utilisation frauduleuse d'Internet et à la cybercriminalité[202] nécessitant l'identification de l'auteur de l'infraction. Bien que les deux sujets soient étroitement liés, il faut distinguer l'appréciation du caractère personnel de l'adresse IP de la détermination de l'imputabilité de l'acte. Ainsi, l'adresse IP, à partir du moment où elle permet l'identification du titulaire de la ligne, notamment en ayant recours à la méthode du faisceau d'indices, doit être considérée comme une donnée indirectement identifiante. Cependant, ce procédé ne doit pas être regardé comme un moyen d'identification fiable à partir du moment où l'adresse IP peut être usurpée et/ou qu'elle ne permet d'identifier de manière certaine l'utilisateur du matériel au moyen duquel a été réalisé l'infraction.

226. Le titulaire de l'adresse IP publique serait dans l'impossibilité de démontrer sa bonne foi et se verrait systématiquement condamné.

227. Il peut toutefois arriver que le fournisseur d'accès internet attribue une adresse IP fixe. Dans ce cadre, l'adresse doit nécessairement être considérée comme une donnée à caractère personnel indirectement identifiante. Rappelons que l'appréciation du caractère personnel de l'adresse IP perd tout son intérêt lorsque l'utilisateur du poste est

---

[200] Crim., 5 nov. 2007, n° 07-81031, Inédit.

[201] Voir notamment CA Paris, 13e ch. corr., 15 mai 2007, n° 06/01954 ; CA Rennes, ch. cCh. om., 28 avril 2015, n° 14/05708.

[202] M. CHAWKI, *E*ssai sur la notion de cybercriminalité, IEHEI, 2006, p. 34 : La cybercriminalité peutêtre définie comme « toute action illicite associée à l'interconnexion des systèmes informatiques et des réseaux de télécommunication, où l'absence de cette interconnexion empêche la perpétration de cette action illicite ».

authentifié au sein du système d'information d'un établissement de santé. En effet, lorsqu'un utilisateur accède au réseau d'un établissement de santé dont le système d'information est conforme au Référentiel général de sécurité des systèmes d'information de santé, il ne fait aucun doute que, selon le niveau de confiance des différents dispositifs d'authentification[203] des utilisateurs susceptibles d'être mis en œuvre, l'identification de l'utilisateur du système peut être réalisée de manière certaine.

228. Ainsi, l'individu qui accéderait aux données à caractère personnel d'un patient ne pourrait répudier ses actions au sein du système. Toutefois, sans vouloir stigmatiser, les acteurs du champ sanitaire, social et médico-social il est fréquent que des petites et moyennes structures, ainsi que des professionnels, par manque de ressources, ou de connaissances, ne dispose pas nécessairement d'infrastructures et de protocoles conformes à l'état de l'art. Par ailleurs, avec le développement de la santé personnalisée et du bien-être, il est légitime de s'interroger sur les moyens d'identification des utilisateurs, à disposition des fournisseurs de service. Dans ce contexte, l'identification du matériel peut constituer un moyen d'identifier les personnes, à partir desquelles l'information est issue ou qui ont pu accéder à l'information de santé. Ainsi, la problématique de l'identification à partir de l'adresse IP est révélatrice des difficultés que peuvent rencontrer les responsables de traitement et juristes sans la qualification de la donnée, lorsque l'information n'est pas directement rattachable à la personne.

B. Une identification respectueuse de la vie privée

229. **Le besoin d'un identifiant national.** Actuellement, tout patient pris en charge au sein du système de santé se voit attribuer un identifiant

[203] Pour connaître les paliers de l'authentification des acteurs de santé,santéLIERS se référer à la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), Référentiel d'authentification des acteurs de santé. p. 12.

différent par le système d'information de chaque cabinet ou structure de soins l'accueillant *(établissement hospitalier, établissements et services sociaux et médico-sociaux, réseau de santé, laboratoire d'analyses de biologie médicale, maison de santé, etc.)* Ainsi, chaque structure adopte, au sein de son système d'information, ses propres règles d'élaboration et d'attribution d'identifiant. Cette absence d'identifiant commun, restreint l'échange et le partage d'informations entre les acteurs du soin.

230. Cette incapacité des systèmes à communiquer entre eux, de manière fluide, constitue un frein au développement des applications et projets régionaux. Ceux-ci peinent à développer un identifiant régional ou à utiliser l'identifiant national de santé calculé (INS-C). En effet, dans le cadre de ces projets nécessitant l'échange et le partage d'informations entre de multiples acteurs présents au sein des territoires de santé (professionnels de santé libéraux, centres hospitaliers, établissements d'hébergement pour personnes âgées dépendantes (EHPAD), laboratoires de biologie médicale…), des règles d'identification sont, le plus souvent, arrêtées entre les acteurs. Ainsi, des identifiants propres à ces projets sont mis en œuvre. Le plus souvent, ils ne se substituent pas à ceux des établissements mais s'y superposent. Leur conception étant inhérente aux projets, elle empêche leur utilisation à des fins d'identification régionale des patients.

231. **Un identifiant unique à des fins d'identitovigilance.** Cette absence d'identifiant commun pour le patient pose, de nombreuses difficultés en matière de sécurité et des problèmes d'identitovigilance. Cette carence augmente le risque que soit commise une erreur médicale pour un patient qui se serait vu attribuer des données mal identifiées. Dans cette situation, des solutions organisationnelles, techniques et juridiques sont mises en œuvre pour répondre aux besoins et pallier les difficultés résultant de l'absence d'identifiant national de santé. Il s'agit notamment de chartes et de cellules d'identitovigilance, de serveurs d'identités

patients avec corrélateurs d'identités[204]. Ces outils ont pour fonction de permettre aux acteurs de surveiller et de gérer les risques et erreurs liées à l'identification des patients tout au long de leur prise en charge et dans les échanges de données médicales et administratives. Malgré ces mesures palliatives, le risque de doublons ou de constater une confusion dans l'identité de patients subsistent. Par ailleurs, le recours à ces moyens fait perdre le bénéfice du recours à un identifiant afin de procéder à la pseudonymisation des données, c'est-à-dire de réduire le risque que peut représenter le traitement de données à caractère personnel, relatives à la santé pour une personne.[205]

232. Au regard de ces développements, il appert que le recours à un identifiant national s'avère nécessaire. La loi du 30 janvier 2007[206] intègre au sein du Code de la santé publique un nouvel article créant l'identifiant national de santé :

233. *« Un identifiant de santé des personnes prises en charge par un professionnel de santé ou un établissement de santé ou dans le cadre d'un réseau de santé défini à l'article L. 6321-1 est utilisé, dans l'intérêt des personnes concernées et à des fins de coordination et de qualité des soins, pour la conservation, l'hébergement et la transmission des informations*

[204] Outil logiciel permettant la gestion de l'identité des patients et le rapprochement à partir de traits d'identification. Il s'agit, le plus souvent de données d'état civil.

[205] Procédé constituant un *« 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 »* Règl. (UE). PE et Cons. UE préc. art. 4. § 5.

[206] 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 février 2007, art. 25 (V).

de santé. Il est également utilisé pour l'ouverture et la tenue du dossier médical personnel. »

234. **Le NIR un identifiant de qualité mais signifiant**. C. Zorn évoque, dans ses travaux, les réflexions qui ont présidées à la définition de cet identifiant national de santé. Elle souligne le caractère fondamental des questions en rapport avec sa nature et, à la protection à lui apporter[207].

235. Historiquement, nous disposons en France d'un identifiant national apportant tous les bénéfices escomptés en matière d'identification des personnes et d'interopérabilité. Il s'agit du numéro d'inscription au répertoire (NIR) communément dénommé *numéro Insee* ou encore *numéro de Sécurité sociale*. Conçu en 1941 par René Carmille, ce code alphanumérique devait initialement, sous couvert d'objectifs civils, permettre secrètement la remobilisation des effectifs de l'armée française, dissoute par l'Armistice du 22 juin 1940. Ce numéro désormais composé de 15 chiffres permet d'identifier une personne dans le répertoire national d'identification des personnes physiques (RNIPP) dont la gestion est confiée à l'Institut national de la statistique et des études économiques (Insee)[208]. Il est qualifié de signifiant, car il comporte en lui-même des informations sur le sexe, l'année et le mois de naissance, ainsi que le code chiffré de la commune de naissance et le numéro d'ordre sur le registre des actes de naissance[209].

236. Ce numéro d'identification présente donc un niveau de fiabilité satisfaisant pour être utilisé à *« des fins de coordination et de qualité des*

---

[207] C. ZORN, *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé*, avant-propos B. Py, préf. I. de Lamberterie, PUN, 2010, p. 270, n° 318.

[208] Décret n° 82-103 du 22 janvier 1982 relatif au Répertoire national d'identification des personnes physiques, art. 1.

[209] Le numéro unique d'identification des personnes physiques, Etude de législation comparée, Sénat, déc. 2007, p. 5.

soins, pour la conservation, l'hébergement et la transmission des informations de santé »[210]. Cependant, il a pour principal défaut sa perfection. Ainsi. dès 2007, la CNIL s'est montrée hostile à l'utilisation du NIR comme identifiant national de santé (INS) en raison de son caractère signifiant[211], unique, pérenne[212] et fiable. En effet, pour la Commission, celui-ci est susceptible d'être reconstitué à partir des éléments d'état civil. Il permet ainsi de manière plus aisée de rechercher de l'information au sein des fichiers de données et l'interconnexion de fichiers.

237. Fort de ce constat, le 26 octobre 2006, le Président de la CNIL, M. Alex Türk, a décidé de la création d'un groupe de travail ayant pour mission l'évaluation de la doctrine de la Commission sur l'utilisation du NIR Les conclusions de ce groupe de travail ont abouties à réaffirmer le caractère particulier du numéro de sécurité sociale[213].

238. C'est pourquoi la Commission a initialement développé une doctrine de cantonnement, autrement dit, la CNIL soutient le développement d'identifiants sectoriels. *« Allant à l'encontre de sa politique de cloisonnement des secteurs, la CNIL a [toutefois] admis que le N.I.R. soit enregistré dans l'ensemble des fichiers des organismes en relation avec le secteur de la sécurité social »*, celui-ci étant *ab initio* utilisé au sein de ce secteur.

239. *« Ainsi, sous l'effet des lois sociales successives, le cercle des partenaires de la sécurité sociale s'est progressivement élargi : caisses de retraite, impôts, CAF, employeurs pour la gestion de leur personnel. Il est*

---

[210] C. santé publ, art. L. 1111-8-1.

[211] Ce code indique le sexe, l'année et le mois de naissance, ainsi que le code chiffré de la commune de naissance et le numéro d'ordre sur le registre des actes de naissance.

[212] Ce numéro est qualifié d'unique et pérenne en raison du fait qu'il est attribué à chaque individu dès sa naissance.

[213] CNIL, délib., 20 février 2007, n° 2007-036.

ainsi illusoire de penser que le N.I.R. n'est pas associé à des données de santé dans la mesure où des données relatives à la santé des personnes figurent dans les fichiers de ces partenaires de la sécurité sociale. »[214]

240. Les préconisations formulées par la CNIL, dans ses conclusions en date du 20 février 2007, divergeaient cependant des projets du Ministère de la santé qui souhaitaient recourir au *« répertoire national d'identification des personnes physiques (RNIPP), géré par l'INSEE et, […] la CNAVTS*[215]*. L'utilisation de l'identifiant du RNIPP, […] et la communication de données issues du RNIPP, notamment pour vérifier l'exactitude du N.I.R. »* [216] *Toutefois, son utilisation requièrant « soit une autorisation de la CNIL, soit des dispositions législatives ou réglementaires prises après avis de la CNIL. »*[217] Le recours au NIR en tant qu'INS demeurait impossible. Le Ministère de la santé justifiait son projet de recourir au *numéro de Sécurité sociale* en invoquant le coût pouvant résulter de la création d'un identifiant sectoriel. Ainsi créer au niveau national *« un système d'identification ex nihilo en attribuant, après avoir vérifié son identité, un identifiant à chaque patient, c'est-à-dire à chaque personne prise en charge par le système de santé en France et donc potentiellement à tous les résidents. La constitution d'un tel système d'identification [générerait] un coût, estimé par le ministère de la santé à 500 000 €, sans compter le coût annuel pour sa mise à jour »*[218].

241. La Cour des comptes en septembre 2007 met en lumière une alternative à ces deux premières solutions. Celle-ci consiste à créer, à partir du NIR, *« un identifiant spécifique au domaine de la santé qui ne serait*

---

[214] C. ZORN, *op. cit*., p. 277, n° 326231.

[215] Caisse nationale de l'assurance vieillesse des travailleurs salariés.

[216] Cour des Comptes, *Rapport sur la Sécurité sociale*, sept. 2007, chap. X., p. 310 et 311.

[217] *Ibid.*

[218] *Ibid.*

pas signifiant. Cette façon de procéder dispenserait de créer un organisme chargé de l'identification des patients, requis pour la mise en œuvre de la première solution. Il nécessite cependant de gérer, de façon sécurisée, si possible en un lieu unique, une table permettant, à partir du N.I.R., d'obtenir l'identifiant santé des patients »[219].

242. **Une identification sectorielle temporaire et respectueuse de la vie privée.** La loi de 2007 laissant à un décret, pris après avis de la CNIL, la détermination des modalités de son exécution, celle-ci s'est heurtée, en l'absence d'un consensus sur sa mise en application, à des investigations tendant à la recherche du meilleur système d'identification. Ce n'est qu'à partir de 2010 qu'un identifiant distinct et anonymisé généré à partir du numéro de sécurité social a été mis en œuvre par l'Agence des systèmes d'information partagés de santé (ASIP Santé) sur les recommandations de la Commission[220]. La CNIL présentait toutefois, dans sa délibération du 2 décembre 2010, le recours à l'INS-C comme une solution provisoire *« dans l'attente de la mise en place de l'INS aléatoire prévu à terme »*[229]. Tous les bénéficiaires de l'assurance maladie n'en étant pas doté, elle considérait, en effet, que cet identifiant national de santé calculé[221] ne permettait pas *« d'apporter la garantie absolue de non collision et d'absence de doublon. ».* C'est pourquoi, l'acceptation de cette solution provisoire ne pouvait valoir accord *« pour qu'elle se perpétue au-delà de ce qui est nécessaire et suffisant pour mettre en place l'INS aléatoire »*. Par conséquent, cet identifiant devait être remplacé, à terme, par un identifiant national de santé généré de manière aléatoire. Son déploiement

[219] N. ETIEN-GNOAN, L'encadrement juridique de la gestion électronique des données médicales, Thèse, Lille, 2014, p. 183.

[220] Communiqué de presse de l'ASIP santé, *Une première étape pour un identifiant national adapté à l'échange et au partage de données de santé*, 9 juin 2010. 229 CNIL, délib., 2 déc. 2010, n° 2010-449.

[221] Cet identifiant national transitoire (appelé INS-C) est calculé localement dans les systèmes de santé en appliquant un algorithme public, choisi par l'ASIP santé avec le support de l'ANSSI, sur les traits d'identités (prénom, date de naissance, N.I.R.) lus en Carte Vitale, éventuellement complétés par l'appel à un télé-service.

sur le territoire national étant lié à celui du Dossier Médical Personnel[222], l'absence de mesures coercitives a nui au développement de cet identifiant.

243. Nous l'avons démontré, les réflexions autour de l'utilisation du NIR comme identifiant national de santé, ont été l'objet de nombreux débat depuis 2007. Rappelant l'affaire SAFARI, le recours au NIR en tant qu'identifiant national de santé a incarné le combat pour les libertés individuelles constituant ainsi plus un symbole qu'un réel risque d'atteinte à la sécurité des données et à la vie privée.

244. **Le NIR comme Identifiant national de santé** Face au développement de l'échange et du partage d'informations et, corrélativement, des systèmes d'information interopérables, il est devenu fondamental de réduire les risques de doublons voir de collisions d'identité. Par conséquent, il devenait de plus en plus difficile pour la Commission de maintenir sa doctrine de cantonnement strict en matière d'identification. Ainsi, dès 2013 la Commission *« s'est montrée ouverte à l'utilisation du N.I.R. comme identifiant dans la sphère de la santé, à la condition que des garanties strictes soient mises en place pour en circonscrire l'utilisation à cette seule finalité »*[223].

245. L'utilisation du NIR aux fins d'identification des patients et usagers s'est progressivement imposée. Fort de ce constat, la loi de modernisation de notre système de santé est venue intégrer à l'article L. 1111-8-1.-I du Code de la santé publique le recours au *« numéro d'inscription au répertoire national d'identification des personnes physiques (…) comme identifiant de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales »*. Le recours au NIR y

[222] Dossier médical personnel désormais dénommé « dossier médical partagé » depuis la Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé. ;.

[223] CNIL, délib., 19 janv.janvier 2017, n° 2017-014.

est subordonné à la détermination des modalités de son utilisation par décret en Conseil d'État, pris après avis de la CNIL.

246. Compte tenu de sa fiabilité en tant que moyen d'identification, la Commission est régulièrement sollicitée pour son utilisation. Au regard des atteintes aux droits et libertés des personnes pouvant en résulter, elle considère que l'extension de son utilisation en tant qu'identifiant au-delà des cas déjà admis accroît le risque d'interconnexion généralisée. Aussi, elle recommande que son utilisation soit cantonnée à la sphère sanitaire et médico-sociale à l'exclusion de toute autre utilisation.

247. **Des risques résiduels pour la vie privée.** À cette fin, la Commission a, dans son avis du 18 septembre 2014 relatif au projet de loi de modernisation de notre système de santé, attiré l'attention du Gouvernement *« sur la nécessité de mener une évaluation de l'unicité du N.I.R. et de la possibilité d'en cantonner l'usage à la sphère sanitaire et médico-sociale à l'exclusion de toute nouvelle utilisation, notamment de tout traitement massif de cette donnée en dehors de ces domaines »*. Au regard des dispositions définitives retenues au sein du décret, il est regrettable que le Gouvernement se soit limité, lors de cette étude, à évaluer l'unicité et la stabilité du NIR à l'exclusion de toute étude approfondie sur les risques sur la vie privée résultant des utilisations déjà admises dans d'autres secteurs.

248. Bien que le décret délimite strictement les organismes et les finalités de l'utilisation de l'identifiant national de santé, celui-ci continue à être utilisé dans d'autres secteurs. Aussi, cette limitation des organismes et finalités, si elle permet de réduire les atteintes susceptibles d'être causées au droit au respect de la vie privée, n'est pas de nature à garantir l'effectivité de ce droit. Ce numéro d'identification demeure, par ailleurs, signifiant et q permet, à partir d'éléments relatifs à l'état civil, d'identifier son titulaire et de faciliter le rapprochement ou l'interconnexion de fichiers.

249. **Une donnée de santé dont le traitement est strictement réglementée.** L'utilisation du NIR comme identifiant national de santé accepte deux principales limites, la première repose sur la finalité du traitement, celui-ci ne pouvant être utilisé que *« pour référencer les données de santé et les données administratives »*[224]. Il en résulte que l'identifiant du patient n'a pas pour unique but la fiabilité du référencement de ses données de santé. En conséquence, au-delà de la recherche de qualité et de sécurité, cette identification a pour finalité secondaire de faciliter la gestion administrative du patient et de l'usager. Dans le même sens, il résulte d'une lecture combinée des dispositions des articles R. 1111-8-2 et R. 1111-8-4 que le ministère des affaires sociales et de la santé n'opère aucune distinction entre le dossier médical et le dossier administratif de la personne prise en charge[225]. Ainsi, à partir du moment où ces deux dossiers ont vocation à permettre la prise en charge du patient, ne serait-ce que pour des considérations de bonne gestion administrative (telle que la prise de rendezvous) et financière, ou encore à des fins de soins les données qui le compose peuvent y être référencé au moyen du numéro de sécurité sociale.

250. La seconde restriction concerne le périmètre du traitement. Elle est cependant exprimée en des termes suffisamment étendues pour comprendre la majeure partie des cas de prise en charge de la perte d'autonomie, de la prise en charge thérapeutique mais également palliative, Le numéro ne concerne que les données des personnes « *bénéficiant ou appelée à bénéficier d'un acte de diagnostique, thérapeutique, de prévention, de soulagement de la douleur, de compensation du handicap ou de prévention de la perte d'autonomie, ou d'interventions nécessaires à la coordination de plusieurs de ces actes*

[224] C. santé publ, art. R. 1111-8-2.

[225] Remarquons que ce rapprochement de l'identification administrative et médicale du patient est conforme à la description de la donnée de santé réalisée au considérant 35 du Règlement 2016/679 qui assimile l'identifiant du patient ainsi que son inscription en vue de bénéficier de services de soins de santé à une donnée à caractère personnel relative à al santé.

»[226].Cette condition doit être complétée par les dispositions de l'article R. 1111-8-4 du Code de la santé publique qui dispose que *« l'utilisation de données de santé et de données administratives référencées avec l'identifiant national de santé n'est autorisée dans le cadre d'un traitement de données à caractère personnel que si (…) le traitement et mis en œuvre dans le respect des dispositions de la loi [de 1978] »*. Il s'agit, depuis l'abrogation de la directive de 1995 par le RGPD des dispositions relatives au traitement de données à caractère personnel relatives à la santé[227]. Ces dispositions supposent la mise en œuvre de mesures appropriées et propositionnelles aux impacts que le traitement est susceptible de faire peser sur la vie privée des personnes concernées.

251. Remarquons que la qualité des personnes habilitées à utiliser le NIR afin de procéder au référencement des données est définie strictement par le Code de la santé publique. Ainsi, il résulte des dispositions de l'article R. 1111-8-3 du Code de la santé publique que le référencement des données mentionnées à l'article R. 1111-8-2 du même code, à l'aide de l'INS, ne peut être exclusivement réalisé que par les professionnels, établissements, services et organismes mentionnés à l'article L. 1110-4 ainsi que par les professionnels constituant une équipe de soins en application de l'article L. 1110-12 et intervenant dans la prise en charge sanitaire ou médico-sociale de la personne concernée. Selon les estimations de la Commission, le nombre de professionnels ainsi habilités à traiter le NIR afin de référencer les données relatives aux patients et usagés dont ils assurent la prise en charge demeure conséquent puisqu'il serait d'environ 2 millions. Nous remarquons toutefois que pour des raisons liées à la sécurité des données et à la vie privée, les Groupements régionaux d'appui au développement de la e-santé (GRADeS) [228] se trouvent écartés de l'utilisation du NIR. Le recours à ce nouvel identifiant

[226] *Ibid.*

[227] V. infra

[228]

étant obligatoire, cela implique de réfléchir en amont des projets régionaux de e-santé à l'organisation de la gestion de l'identification et de l'identitovigilance.

252. Il ressort de l'ensemble des dispositions précitées et d'une lecture combinée des dispositions des articles R. 1111-8-2 et 3 du Code de la santé publique que celles-ci ont vocation à empêcher tout autre organisme, y compris les organismes d'assurance maladie complémentaire de traiter l'identifiant national de données de santé. Toutefois, cette restriction nous semble insuffisante. Au regard des risques susceptibles de peser sur les droits et libertés de la personne et afin de mettre fin à toute ambigüité sur le périmètre d'utilisation de l'identifiant national de santé, celle-ci devrait expressément interdire tout traitement de cet identifiant par toute personne physique ou morale n'intervenant pas à dans la prise en charge sanitaire, le suivi social et médico-social de la personne.

253. **Une utilisation restreinte du télé-service de recherche et de vérification d'identité.** Afin de procéder au référencement des données dans le respect des conditions prévues par les articles R. 1111-8-1 à R. 1111-8-5 et R. 1111-8-7 du Code de la santé publique, les professionnels habilités doivent avoir accès au NIR. Celui-ci est accessible à partir de la carte électronique individuelle inter-régimes[229] du bénéficiaire des actes ou actions mentionnés à l'article R. 1111-8-2. Cependant, dans la pratique, il est relativement fréquent qua la carte de l'assuré ne soit pas toujours accessible, notamment lorsque le référencement est réalisé au sein d'un établissement de santé. Il peut également arrivée, qu'elle ne contienne pas l'information recherchée. Aussi, l'article R. 1111-8-6 du Code de la santé publique prévoit, dans ce cadre, la mise en œuvre de *« services de recherche et de vérification de l'identifiant de santé mis en œuvre par la Caisse nationale de l'assurance maladie des travailleurs salariés »*

[229] CSS, art. L. 161-31.

autorisés par décret en Conseil d'État, pris après avis motivé et publié de la CNIL[230].

254. *« À cet effet, la Commission demande qu'une étude des risques du traitement et notamment son impact sur la vie privée soit réalisée à l'appui de cet encadrement réglementaire, ainsi qu'un descriptif de l'architecture technique retenue et des mesures de sécurité mises en œuvre ou prévues, notamment au regard des réserves formulées. »*[240]

255. Bien que ces services soient nécessaires, leur mise en œuvre doit faire l'objet d'une vigilance particulière car il concerne un nombre élevé d'usagers. Aussi, afin de restreindre l'accès au RNIPP ou au Système national de gestion des identifiants (SNGI) il est prévu que ces services permettent uniquement de réaliser des requêtes ndividu par individu[231]. Par ce garde-fou, les professionnels ne pourrons accéder, à l'ensemble des données à caractère personnel concernant la population française et les personnes résidant sur le territoire afin d'empêcher la réplication de ces bases. Ainsi, Ces dispositions sont également de nature à éviter que des interconnexions et détournements de finalités soient réalisés.

256. Il est regrettable de constater que ces services, outre le fait qu'ils soient soumis au principe de subsidiarité et au régime de l'article 27 de la loi Informatique et Libertés, ne soient pas accompagnés d'autres mesures de sécurité techniques et juridiques explicites rendant l'accès à ces services exceptionnel et limité à un nombre restreint de professionnels afin d'éviter que le NIR ne soit diffusé plus que nécessaire :

257. *« En tout état de cause, la Commission estime que le recours au téléservice ne devrait être autorisé que pour des finalités bien déterminées, répondant à des impératifs justifiés, par exemple nécessité d'obtenir le NIR*

[230] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, (art. .).27. 240 *IbidIbid.*

[231] CNIL, délib. 19 janvier 2017, n° 2017-014.

d'un ayant droit tant que cette information est absente de la carte vitale, personne ne disposant pas de carte vitale et identito-vigilance »[232]

[232] *Ibid.*

Section 2. Une donnée de santé

259. La protection accordée à la donnée à caractère personnel est nécessaire mais insuffisante. Elle implique l'application des dispositions de la loi relative à l'informatique, aux fichiers et aux libertés ainsi que du Règlement général sur la protection des données. Cependant, pour que les données relatives à la santé fassent l'objet d'une protection adaptée, il est indispensable qu'elles soient considérées comme des données sensibles. Ainsi, la qualification de donnée de santé est déterminante.

260. Toutefois, en l'absence de définition textuelle, des données susceptibles d'apporter des informations sur l'état de santé d'une personne se sont trouvées écartées de ce régime protecteur. Cette situation étant de nature à porter atteintes aux droits et libertés de la personne, une définition s'est avérée nécessaire (paragraphe 1). La réforme de 2016 a finalement définie la donnée de santé en y intégrant des données analogues transformant ainsi la donnée de santé en une notion attractive (paragraphe 2).

§ 1. Une définition nécessaire

262. **Une donnée initialement non protégée.** La notion de donnée de santé résulte de la Convention du Conseil de l'Europe du 28 janvier 1981 *« pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel »*. Premier traité international contraignant en matière de traitement de données à caractère personnel, la Convention 108 confère aux données de santé un statut spécifique[233]. Celles-ci font partie d'une catégorie particulière de données au même titre que « *l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives […] à la vie sexuelle »* dont le traitement automatique est par principe prohibé. Si le traitement automatique de ces données est interdit, la Convention l'autorise par exception lorsque le droit interne prévoie des garanties appropriées. Il s'agit de mesures législatives, réglementaires ou administratives spécifiques, assurant un degré de protection suffisant et permettant de maintenir un équilibre entre les droits de la personne concernée et toute mesure nécessaire dans une société démocratique aux intérêts de l'État et *« à la protection de la personne concernée et des droits et libertés d'autrui »*[234]. L'évolution des technologies, des usages et besoins, a nécessité la création d'un cadre réglementaire commun afin d'harmoniser la protection des données à caractère personnel et d'assurer un "niveau de protection équivalent" des droits et libertés des personnes à l'égard du traitement de ces données dans tous les États membres supérieur à celui de la Convention 108 »[235]. La directive 95/46/CE du Parlement

[233] Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE n°108, 28 janv. 1981, entrée en vigueur le 1er1 oct. 1985, art. 6.

[234] Convention du Conseil de l'Europe du 28 janvier 1981 « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », art. 9.»

[235] N. METALLINOSMétallinos, « L'évolution du droit européen en matière de protection des données à caractère personnel et sa pénétration dans les droits

européen et du Conseildu 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 » a permis la mise en place de ce cadre en garantissant un niveau élevé de protection de la vie privée des citoyens des États-membres de l'Union ainsi que la libre circulation des données à caractère personnel. Inspirée des principes de la loi du 6 janvier 1978[236], la directive 95/46/CE a été transposée en droit interne par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

263. Celle-ci est venue modifier les dispositions de la loi Informatique et Libertés en reprenant les principes élaborés par le comité d'experts gouvernementaux sous l'autorité du Comité européen de coopération juridique (CDCJ) lors de la rédaction de la Convention du 28 janvier 1981.Auparavant, la loi Informatique et Libertés ne traitait pas de la donnée relative à la santé mais des « informations nominatives ». Ainsi, jusqu'au 1er octobre 1985[237], date d'entrée en vigueur de la Convention 108, les données de santé constituaient des données à caractère personnel soumises au régime de droit commun[238]. Les informations nominatives relatives à la santé pouvaient, dans le respect des dispositions relatives au secret professionnel, faire l'objet d'un traitement dans les mêmes conditions que toute autre information permettant, *« sous quelque forme que ce soit, directement ou non l'identification des personnes physiques auxquelles elles s'appliquent ».* En raison de la transposition de la

nationaux : principes fondateurs et instruments de régulation », L'Observateur de Bruxelles, juillet 2013, n° 93n093, p. 8.

[236] Ph. GOSSELIN, *Rapport fait au nom de la commission des Affaires européennes sur la proposition de règlement 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*, n° 4325, Assemblée nationale, 7 févr. 2012.

[237] Loi n° 82-890 du 19 octobre 1982, autorisant l'approbation de la convention pour la protection des personnes à l'égard du traitement automatise des données à caractère personnel, JORF, 20 oct. 1982, p. 3163.

[238] R. PELLET, « La protection des personnes à l'égard des traitements informatisés des données à caractère médical depuis les ordonnances du 24 avril 1966 », RDSS 1996, p. 853.

directive95/46/CE, les données de santé à caractère personnel appartiennent désormais, au sens de l'article 8 alinéa 1 de la loi relative à l'informatique, aux fichiers et aux libertés, à une catégorie particulière d'informations à caractère personnel. Cette famille de données qualifiées de sensibles admet les « *données à caractère personnel 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 vie sexuelle de celles-ci* ». Du fait de leur caractère éminemment privé, ces données bénéficient dorénavant d'un régime de protection distinct du régime classique de protection accordé aux autres données à caractère personnel. Cette protection accrue repose sur un principe d'interdiction de traitement dont les exceptions sont strictement limitées à des finalités déterminées définies par l'article 8 de la loi Informatique et Libertés.

264. **Un besoin de qualité et de prévisibilité.** Bien qu'elles réglementent le traitement de cette catégorie de données, les législations française et européenne postérieures au RGPD ne définissaient pas la donnée de santé. De ce fait, la notion était le plus souvent explicitée selon les circonstances du traitement. En raison de cette situation, propice aux atteintes aux droits de la personne, il ressortait de la jurisprudence française et communautaire que les juridictions admettaient une interprétation extensive de la donnée de santé et ce, afin d'étendre le champ d'application de la loi Informatique et Libertés.

265. Ainsi, la Cour de justice des Communautés européennes, ,dans son arrêt en date du 6 novembre 2003 a pu considérer *« que l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, paragraphe 1, de la directive 95/46 »*[239].

[239] CJCE, 6 nov. 2003, Bodil Lindqvist, C-101/01.

266. Pareillement, le Conseil d'État a pu considérer que les données relatives à la scolarisation d'élèves en classes pour l'inclusion scolaire (CLIS) constituaient des données à caractère personnel relatives à la santé :

267. *« La mention exacte de la catégorie de classe d'intégration scolaire (CLIS) identifiée par l'un des quatre chiffre codant le type de handicap ou de déficience des élèves en bénéficiant, dont la seule mention permet par suite d'identifier immédiatement la nature de l'affection ou du handicap propre à l'élève concerné, […] que la mention de la CLIS doit donc être regardée comme une donnée personnelle relative à la santé.*[240]*»*

268. S'agissant d'une requête en annulation pour excès de pouvoir, présentée par le syndicat national des enseignants du second degré (SNES), à l'encontre du décret n° 2012-342 du 8 mars 2012 portant création d'un traitement automatisé de données à caractère personnel dénommé *« SIRHEN »* relatif à la gestion des ressources humaines du ministère de l'éducation nationale, de la jeunesse et de la vie associative, et du ministère de l'Enseignement supérieur et de la recherche, le Conseil d'État a pu considérer que :

269. *« La mention du taux d'incapacité permanente ou du taux d'invalidité du "conjoint ou partenaire" et des personnes à la charge de l'agent n'est pas une donnée "relative à la santé" au sens des dispositions précitées de l'article 8 la loi du 6 janvier 1978, dès lors qu'il n'est pas allégué qu'elle donnerait une information sur la nature du handicap. »*[241]

[240] CE, 10ème / 9ème SSR, 19 juillet 2010, 317182. Publié au recueil Lebon.

[241] CE, 10ème / 9ème SSR, 28 mars 2014, 361042

270. Le taux d'incapacité permanente ou le taux d'invalidité, bien qu'il ne donne pas nécessairement d'informations sur la nature du handicap dont la personne est atteinte, constitue une donnée permettant à toute personne y ayant accès de constater que la personne concernée souffre d'une diminution durable de ses capacités physiques ou mentales susceptible d'entrainer une perte définitive, partielle ou totale de la capacité d'exercer une activité professionnelle en raison d'une maladie professionnelle ou d'un accident du travail.

271. De la même manière, le Conseil d'État, saisi d'une demande en annulation des décisions du ministre de l'Education nationale portant création d'un traitement automatisé de données à caractère personnel dénommé *« base nationale des identifiants élèves »,* a estimé que :

272. *« La mention d'un code de référence des établissements de soins, si elle permet de savoir que l'élève a été souffrant, ne fournit, par elle-même aucun[e] information sur la nature, la durée, ou la gravité de l'affection de l'élève, information qui ne peut être obtenue qu'en accédant à un autre fichier mettant en correspondance les codes et la dénomination de l'établissement, qui n'est que très rarement explicite quant à la nature des pathologies qu'il soigne ; qu'en conséquence, les décisions attaquées ne peuvent être regardées comme portant sur ces données relatives à la santé en méconnaissance des dispositions de l'article 8 de la loi du 6 janvier 1978 relative à l'informatique et aux libertés ».*[242]

273. Au regard de ce qui précède, il est aisé de constater qu'une définition au cas par cas s'avère fastidieuse et ne témoigne pas de la qualité

[242] CE, n°19 juillet 2010 : n°334014.

et de la prévisibilité du droit. La révélation de ces informations est de nature à porter atteinte à la vie privée de la personne ou à lui refuser le bénéficie d'un droit. En conséquence, l'absence de définition légale peut conduire à ce que cette catégorie particulière de données ne fasse pas l'objet mesures de protection adaptée permettant ainsi la réalisation d'atteintes aux droits de la personne.

§ 2. Une notion attractive

> *« 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. »*[243]

274. **La donnée de santé, une donnée convoitée.** Les évolutions technologiques de ces dernières années ont menées à la personnalisation croissante de la santé et par conséquent à la consolidation du caractère personnel des données. En parallèle, ces évolutions se sont accompagnées d'une démocratisation de la technique et du développement de services reposant sur des dispositifs de *quantified self* ou encore bien être.

275. Ces dispositifs permettent aux individus de mesurer et de capter un ensemble de données physiologiques qui, au regard de leur quantité et/ou qualité, renseignent sur l'hygiène de vie de la personne, ses performances physiques ou permettent encore d'apprécier l'état de santé d'un individu. Ces dispositifs ont volontairement été présentés comme des dispositifs de bien-être afin d'échapper à un régime perçu comme contraignant ou trop protecteur. De cette manière, ils ont contribué à obscurcir la notion de donnée de santé et à en complexifier l'appréciation.

[243] Règl. (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, art. 4, § 15, Préambule, JOUE L 119, 4 mai 2016.

276. Par ailleurs, du fait de la diversification des modes d'exercices et de pratiques de santé, celle-ci a franchi les murs des institutions traditionnelles et s'est numérisée[244]. À ce titre, le Conseil National du Numérique, dans un rapport datant de 2015, constatait « *la profusion d'innovations en santé - technologiques, médicales, sociales, d'usages, etc. - qui inondent notre actualité quotidienne, l'effacement des frontières du champ de la santé vis-à-vis d'autres sphères (sociale, environnementale, professionnelle, etc.), l'évolution des enjeux de santé publique »*[245] qui n'ont pas épargné le monde de la santé.

277. La donnée à caractère personnel relative à la santé bénéficie, en raison de l'intérêt qu'elle suscite et du risque qu'elle est susceptible de faire peser sur la vie privée de la personne, d'un régime de protection spécifique. À titre d'information, le marché mondial de la e-santé est chiffré à 2,4 milliards d'euros et sa progression est évaluée entre 4 à 7 % par an d'ici à 2019. *« Le marché mondial de la m-santé est quant à lui estimé à 19 milliards d'euros. L'utilisation des tablettes et téléphones intelligents au soutien de la santé pourrait ainsi concerner 3,4 milliards de personnes dans le monde (un utilisateur de smartphone sur deux) dès 2017 »*[246].

278. Les données à caractère personnel relatives à la santé *« catalysent tous les enjeux liés aux données »*[247] et ont aujourd'hui une valeur qui dépasse sur le marché noir la valeur de numéros de cartes bancaires[248]. La donnée de santé attise les *convoitises « de certains géants du numérique,*

---

[244] S. LANGARD, Approche juridique de la télémédecine – *E*ntre Droit commun et règles spécifiques, Thèse, Nancy, 2012.

[245] Conseil national du Numérique, *La santé, bien commun de la société numérique*, Rapport, oct. 2015, p. 6.

[246] Etude du cabinet américain Research guidance, 7 mars 2013 cité *in* Conseil National du Numérique, op. cit., p. 24.

[247] M. CAVALIER, La propriété des données de santé, Thèse, Lyon, 2016, p. 32, n° 39.

[248] A. LYNNE, Rapport sur les cybermenaces dans le secteur de la santé, cité *in* Conseil national du Numérique, *op. cit*., p. 47.

professionnels de l'assurance, de la banque, hackers mal intentionnés »[249]. Concernant le secteur de la santé, l'année 2015 marque un véritable tournant. Selon les calculs de Websense[250]. on aurait ainsi enregistré au cours de cette année une hausse de 600% des attaques contre les établissements hospitaliers. En France, le laboratoire de biologie médicale Labio se serait vu réclamé 20 000 euros afin de récupérer et de ne pas voir publier les 40 000 identifiants et les centaines de bilans médicaux et d'analyses sanguines qu'il s'est fait dérobé. Il est donc devenu fondamental de définir a priori la notion de donnée de santé car sa protection repose sur sa qualification.

279. **Une définition exhaustive.** Le Conseil de l'Union européenne et le Parlement européen ont pris le parti de définir de manière extensive la donnée à caractère personnel relative à la santé au sein du Règlement. L'objectif assumé étant d'englober l'ensemble des données ayant attrait à la santé et par ce moyen de protéger les personnes concernées par le traitement de leurs données à caractère personnel afin de préserver la confiance dans le système de santé mais aussi vis-à-vis de l'usage de l'outil numérique. Cette définition ne dispense pas les responsables de traitement de se livrer à une appréciation *in concreto* des conditions de sa mise en œuvre afin de procéder à la qualification de la donnée et ainsi, de déterminer les dispositions qui lui sont applicables**.**

280. Afin d'assister les responsables de traitement et sous-traitant dans la qualification, *a priori*, de la donnée, et de leur permettre de définir et de mettre en œuvre les mesures assurant l'effectivité des droits de la personne et un niveau de sécurité appropriée des données, la CNIL a dégagé de cette définition trois critères. Le premier de ces critères a attrait à la nature de la

[249] Conseil national du Numérique, op. cit., p. 46.

[250] Entreprise américaine fondée en 1994 spécialisée dans le filtrage Web et dans la sécurité informatique et la bureautique. Cette entreprise a été rachetée au cours de l'année 2015 afin de constituer la société Forcepoint. Les informations sont consultables à l'adresse suivante : https://www.forcepoint.com/fr

donnée, à laquelle la Commission y assimile l'origine de la donnée. Ce faisant, elle confirme le principe précédemment posé selon lequel, les données recueillies ou produites par les acteurs du système de santé, qu'il s'agisse de personnes physiques ou morales, dès lors qu'elles concernent le patient et permettent directement ou indirectement son identification, doivent être considérées comme constituant des données de santé. Ainsi, constituerait une donnée à caractère personnel relative à la santé toute information sur une *« personne physique collectée 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*[251] *au bénéfice de cette personne physique ».*

281. Cette condition liée à l'origine de la donnée n'est pas toujours exclusive ou déterminante, elle doit être rattachée au critère relatif à la nature de la donnée, c'est-à-dire à son essence et plus précisément à son contenu informationnel. Il peut ainsi s'agir de toute donnée se rapportant à des informations relatives à la santé physique ou mentale d'une personne physique, *« 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 »*[252]. Par conséquent, toute information recueillie à l'occasion *« d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social »* ou en dehors de ces activités, dès lors qu'elle porte sur des informations relatives à la santé de la personne doit être considérée comme une donnée à caractère personnel relative à la santé. Ces deux conditions

[251] 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, *JOUE* (JO L 88, 4 avril 2011, p. 45.

[252] Règl. (UE) UE 2016/679 du Parlement européen et du Conseil du 27 avrilavr 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, considérant 35.

étant remplies, le Règlement général sur la protection des données établie, en la matière, une présomption irréfragable.

282. Par ce moyen, la CNIL met en exergue que la définition de l'article 4 du Règlement ne restreint pas la qualification de la donnée et ainsi l'application des dispositions protectrices de l'article 9 exclusivement à des considérations liées à son contenu informationnel.

283. Le second critère identifié par la CNIL porte sur les données qui deviennent des données de santé par destination. Il s'agit, selon la Commission, de données qui ne portent pas sur l'état de santé d'une personne mais qui sont susceptibles d'être utilisées à des fins thérapeutiques ou de prévention. À titre d'exemple, l'appartenance à une origine ethnique, l'orientation sexuelle, l'appartenance à une confession peuvent être collectée afin d'adapter un traitement de réaliser une meilleure évaluation des risques, ou encore d'identifier des pathologies**.**

284. Enfin, un troisième critère consiste à ne pas considérer une donnée isolément pour apprécier la qualification non plus de la donnée mais du traitement. Ainsi, bien qu'un traitement puisse ne comporter aucune donnée relative à des examens médicaux, des résultats de biologie ou tout autre élément de diagnostic et ne poursuive, a priori, aucune finalité thérapeutique, la mise en relation d'une ou plusieurs des données qui le compose, peut aboutir à la génération d'informations susceptibles de révéler des indications sur l'état de santé passé, présent ou futur de la personne concernée.

285. À titre d'exemple, une application de *coaching* sportif collectant des informations sur l'âge, l'identité sexuelle, les habitudes alimentaires journalières d'une personne ainsi que son niveau d'activité physique quotidien.

286. Cette définition élargie est donc en rupture avec la décision du Conseil du 19 juillet 2010, relative à la base nationale des identifiants des élèves du ministère de l'éducation, par laquelle le juge subordonnait la

qualification de donnée à caractère personnel relative à la santé à la présence de contenu informationnel significatif sur l'état de santé de la personne. Bien que rédigée en des termes suffisamment large, il résulte des actions de communication de la CNIL que cette définition repose sur des critères objectifs permettant ainsi de renforcer la protection des droits et libertés des personnes lorsque leurs données sont traitées dans un cadre non traditionnel.

287. **La donnée de santé, une donnée médicale.** Le G29 adopte une approche extensive de la donnée médicale. Ainsi, dans son document de travail de 2007[253], le G29 applique ce qualificatif *« aux données à caractère personnel lorsqu'elles présentent un lien clair et étroit avec la description de l'état de santé d'une personne »*. Il recommande d'inclure dans cette définition l'ensemble des données figurant dans les dossiers médicaux en considérant *que « si elles n'étaient pas pertinentes dans le cadre du traitement du patient, elles n'auraient pas été, et n'auraient pas dû être, incluses dans un dossier médical »*[254]. Figurent parmi ces données, « *les données sur la consommation de médicaments, d'alcool ou de drogue et les données génétiques (…) données administratives (numéro de sécurité sociale, date d'admission à l'hôpital, etc.) – contenues dans les documents médicaux relatifs au traitement d'un patient »*.

288. **La donnée de santé, une donnée médico-sociale.** C. BRETON-RAHALI soutient que *« la distinction entre les données de santé et les données médico-sociales ne semble pas réalisable. Les données médico-sociales sont des données personnelles, des données de santé, des données sensibles, mais ne sont pas une catégorie sui generis de données »*[255].

---

[253] Groupe de travail de l'article 29 (G29) 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.

[254] *Ibid*., p. 8.

[255] C. BRETON-RAHALI, Le secret professionnel et l'action médico-sociale, Thèse, Nancy, 2014, p. 187.

289. Bien qu'au regard de la définition de la donnée de santé retenue au sein du paragraphe 15 de l'article 4 du Règlement et à la distinction opérée entre les systèmes de soins de santé et de la protection sociale, au sein des considérants 52 et 53 cette thèse ne semble pas trouvé d'écho au niveau communautaire, nous y adhérons.

290. Les données médico-sociales sont composées de données relatives à la santé physique ou mentale, aux services de soins dispensés aux usagers, ainsi que des données d'état civil, des données relatives aux aidants familiaux, ainsi qu'aux autres services, dont l'usager est bénéficiaire, tel que l'aide à domicile, etc.

291. Les données en rapport à la protection sociale ou avec un handicap ne posent pas de difficultés particulières quant à leur nature car elles intègrent, eu égard aux dispositions du considérant 35 du Règlement, les données à caractère personnel relatives à la santé. En ce qui concerne les données relatives à la perte d'autonomie, aux aidants familiaux, aux services d'aide à domicile etc., si elles ne paraissent pas, de prime abord, constituer des données de santé, elles peuvent toutefois apporter des éléments d'information voire d'identification de la pathologie dont souffre les usagers. De ce fait, elles peuvent donc être considérées comme des données de santé.

292. Les modifications intervenues suite à loi de modernisation de notre système de santé[256] semblent confirmer cette appréciation. En effet, il résulte de cette récente réforme une homogénéisation des règles relatives au secret et de manière indirecte, à la protection des données traitées dans les champs sanitaires et médico-sociaux. Ainsi, les dispositions de l'article L. 1110- 4 alinéa 1 du Code de la santé publique reconnait désormais, dans les mêmes termes, aux patients, usagers le même droit au respect de sa vie privée et du secret des informations les concernant. Il en résulte que les

[256] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

informations mais aussi les données sont soumises au même régime de protection en ce qui concerne la préservation de l'intimité.

293. Par ailleurs, les nouvelles dispositions de l'article L. 11118 du Code de la santé publique obligent dorénavant les hébergeurs proposant leurs services aux professionnels de l'action sociale et médico-sociale d'être préalablement autorisés pour exercer cette activité. Cette obligation est toutefois limitée à l'hébergement des données à caractère personnel relatives à la santé recueillies à l'occasion d'activité de suivi social et médico-social. Il semble toutefois, difficile de concevoir que les professionnels et structures sociales et médico-sociales puissent aisément distinguer, au cours de leur activité, les données présentant un caractère social des données de santé ainsi que les finalités des traitements mis en œuvre et ainsi recourir à différents supports et hébergeurs en fonction de la nature des données collectées et conservées. Aussi, cette nouvelle obligation pourrait conduire *de facto* à une harmonisation de la protection.

CONCLUSION DU CHAPITRE 2

295. **La qualification de la donnée détermine le régime de protection applicable**. Ainsi, le rattachement d'une donnée à une personne, permet l'application des dispositions de la loi relative à l'informatique, aux fichiers et aux libertés ainsi que l'application du Règlement général sur la protection des données.

296. **Le caractère indirectement identifiant une source de complexité mais de sécurité.** S'agissant de données ayant fait l'objet de mesures de pseudonymisation, ou d'un procédé d'anonymisation, l'appréciation du caractère indirectement identifiant n'est pas toujours aisé. *« Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de 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 ».*[257] Il appartient au responsable de traitement de contrôler tout au long de la réalisation des opérations de traitements, que les conditions initiales de sa mise en œuvre sont toujours satisfaites.

297. **L'identification est une condition essentielle et déterminante.** La qualification est déterminante de l'application des dispositions de droit national et communautaire relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

[257] Règl. (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, considérant 26, Préambule, JOUE L 119, 4 mai 2016.

298. Les traitements peuvent recourir à un identifiant. Ce moyen constitue une mesure de sécurité supplémentaire afin de préserver la vie privée de la personne concernée par le traitement de ses données. Au sein du système d'information de santé, le recours à un identifiant national constitue essentiellement un moyen permettant de limiter les risques et erreurs liés à l'identification des personnes prises en charge. Il fiabilise l'identification de ces personnes et des données de santé les concernant afin de permettre l'échange et le partage de données médicales et administratives tout au long de leur prise en charge.

299. Nous ne sommes pas favorable à l'utilisation du numéro d'inscription au répertoire des personnes physiques en qualité d'identifiant national de santé en raison de son caractère signifiant. Bien que son utilisation diminue drastiquement les risques d'identito-vigilance susceptibles de ses présenter, le recours au NIR en qualité d'identifiant national de santé, augmente le risque d'atteintes à la vie privée en raison de la facilité avec laquelle il permet de rapprocher les informations relatives à une même personne. Cet identifiant constitue effectivement un identifiant sectoriel puisque son utilisation devient obligatoire dans le secteur de la santé[258].

300. Toutefois, celui-ci étant utilisé dans d'autres secteurs d'activité, il ne constitue pas, selon nous, un identifiant adapté. A titre d'exemple, le traitement de ce numéro d'identification est également réalisé par les organismes d'assurance, ou de capitalisation mais aussi *« par des services ayant pour mission d'établir l'assiette, de contrôler et de recouvrer des impositions*[259] *»*. Afin de diminuer les risques qui pèsent sur la sécurité des données de santé ainsi que sur les droits et libertés de la personne, il

[258] C. santé publ. art. R. 1111-8-1.

[259] Délibération n° 2017-245 du 14 septembre 2017 portant avis sur un projet d'arrêté portant création à la direction générale des finances publiques d'un traitement automatisé de données à caractère personnel de reconnaissance des usagers et de restitutions enrichies dans le cadre du prélèvement à la source (demande d'avis n° 2057436).

conviendrait de revenir à une politique de cantonnement de l'identifiant nationale santé afin de restreindre son utilisation dans le but qu'elle soit dédiée au secteur de la santé.

CONCLUSION DU TITRE I

302. **Le système de santé protège l'information.** Que la protection soit réalisée en ayant recours aux moyens traditionnels du droit. c'est-à-dire à la confidentialité[260] ou au secret professionnel[261]. l'information confiée ou traitée au sein du système de santé fait l'objet d'une protection exhaustive. Les professionnels intervenant dans le système de santé, qu'il s'agisse des professionnels de santé, de professionnels du champ social et médico-social, de professionnel du département de l'information médicales, sont soumis au secret professionnel. Leur obligation de se taire ne peut être levée qu'en raison d'une valeur sociale protégée jugée supérieure.

303. Les données de santé à caractère personnel, peuvent être partagées dans les conditions définies à l'article L. 11110-4 du Code de la santé publique. Ainsi, l'assujettissement au secret professionnel, ne constitue, pas un obstacle à la circulation de l'information ou de la donnée de santé par l'échange ou le partage.

304. La définition de la notion de donnée de santé issue de l'article 4 du Règlement inclus toute une série de données qui échappait auparavant aux dispositions applicables aux traitements de données sensibles. La qualification de données à caractère personnel relative à la santé doit être appréciée au cas par cas et tenir compte de trois critères.

[260] C. civ. art 9.

[261] C. pén. art. 226-13.

305. **Le critère de la nature de la donnée.** Entre dans ce critère les données produites par le système de santé. Celles-ci ne semblent toujours pas poser de difficultés.

306. En raison des dispositions de l'article 4, 15 et du considérant 35 du Règlement 2016/679 cette donnée constitue une donnée à caractère personnel relative à la santé qu'elle soit collectée lors de l'inscription de la personne physique en vue de bénéficier de services de soins de santé, qu'il s'agisse d'un numéro, d'un symbole ou d'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 »*

307. **Le critère du croisement de données.** Le croisement de données peut résulter d'un rapprochement ou d'une interconnexion de fichiers. Les données de bienêtre relèvent habituellement de cette catégorie. Ainsi les données physiologiques telles que le poids, la fréquence cardiaque, la tension lorsqu'elles sont croisées entre elles où avec des données à caractère personnel communes telles que l'âge, le sexe ou encore avec des données d'activité ou de diététique, sont susceptibles de fournir des informations sur l'état de santé d'une personne.

308. **Le critère de a destination.** Ce critère concerne des données qui ne portent pas sur l'état de santé d'une personne mais qui sont susceptibles d'être utilisées à des fins thérapeutiques ou de prévention. À titre d'exemple, l'appartenance à une confession peut être collectée afin de

proposer un régime alimentaire adapter lorsque la personne présente des carences.

309. Dès lors que la qualification de données à caractère personne relative à la santé est retenue, son traitement sera régie par des dispositions particulières adaptées aux risques que représente le traitement pour la vie privée de la personne.

TITRE II. UNE PROTECTION EFFECTIVE

310. **La donnée de santé, un bien convoité.** L'actualité ne cesse de nous rappeler à quel point les données à caractère personnel relatives à la santé sont un bien[262] sujet à convoitise. La cybercriminalité explose et les vols d'information sont de plus en plus sophistiqués, avec des conséquences parfois majeures sur la vie privée. Le Règlement européen sur la protection des données personnelles (RGPD) a pour objectif d'assurer une protection effective des données à caractère personnel dans l'ensemble de l'Union européenne, et d'autre part de lever les entraves à la libre circulation des données à caractère personnel au sein du marché intérieur.

311. **Un renforcement et une uniformisation de la protection des données.** La protection des droits fondamentaux des personnes concernées, notamment de leur vie privée, ainsi que la libre circulation des données à caractère personnel passe nécessairement par une protection effective et efficace des données à caractère personnelle, cela afin de s'assurer notamment de la confiance des personnes concernées par le traitement de leurs données dans les opérations réalisées,. Le RGPD adapte ainsi le régime de protection des données à caractère personnel aux nouvelles technologies, par la même le renforce et l'uniformise au sein de l'Union européenne afin d'en assurer l'effectivité et favoriser la circulation de l'information.

312. **Une protection des données reposant sur deux piliers.** Cette effectivité repose sur deux piliers le premier étant une utilisation maitrisée de la donnée à caractère personne (Chapitre 1) passant par une consolidation des droits de la personne sur ses données et la responsabilisation accrue des acteurs vis-à-vis des traitements de données.

[262] Le terme est ici employé de manière usuelle.

313. Le second pilier consiste en le renforcement du contrôle a posteriori (Chapitre 2) et des pouvoirs de sanction de l'autorité national de contrôle afin de dissuader les responsables de traitement de manquer à leurs nouvelles obligations

CHAPITRE 1. UNE UTILISATION MAITRISEE

315. Le recours aux technologies de l'information et de la communication, contribue à la diffusion et à faciliter l'accès à la donnée de santé. Au-delà des problématiques de sécurité des systèmes d'information, les principales atteintes à la vie privée résultent habituellement d'erreurs humaines commises par les détenteurs des données, qui, en raison d'organisations ou de comportements inadaptés aux menaces, rendent accessibles des informations qualifiées de sensibles. Ainsi, la consolidation des droits de la personne sur ses données (Section 1), requière en contrepartie sa responsabilisation afin d'en préserver la sécurité et de la confidentialité. La protection effective des données à caractère personnel relatives à la santé s'accompagne également de mesures ayant pour objet de responsabiliser les autres acteurs qui concourent à la mise en œuvre des traitements (section 2).

Section 1. Une consolidation des droits de la personne

« Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant (…) »[263]

317. **De la protection à l'autonomisation.** Le Règlement général sur la protection des données, préserve la logique personnaliste qui a toujours présidée à notre réglementation nationale en protégeant non pas les données personnelles dont chacun serait propriétaire mais l'individu dont elles émanent. Cette approche a aujourd'hui besoin d'être complétée afin qu'elle ne permette pas seulement une protection des personnes mais aussi leur autonomisation dans l'univers numérique. Cette autonomisation s'entend comme la capacité des personnes à exprimer leur volonté quant à l'utilisation de leurs données.

318. **La liberté de choisir et de contrôler ses données.** Il était nécessaire d'adapter notre législation afin de tenir compte des évolutions que le droit au respect de la vie privée et le droit à la protection des données à caractère personnel ont subies ces dernières années. Ces transformations

[263] Cet alinéa supplémentaire à l'article 1 de la loi informatique et libertés, résulte de l'article 54 de la loi pour une République numérique. Il fait suite à une proposition du Conseil d'Etat formulée dans son étude annuelle pour l'année 2014 et portant sur « Le numérique et les droits fondamentaux ». Ce rapport s'inspire lui-même du principe d'autodétermination informationnelle consacré par un arrêt de la Cour constitutionnelle fédérale allemande du 15 décembre 1983. A l'occasion de cet arrêt, la cour allemande a défini ce droit comme « le pouvoir reconnu à l'individu (…) de décider en premier lieu lui-même quand et dans quelle mesure des faits relatifs à sa propre existence sont divulgués ».»

s'apparentent de plus en plus à une exigence de libre épanouissement de la personnalité et à un désir d'autonomie individuelle.

319. *« L'individu ne s'attend pas seulement à voir sa vie privée préservée de toute immixtion extérieure, il revendique également la liberté de choisir et de contrôler les conditions dans lesquelles ses données personnelles peuvent être collectées et utilisées. »*[264]

320. Il n'est pas ici question de remettre en cause la philosophie générale de la législation sur l'informatique et les libertés, fondée sur la protection de la personne et non celle de ses données. Il s'agit au contraire de la conforter *« en lui donnant pour objectif de réparer l'asymétrie informationnelle et décisionnelle qui existe actuellement entre les individus et les responsables de traitements. Pour ce faire, le principe de consentement préalable de l'individu au traitement de ses données à caractère personnel relatives à sa santé doit être conservé, généralisé mais également adapté à l'ère numérique »*[275] (Paragraphe 1). Pour que le consentement de l'individu soit parfaitement éclairé et effectif, il doit également se voir reconnaître un droit à l'information et de véritables droits d'action dans la mise en œuvre de ces traitements. (Paragraphe 2).

[264] C. PAUL, C. FERAL-SCHUHL, Rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, n° 3119, Assemblée nationale, oct. 2015. 275 *Ibid.*

§ 1. Un pouvoir de décision affirmé

322. *« Le droit au respect de la vie privée comporte donc deux composantes : un droit 'interne' de préserver sa sphère d'intimité des intrusions extérieures, et un droit « externe » de déployer librement sa personnalité dans la vie sociale, notamment en communiquant ses informations personnelles selon sa convenance. L'extension croissante des domaines de la vie connectés soulève évidemment de nombreuses questions en matière de protection de la vie privée. »*[265]

323. **Un pouvoir de décision consolidé mais encadré.** Le Règlement consolide le lien entre la personne concernée par un traitement et ses données à caractère personnel, en lui reconnaissant le droit d'affirmer sa volonté. Par cette autonomisation, la personne devient un véritable acteur de la protection de ses données (A). Le Règlement comporte pour autant des garde-fous laissant aux Etats membres de l'Union européenne la possibilité par une disposition législative nationale, de protéger la personne concernée par un traitement d'elle-même (B).

A. La personne concernée : un acteur de la protection

324. *« Alors que le droit à la protection des données peut être perçu comme un concept défensif, le droit à l'autodétermination lui donne un contenu positif : il ne s'agit plus seulement de protéger le droit au respect de la vie privée, mais d'affirmer la primauté de la personne qui doit être en mesure d'exercer sa liberté (…) En ce sens,*

[265] CNCDH. *Avis « protection de la vie privée à l'ère numérique »,* 22 mai 2018. p. 7.

le droit à l'autodétermination répond d'avantage à l'aspiration croissante des individus à l'autonomie de la décision »[266]

325. **La consécration du principe d'autodétermination informationnelle.** L'individu n'est pas réductible aux informations qu'il produit ou qui sont collectées à son égard. En conséquence, ses données à caractère personnel ne sont pas consubstantielles de sa personne. Elles doivent toutefois être considérées comme des empreintes de son individualité. Le principe d'autodétermination informationnelle dégagé par la Cour constitutionnelle fédérale allemande[267] dès 1983 s'inscrit dans cette pensée. À l'occasion de cet arrêt, la Cour allemande a défini ce droit comme *« le pouvoir reconnu à l'individu (…) de décider en premier lieu lui-même quand et dans quelle mesure des faits relatifs à sa propre existence sont divulgués ».* La Cour de Karlsruhe, a observé *ab initio* que ce droit devait être rattaché aux principes de dignité de la personne humaine et au droit au libre développement de la personnalité, entendu comme le droit à l' *« autonomisation dans l'univers numérique* »[268].

326. **L'intégration de ce nouveau principe en droit français.** En droit français, cette notion n'est pas exprimée[269] mais transparait du droit à la liberté reconnus à l'article 2 de la Déclaration des droits de l'homme et du citoyen du 26 août 178 auquel le Conseil constitutionnel a rattaché le droit au respect de l'intimité de la vie privée[270].

---

[266] Etude annuelle du Conseil d'État, « Le numérique et les droits fondamentaux », 2014, p.267-268

[267] Tribunal constitutionnel allemand, 15 oct. 1983 (B VerfGE 65,1 - Volkszählung Urteil des Ersten Senats vom 15 Dezember 1983 auf die Mündliche Verhandlung vom 18 und 19 oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den verfahren über die Verfassungsbeschwerden).

[268] C. PAUL, C. FERAL-SCHUHL, Rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, n° 3119, Assemblée nationale, oct. 2015.

[269] X. BIOY, *« Le libre développement de la personnalité en droit constitutionnel : essai de comparaison (Allemagne, Espagne, France, Italie, Suisse) », RIDC,* janvier-mars 2003, p. 123.

[270] Cons. const. 23 juillet 1999, 99-416 DC.

327. Ce principe s'est développé progressivement en Europe puis, a été intégré à notre législation nationale au moyen de la loi de 2004 transposant la directive de 1995. Celle-ci confie à la personne concernée la responsabilité d'apprécier les risques que représente le traitement sur ses droits et libertés et de décider, en fonction de son propre intérêt, si elle admet que ses données soient traitées.

328. Jusque l'adoption de la loi pour une République numérique, ce principe transparaissait des dispositions de la loi Informatique et Libertés mais n'était pas distinctement exprimé. L'article 54 de la loi du 7 octobre 2016 adjoint aux dispositions de l'article 1 de la loi Informatique et Libertés un alinéa supplémentaire : *« Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant (…) »*

329. Cet alinéa fait suite à une proposition du Conseil d'Etat formulée dans son état annuel pour l'année 2014 et portant sur *« Le Numérique et les droits fondamentaux »* qui s'inspire lui-même du principe consacré par la Cour constitutionnelle fédérale allemande. Ces nouvelles dispositions vont au-delà du simple cadre de l'expression de la volonté et consacre explicitement en droit français le droit pour la personne de décider librement et pour elle-même des usages qui sont faits ou pourront être fait de ses données mais aussi, sa faculté de contrôler cette utilisation. Comme le souligne A. Nieto : *« La vie privée semble trouver son axe de développement à travers l'autodétermination et le contrôle informationnel des données personnelles »*[271].

330. **Une conception personnaliste et active de la protection.** Le règlement général sur la protection des données octroie des droits supplémentaires à la personne par « une quatrième génération de droits,

[271] A. NIETO, *La vie privée à l'épreuve de la relation de soin*, Thèse, Montpellier, 2017, p. 98.

positifs et non pas réactifs »[272] afin de renforcer par des mesures juridiques concrètes ce principe intégré par le droit français en 2004. La reconnaissance de ces nouveaux droits ou encore la consolidation de droits préexistants ne se limite pas à l'information et au consentement de la personne. Celle-ci peut s'exprimer librement et de manière éclairée quant aux opérations susceptibles d'être réalisées sur ses données (collecte, conservation, transfert, etc.) ainsi que sur la finalité poursuivie par le responsable du traitement. Cependant, elle est désormais dotée de moyens de nature à lui permettre de maitriser la gestion de ses données. Malgré cela, ce droit s'inscrit dans une approche personnaliste et non patrimoniale qui s'oppose ainsi à la législation Américaine en matière de protection des données : *« (…) étant propriétaire de ses données, l'individu pourrait les vendre, notamment à des acteurs étrangers. Or la grande supériorité intellectuelle du droit à la protection des données personnelles réside dans le fait qu'il reconnaît le droit d'un individu même si les données sont traitées par d'autres »*[273].

331. Il ne s'agit donc pas de considérer la protection des données à caractère personnel *« comme une valeur en soi, finale,*[274] *mais 'seulement' comme une valeur 'instrumentale' un outil, essentiel toutefois, au service de l'exercice par les individus de leur droit fondamental, au libre développement de leur personnalité »* [275]. Ce principe procède d'une conception positive et active de la protection des données et de la vie privée. La personne concernée par le traitement n'est pas considérée comme un spectateur passif bénéficiant d'une protection certes accrue

[272] I. FALQUE-PIERROTIN, auditionnée par C. PAUL, C. FERAL-SCHUHL, rapport préc. p. 135.

[273] *Ibid.*

[274] R. REZSOHAZY, *Sociologie des valeurs*, Armand Colin, 2006, p. 144.

[275] Y. POULLET, A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel – Une réévaluation de l'importance de la vie privée pour la démocratie

», in K. BENYEKHLEF, BenyekhlefP. TRUDELTrudel (dir.), *État de droit et virtualité*, Montréal, Thémis, 2009.

mais uniquement fondée sur une approche défensive. Elle n'est pas privée de sa capacité à déterminer par elle-même les limites de son intimité et à assurer la protection de ses choix privés dans la sphère publique. Ainsi, elle peut également décider de retirer son consentement à tout moment, aussi simplement que lorsqu'elle l'a exprimé. Ce retrait ne compromet pas la licéité du traitement antérieur fondé sur le consentement et démontre que la personne concernée est un acteur de la protection des données. Elle n'est pas enserrée de manière irrémédiable et doit pouvoir bénéficier d'un véritable pouvoir décisionnel quant à l'utilisation de ses données y compris lorsque celles-ci sont ont été confiées au responsable du traitement.

332. **Une dérogation au principe d'interdiction de traitement de données sensibles.** Bien que la protection des données à caractère personnel relatives à la santé repose sur un principe d'interdiction général de toute opération portant sur cette catégorie de données [276], la loi Informatique et Libertés « pré-légitimise », à titre d'exception, certains traitements[277].

333. À ce titre, le consentement constituait, *ab initio*, l'une des dérogations admises dans le cadre de la version initiale de la loi de 1978[278]. En 1995 puis en 2016, le Parlement européen et le Conseil de l'Union européenne, ont repris cette dérogation au sein du paragraphe 2, a) de l'article 8 de la directive puis 2, a) de l'article 9 du règlement 2016/679.

334. Contrairement aux autres exceptions définies au sein de l'article 9, tels que les traitements mis en œuvre dans le cadre de la santé

[276] Dir. (UE). PE et Cons. UE 1995/46, 24 oct. 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, art. 8.,. JOUE L 281, 23 nov. 1995.

[277] C. ZORN, *op. cit*., p. 226, n° 254.

[278] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 31.

publique[279], ou encore nécessaires aux fins *« de la médecine préventive, (…) 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 (…) »*[280] , cette dérogation constitue une profonde remise en cause du principe d'interdiction de traiter des données « sensibles ». En effet, celle-ci ne se limite pas à une finalité prédéfinie par la réglementation. De ce fait, il est laissé une entière liberté à la personne, d'autoriser, le responsable du traitement à déroger au principe de l'interdiction de traiter des données de santé.

335. C'est pourquoi, en ce qui concerne la volonté de la personne, le droit ne peut faire l'économie de garanties visant à s'assurer la réalité du consentement afin que la volonté de l'individu ne soit pas supplantée. Dans ce cadre, les conditions d'expression et de recueil du consentement ont été volontairement explicitées au sein du Règlement.

B. La personne concernée : une personne protégée

336. L'autodétermination informationnelle permet à la personne de librement décider de l'utilisation de ses données à caractère personnel mais au-delà de cette notion d'autonomie il s'agit également de préserver l'intimité de sa vie privée et ses droits et libertés. Ainsi, l'autodétermination informationnelle *« fait (re)surgir un débat juridique et philosophique sur le libre arbitre de l'homme qui oppose, sans fin, les tenants d'une nécessaire protection de l'homme contre lui-même au nom du principe de dignité de la personne humaine (ce qui fonde une conception relativiste du consentement) aux partisans d'une liberté individuelle inconciliable avec de quelconques restrictions à l'autonomie*

[279] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, art. 9, (i),). JOUE L 119, 4 mai 2016.

[280] UE *Ibid.*

de la volonté et donc d'une conception absolutiste du consentement vu comme "le pouvoir de soi sur soi" « [281].

337. **Une conception relativiste du consentement.** Il existe des situations où la personne concernée n'est pas réellement en mesure de pouvoir décider. Il peut arriver qu'elle soit dans une situation défavorable la poussant à accepter un traitement de ses données susceptible de la léser. Il apparaît donc que le consentement n'est pas toujours le moyen le plus indiqué pour légitimer le traitement de données sensibles. Le principe d'autodétermination informationnel n'est, par conséquent, pas sans limite[282]. Tout comme le paragraphe II, a) de l'article 8 de la directive de 1995, le paragraphe II, a) de l'article 9 du règlement 2016/679, nuance la portée du consentement explicite en tant que dérogation à l'interdiction de traiter des données à caractère personnel relatives à la santé. Cette subtilité, ne constitue pas une véritable remise en cause du principe d'autodétermination informationnelle mais laisse toute latitude aux États-membres pour introduire les garde-fous nécessaires afin d'empêcher que des atteintes disproportionnées aux droits et libertés soient consenties par la personne, que celle-ci soit mal avisée ou confrontée vis-à-vis du responsable du traitement à un rapport déséquilibré.

338. Cette disposition permet aux institutions de chaque État, d'apprécier, en fonction de leur histoire et culture propre, où doit être placé le curseur entre les libertés individuelles ainsi que d'autres valeurs protégées ou intérêts escomptés. C'est dans ce cadre que la France a adopté, en 2003, sur les recommandations de la commission des lois, cette restriction au principe d'autonomie[283]. En ce sens, il est notamment interdit

---

[281] E. BROSSET, *« Brosset. Consentement, santé et droit européen » in* A. LAUDE (dir.), *Consentement et santé*, Dalloz, coll. Thèmes et commentaires, 2014, p. 165..

[282] F.Fr RIGAUX, La protection de la vie privée et des autres biens de la personnalité, Bruxelles-Paris, Bruylant-LGDJ, 1990, p. 588-589, n° 532.

[283] A. TÜRK, Rapport fait au nom de la commission des lois sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, n° 218, Sénat, Session ordinaire 2002-2003, p. 60.

pour les assureurs de traiter des données génétiques[284] et le consentement de la personne concernée ne peut défaire ces entreprises et organismes de cette interdiction[285]. Cette exception à l'exception constitue une entrave supplémentaire à la libre circulation des données, mais ne devrait pas être considéré comme caractérisant une remise en cause du principe d'autodétermination informationnelle conforté par le règlement. Il s'agit principalement d'une mesure visant à protéger la personne concernant des traitements pouvant porter une grave atteinte à ses droits et libertés notamment à l'intimité de sa vie privée.

339. *« Il est (…) essentiel de préciser les limites du consentement et de s'assurer que seul un consentement conforme au droit est considéré comme tel. »*[286] Il résulte des dispositions du paragraphe 11 de l'article 4 que le consentement doit être compris comme « *toute manifestation de volonté, libre, spécifique, informée et explicite par laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement »* [287] . Le Parlement européen et le Conseil de l'Union européenne, en précisant les conditions du consentement, ont renforcé, au moyen du règlement, la force et la portée de la volonté de la personne. Il ressort des considérants 33 à 34 de la proposition[288] et 43 du règlement que

[284] Convention européenne sur les Droits de l'Homme et la biomédecine, signée à Oviedo le 4 avril 1997, art. 12.

[285] Voir notamment art. 16-10 du Code civil, L. 133-1 du Code des assurances et L. 1141-1 C. santé publ.

[286] Avis du contrôleur de la protection des données du 14 janvier 2011

[287] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, art. 4 (11). JOUE n° L 119, 4 mai 2016.

Dans la définition, figurent en caractères gras, les éléments additionnels par rapport à l'art. 2, (h), de la Directive 95/46/CE PE et Cons., 24 oct. 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.

[288] Proposition de Règlement du Parlement européen et du Conseil 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, 25 janv. 2012, COM(2012) 11 final, 2012/0011 (COD),) p. 8.

la réalité du consentement devrait être appréciée *in concreto* en prenant notamment en considération le rapport de force entre le responsable du traitement et la personne concernée. De ce fait, pour que le consentement de la personne soit exprimé librement, il ne devrait pas exister de rapport manifestement déséquilibré entre les parties : *« L'autonomie de la personne concernée est à la fois une condition préalable et une conséquence du consentement »* [289] . Ainsi, l'existence de mesures coercitives, de tromperies ou encore de conséquences néfastes de l'acceptation ou au refus d'une opération de traitement de données à caractère personnel sont de nature à vicier le consentement car celui-ci n'est pas exprimer librement.

340. Ce faisant, le règlement reprend les travaux du G29 sur la notion de consentement. Ainsi, pour être libre, le consentement nécessite *« l'absence de toute coercition, qu'elle soit sociale, financière, psychologique ou autre »*[290]. Au sein de ce même avis, le G29 précise que le consentement, lorsqu'il est donné *« sous la menace de privation de traitement ou de traitement de moindre qualité dans une situation médicale ne saurait être considéré comme libre. [...] lorsque la situation médicale exige nécessairement et inévitablement que le praticien de la santé traite des données à caractère personnel dans un système DME, il est trompeur que ce praticien cherche à légitimer ce traitement par le consentement. Le recours au consentement doit être limité aux cas où la personne concernée est véritablement libre de son choix et a la possibilité de retirer ultérieurement son consentement sans subir de préjudice »*[291].

[289] Groupe de travail de l'article 29 (G29) sur la protection des données, Avis 15/2011 sur la définition du consentement, adopté le 13 juillet 2011, p. 9.

[290] *Ibid.*,p.14.

[291] *Ibid.* Voir aussi Groupe de travail de l'article 29 (G29) sur la protection des donnéesG29), 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.

341. En ce sens, la personne peut consentir ou s'opposer de manière éclairée, libre et indubitable à un traitement de ses données de santé. Elle n'est pas *in abstracto* et *de jure* considérée, à l'instar du consommateur, comme une partie vulnérable. Elle doit toutefois être protégée lorsque sa situation l'exige. Ainsi, le consentement exprimé par une personne en situation de vulnérabilité notamment économique devrait, au regard de la sensibilité de ces données et de sa situation être considérée comme étant vicié.

342. Notons qu'il ressort des travaux préparatoires que le qualificatif « explicite » a été volontairement ajouté à la liste des critères *« afin d'éviter tout parallélisme prêtant à confusion avec le consentement « indubitable »*[292] *et de disposer d'une définition unique et cohérente du consentement, garantissant que la personne concernée donne son consentement [sans ambiguïté et] en toute connaissance de cause »*[293]. De la même manière, *« la directive [va au-delà de cette simple acception puisqu'elle] considère que les risques pour les droits et libertés de la personne concernée sont présumés maîtrisés dès lors que celle-ci a valablement consenti au traitement de ses données médicales ».*

343. Enfin, pour que le consentement soit valable, il doit reposer sur l'information de la personne concernée. Le Règlement général sur la protection des données de santé exige en son article 13 que celle-ci soit formulée de manière compréhensible et être délivrée de façon concise et

---

Voir également l'Avis 8/2001 sur le traitement de données à caractère personnel dans le contexte professionnel du Groupe de travail de l'article sur la protection des données (G29), WP 48, point 10.

[292] Le consentement est indubitable lorsque « la procédure relative à l'obtention et à l'octroi du consentement ne [laisse] aucun doute quant à l'intention de la personne concernée de donner son consentement. En d'autres termes, la manifestation de volonté par laquelle la personne concernée marque son accord ne doit laisser aucune ambiguïté quant à son intention. S'il existe un doute raisonnable sur l'intention de la personne concernée, il y a ambiguïté (…). » (Groupe de travail de l'article 29 (G29) sur la protection des données, Avis 15/2011 sur la définition du consentement, p. 23)

[293] Proposition de Règlement, préc., p. 8.

transparente afin d'être accessible pour le grand public. Ces critères posent beaucoup de difficultés notamment en ce qui concerne les traitements comportant plusieurs finalités pour lesquels les personnes concernées doivent consentir individuellement. Compte tenu du nombre de traitements mis en œuvre par les acteurs intervenant dans le système de santé, notamment en ce qui concerne les projets régionaux, cette obligation n'est pas sans poser de difficultés et interroger sur la compréhension qu'ont les personnes concernée des traitements et de leurs droits. La CNIL préconise ainsi de travailler sur les supports d'information afin de les rendre les plus intelligibles possible, en ayant par exemple recours à l'utilisation de pictogrammes visuels, la mise en valeur des informations essentielles sur les supports afin de les rendre l'information la plus intelligible possible.

344. Notons toutefois que, quel que soit le traitement mis en œuvre par les acteurs du système de santé, les droits de la personne ne changent pas. Il est donc possible, lorsque l'organisation des acteurs le permet de proposer une information standardiser en ce qui concerne les modalités d'exercice des droits de la personne et de l'accompagner d'une information spécifique et adaptée en fonction des modalités propres aux finalités poursuivies. Enfin, il est également concevable d'adapter le support en fonction du public. De recourir à l'emploi de vidéos, de messages audio, de fiches standardisées.

§ 2. Des droits de gestion étendue

346. *« L'individu ne s'attend pas seulement à voir sa vie privée préservée de toute immixtion extérieure ; il revendique également la liberté de choisir et de contrôler les conditions dans lesquelles ses données personnelles peuvent être collectées et utilisées. »*[294]

347. Depuis sa genèse, la règlementation relative aux traitements de données à caractère personnel se caractérise, à l'instar des droits des malades, par un *empowerment* graduel de l'individu[295]. Celui-ci se voit, au fur et à mesure de l'adoption de nouveaux textes, octroyer davantage de droits afin de lui permettre, d'être participatif, d'agir pour la protection de ses données. Pour être effectifs, ces droits devraient être accompagnés de moyens organisationnels, techniques et, de mesures de contrôle permettant de s'assurer que l'individu est indubitablement en mesure d'accéder à ses données, de s'opposer à leur transfert, d'en obtenir l'effacement ou, le cas échéant, la rectification, ou encore la communication dans un format structuré, couramment utilisé et lisible par machine[296].

348. Des droits faisant l'objet de dispositions spécifiques. Contrairement à la directive de 1995 et à la loi Informatique et Libertés, les droits d'accès de rectification, d'effacement font l'objet, au sein du RGPD, de dispositions spécifiques en précisant la teneur.

---

[294] C. PAUL, C. FERAL-SCHUHL, Rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, n° 3119, Assemblée nationale, oct. 2015, p. 125.

[295] La loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé illustre cette évolution. En ce sens, elle vise à l'information et l'expression de la volonté du patient pour un meilleur partage des informations et des décisions et lui reconnait un droit d'accès direct à son dossier médical.

[296] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, JOUE L 119, 4 mai 2016, art. 20.

349. À proprement parlé, en ce qui concerne le droit d'accès[297], celui-ci constitue un véritable pouvoir de contrôle exercé par l'individu sur ses données. Il présente un double intérêt pour la personne. Il lui permet de vérifier que ses données font effectivement l'objet d'un traitement, de contrôler les catégories de données ainsi que les données traitées et enfin, de pouvoir exercer ses autres droits auprès du responsable du traitement, notamment de mise à jour, de modification, de rectification de verrouillage et d'effacement.

350. Notons que la Directive prévoyait initialement que dans l'intérêt de la personne concernée ou en vue de protéger les droits et libertés d'autrui, notamment lorsque les données étaient collectées auprès de tiers, les États-membres de l'Union européenne pouvaient limiter le droit d'accès aux données. De ce fait, ils pouvaient, par exemple, préciser que s'agissant de données à caractère médical, cet accès ne pouvait être obtenu que par l'intermédiaire d'un professionnel de santé[298]. Cette faculté semble disparaître du règlement ce qui pose la question du maintien de cette spécificité en droit français notamment en ce qui concerne les dispositions des articles L. 1111-7, R. 11111 et R. 1111-6 du Code de la santé publique relatifs à l' *« accès aux informations de santé à caractère personnel des majeurs et mineurs »*.

351. Rappelons à cette occasion, que la CNIL a durcie, ces deux dernières années, sa position concernant l'exercice des droits de la personne notamment en ce qui concerne le droit d'accès à ses données. Dans une délibération n°SAN-2017-008 en date du 18 mai 2017[299], la Commission est allée jusqu'à prononcer une sanction pécuniaire conséquente à l'encontre d'un cabinet de chirurgien-dentiste. En l'espèce,

---

[297] Règl. (UE). PE et Cons. UE préc. art. 15.

[298] Dir. (UE). PE et Cons. UE 1995/46, 24 oct. 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, considérant 42.

[299] CNIL, délib., 18 mai 2017, n° SAN-2017-008 prononçant une sanction pécuniaire à l'encontre de la société d'exercice libéral à responsabilité limitée X.

la CNIL avait été saisie d'une plainte déposée par un ancien patient du cabinet. Celui-ci ne parvenait pas à obtenir, du responsable de traitement, de réponse à ses demandes d'accès aux données à caractère personnel relatives à sa santé, contenues dans son dossier médical. Après avoir sollicité, à deux reprises, le cabinet afin qu'il présente ses observations, la

352. Commission l'avait mise en demeure de définir et de mettre en œuvre une procédure effective de droit d'accès. La CNIL avait également demandé au cabinet de communiquer au plaignant une copie de ses données. Celui-ci n'ayant pas donné suite à ses différentes sollicitations, la Commission avait prononcé une sanction pécuniaire d'un montant de dix mille euros.

353. Cette délibération témoigne de la volonté de la Commission de consolider ses activités et de s'assurer de l'effectivité des dispositions de la loi relative à l'informatique et aux libertés, d'une part, en prononçant des sanctions pécuniaires sévères lorsque le responsable de traitement se montre peu coopératifs et, d'autre part, en procédant également à la publication de ses délibérations.

354. Le droit à l'effacement[300] ou droit à l'oubli numérique ne doit pas être confondu avec le *sculpting* qui consiste principalement, pour une personne, à soigner son image en supprimant les liens vers les pages non désirées ainsi que les contenus non souhaités présents sur le web et, le cas échéant, en leur substituant de nouvelles informations présentant une connotation positive.

355. Rappelons que le droit à l'effacement relève des dispositions de l'article 12 de la Directive de 1995, tandis que la mention du droit à l'oubli au sein d'une norme communautaire résulte de l'adoption de l'article 17 du règlement. Le Parlement européen s'est opposé à l'utilisation de cette

[300] Règl. (UE). PE et Cons. UE 2016/679, préc., art. 16 et 17.

notion au sein du règlement mais le Conseil y était favorable en considérant qu'il s'agissait d'un droit spécifique.

356. Nous partageons cette analyse, selon nous, le droit à l'oubli peut être appréhendé comme une déclinaison du droit à l'effacement. Il s'agit d'un droit de suppression limité aux données à caractère personnel traitées dans le cadre de l'offre de services de la société de l'information et qui concerne uniquement les données publiées dans la sphère publique.

357. Cependant, nous ne partageons pas le choix de mentionner expressément dans le titre de l'article 17 « Droit à l'effacement » (« droit à l'oubli ») car celui-ci porte à confusion. Au regard de ces spécificités, notamment en ce qui concerne les obligations d'information pesant sur le responsable du traitement ayant rendu les données publiques, il aurait été préférable de dédier, au sein du règlement, une section au droit à l'effacement comportant un article spécifique sur le droit à l'oubli.

358. Nous constatons, en ce qui concerne le droit à l'oubli, que si le responsable du traitement est tenu d'effacer les données en sa possession, y compris les copies, il n'est pas exigé qu'il impose cette obligation aux tiers qui auraient pu avoir accès à ces données ou auxquels il aurait pu les communiquer. Ainsi, il ne dispose d'aucun pouvoir concret pour imposer leur effacement. Il n'est soumis qu'à une simple obligation de moyen consistant en l'information, des autres responsables du traitement, concernant la demande de la personne concernée d'obtenir l'effacement de ses données.

359. Au regard de cette analyse, il est raisonnable de se questionner sur l'effectivité de ce droit lorsque des données de santé ont été rendues publiques par la personne concernée ou un tiers au moyen des médias sociaux ou de tout autre moyen.

360. Nous remarquons par ailleurs, qu'aucun délai n'est imposé par le règlement, au responsable du traitement, pour procéder à l'effacement des données.

361. Cette absence est de nature à remettre sérieusement en question l'effectivité de ce droit. Le considérant 59 du règlement laisse toutefois suggérer que le responsable du traitement *« devrait être tenu de répondre aux demandes émanant de la personne concernée dans les meilleurs délais et au plus tard dans un délai d'un mois »*.

362. Il est regrettable que cette mesure ne se limite qu'à une simple suggestion. Il conviendra d'analyser ultérieurement comment les Autorités de contrôle nationales apprécieront cette recommandation et le respect du règlement par les responsables du traitement. Nous notons cependant, qu'en droit Français, la loi pour une République numérique modifiant la loi de 1978 a anticipé l'entrée en vigueur du règlement en intégrant au sein de l'article 40 de la loi Informatique et Libertés cette nouvelle mesure :

363. *« En cas de non-exécution de l'effacement des données à caractère personnel ou en cas d'absence de réponse du responsable du traitement dans un délai d'un mois à compter de la demande, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés, qui se prononce sur cette demande dans un délai de trois semaines à compter de la date de réception de la réclamation. »*

364. En conséquence, ces dispositions apportent des garanties supplémentaires quant à l'effectivité de ce droit puisque la CNIL peut être saisie par l'auteur de la demande et est tenue de rendre une décision dans le délai de trois semaines à compter de la réception de la réclamation. Elle pourra, le cas échéant, solliciter le responsable du traitement afin de déterminer les raisons de ce silence, mener une enquête sous la forme d'un audit, lui adresser un avertissement ou encore ordonner au responsable du traitement de satisfaire à la demande adressée par la personne concernée, etc.[301] De surcroit, nous constatons que la loi de 1978 modifiée oblige dès à présent le responsable du traitement qui aurait l'intention de ne pas

[301] Règl. (UE). PE et Cons. UE 2016/679, données art. 58.

donner suite à une demande d'effacement de motiver sa réponse avant l'expiration de ce délai d'un mois[302].

365. Ce droit, tel qu'il est décrit au sein du règlement, constitue une garantie au respect des différents principes gouvernant la réglementation en matière de traitement de données à caractère personnel. En ce qui concerne le principe de proportionnalité[303], la personne peut demander l'effacement des données qui ne sont plus nécessaires au regard des finalités poursuivies par le responsable du traitement et pour lesquelles elles ont été traitées. Concernant le principe d'autodétermination informationnelle, la personne est fondée à demander, au responsable du traitement, la suppression des données lorsqu'elle a retiré son consentement sur lequel était fondé le traitement. À propos de la condition de loyauté et de licéité des traitements également regroupés sous le principe de transparence[304], la personne peut également demander à ce que les données qui sont par exemple, collectées par un procédé jugé frauduleux, déloyal ou illicite, soient effacées.

366. De ce fait, nous sommes en mesure de considérer que notre droit national confère à la personne concernée un réel droit à l'effacement des données. Nos propos doivent toutefois être nuancés. En effet, au regard des dispositions de l'alinéa 3 du II de l'article 40 de la loi Informatique et Libertés et du paragraphe 3 de l'article 17 du Règlement général sur la protection des données, le droit à l'effacement serait rendu inopérant en ce

[302] Le Code de la santé publique aménage aux articles L. 1111-7 et R. 1111-1 le droit d'accès du patient à l'ensemble de ses informations concernant sa santé qui sont formalisées et détenues par les professionnels de santé ou les établissements de santé. Il prévoit des délais de communication maximums spécifiques en fonction de l'antériorité des informations. Ces dispositions ont vocation à s'appliquer en raison de l'adage « *specialia generalibus derogant* ». Ce délai doit être anticipé dans la conclusion des contrats et lorsqu'il est procédé à l'externalisation de l'hébergement sous peine de pas pouvoir être respecté.

[303] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 5.

[304] *Ibid.*

qui concerne les traitements nécessaires *« pour des motifs d'intérêt public dans le domaine de la santé publique ».*

367. Le paragraphe 3 de l'article17 renvoi aux notions d'intérêt public et de santé publique qui, si nous nous référons à la définition donnée par l'Organisation mondiale de la Santé en septembre 1952[305], serait limitée aux données exploitées dans le cadre de traitements mis en œuvre à des fins de veille sanitaire, de « 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 »[306].

368. Bien qu'il soit compréhensible que ces motifs d'intérêt général soient considérés comme représentant une valeur supérieure au droit individuel de la personne, cette exception constitue une atteinte importante au droit à l'effacement et aux principes qu'il sous-tend. Cependant, les données collectées en France à ces fins son protégées par le secret professionnel ainsi que par des moyens organisationnels et techniques tel que la soumission à des organismes ayant pour mission de valider les modalités du traitement ou d'accès aux données, la pseudonymisation, le cryptage ou la limitation et la mise en œuvre de mesures techniques de contrôle des accès. Par ailleurs, bien que ces données ne soient pas supprimées, elles sont également soumises aux principes de proportionnalité et de temporalité.

369. Pour autant, le paragraphe 3 renvoi également aux dispositions de l'article 9, paragraphe 2, point (h) qui concerne les traitements nécessaires aux fins de la médecine préventive, à la médecine du travail, aux diagnostics médicaux, à la prise en charge sanitaire ou sociale, ou de la

[305] La santé publique serait « la science et l'art de prévenir les maladies, de prolonger la vie et d'améliorer la santé et la vitalité mentale et physique des individus, par le moyen d'une action collective concertée. » Comité d'experts de l'Administration de la Santé Publique, Premier rapport, Série de rapports techniques, OMS, Genève, septembre 1952.

[306] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 9 § 2 point (i)..

gestion des systèmes et des services de soins de santé ou de protection sociale. Ainsi, malgré qu'il soit explicitement fait référence aux motifs d'intérêt public dans le domaine de la santé publique, il est légitime, au regard de ces dispositions, de s'interroger sur la portée de cette exception.

370. Devons-nous considérer que cette exception concerne l'ensemble des traitements mis en œuvre par les structures, les services et professionnels du soin, auquel cas, cette atteinte serait injustifiée. De la même manière, un traitement ayant pour finalité la gestion des systèmes et des services de soins de santé ou de protection sociale n'étant pas incompatible avec un droit à l'effacement conditionné, cette exclusion nous semble disproportionnée. Ainsi, un patient devrait être en mesure de demander la suppression d'un examen, de son dossier de soins, s'il est établi que celui-ci concerne un autre patient et qu'il figure dans son dossier en raison d'une erreur d'identification.

371. De la même manière, un patient devrait être fondé à demander l'effacement d'un examen de biologie médicale, lorsque des erreurs ont été constatés sur ses résultats d'analyses [307]. Pareillement, dans l'hypothèse d'un acte thérapeutique ayant occasionné un préjudice corporel, l'obligation de conservation des données devrait être limitée à une durée n'excédant pas le délai de prescription en tenant toutefois compte de l'éventuelle minorité du patient et, le cas échéant, de l'épuisement des voies de recours. Au-delà de ce délai, le patient ayant constaté suite à l'exercice de son droit d'accès, que ses données sont encore conservées par un établissement de santé, devrait être en droit d'en demander la suppression après en avoir obtenu une copie.

[307] Voir notamment le rapport de l'Inspection des affaires sociales, La biologie médicale libérale en France, bilan et perspective, avril 2006. Ce rapport a mis en exergue un taux d'erreur de 10% des résultats d'analyse de biologie médicale et à la suite duquel un mécanisme d'accréditation des laboratoires d'analyses médicales a été mis en œuvre à compter de 2013.

372. Au regard de ces différentes observations nous n'adhérons donc pas à cette analyse. Celle-ci aboutirait à une ineffectivité du droit à l'effacement et serait source d'insécurité pour la personne concernée. Ainsi, nous recommandons que ce renvoi soit précisé, le cas échéant supprimé ou que l'effacement soit conditionné afin que l'atteinte aux droits de la personne soit limitée.

373. Un droit d'opposition renforcé. L'article 38 de la loi 78-17 du 6 janvier 1978 dispose que *« toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur ».*

374. En conséquence, il ressort de ces dispositions qu'en l'état actuel du droit, une personne alléguant des motifs légitimes peut s'opposer au traitement de ses données à caractère personnel notamment relatives à sa santé. Ces dispositions sont également reprises par l'article L. 1111-8 du Code de la santé publique relatif à l'hébergement de données de santé à caractère personnel.

375. *« Toute personne qui héberge des 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, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil desdites données ou pour le compte du patient lui-même, doit être agréée à cet effet. Cet hébergement, quel qu'en soit le support, papier ou électronique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime. »*

376. Ainsi, le responsable du traitement reste donc fondé à apprécier les motifs invoqués par la personne concernée et, le cas échéant ne pas

donner suite à sa demande. Il en résulte qu'il dispose d'un certain temps pour apprécier le bienfondé des motifs invoqués et peut en rejeter la légitimé. Au regard de ces dispositions et de celles de l'article 14 de la directive de 1995, cette motivation du droit d'opposition peut constituer une atteinte à la volonté de la personne ainsi qu'à l'intimité de sa vie privée.

377. Toutefois, le responsable du traitement qui rejetterait de manière systématique la légitimité des motifs invoqués par la personne concernée encourrait, compte tenu des dispositions de l'article 226-18-1 du Code pénal, risque sérieux puisque *« le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».*

378. En ce qui concerne le règlement du 27 avril 2016, celui-ci reprend la plupart des dispositions antérieures. Cependant, son article21 renforce le droit d'opposition en ce qu'il renverse la charge de la preuve. Ainsi, sauf à démonter l'existence d'un motif légitime « et impérieux », le responsable du traitement est confronté à la nécessité de donner, sans délai, une réponse favorable à la personne ayant manifesté son opposition au traitement de ses données. Ces motifs étant dégagés par la jurisprudence, il est difficile d'en apprécier la portée. Toutefois, il parait concevable qu'un refus puisse être motivé par le fait qu'une réponse favorable serait de nature à compromettre la pérennité du système de santé ou de la protection sociale supposant ainsi, qu'il n'y est pas d'autres alternatives que de procéder au traitement considéré.

379. En tout état de cause, en cas de contentieux, le responsable du traitement ne pourrait désormais plus continuer à traiter les données dans l'attente de l'issue d'un procès. *A contrario*, la personne serait fondée à

recourir à une procédure d'urgence afin de faire respecter ses droits sans être confronté à la nécessité d'invoquer un motif légitime.

380. De cette manière, le règlement consolide les droits de la personne et créé une nouvelle responsabilité à la charge du responsable du traitement. En exigeant un motif légitime et impérieux préalablement dégagé par la jurisprudence, le règlement restreint par ailleurs les hypothèses pour lesquelles, le responsable du traitement serait légitime à s'opposer à la demande de la personne concernée. De ce fait, il déplace le curseur au profit des droits de la personne et fait peser sur le responsable du traitement une obligation supérieure à celle initialement imposée à la personne concernée par l'article 14, a) de la directive de 1995.

381. Nous remarquons par ailleurs qu'au regard du principe de légalité criminelle, les dispositions de l'article 226-18-1 du Code pénal devront être reformulées afin de tenir compte de ce renversement de la charge de la preuve.

Section 2. Une responsabilisation accrue des acteurs

383. **La responsabilisation des acteurs.** Les (co)responsables et sous-traitants sont désormais les acteurs de leur mise en conformité au Règlement général sur la protection des données. A ce tire, ils doivent penser et mettre en œuvre un système organisationnel leur permettant de préciser les rôles et responsabilités de chacun (Paragraphe 1). Concernant les traitements de données de santé, les responsables de traitements et sous-traitants sont astreints à des obligations de sécurité renforcées (Paragraphe 2) et doivent être désormais en capacité de prouver la mise en œuvre de mesures conformes aux standards nationaux.

§ 1. La mise en œuvre d'une gouvernance de la protection

384. *« La question pour une entreprise n'est plus aujourd'hui de savoir si elle va être ou non confrontée au cyber risque. Elle l'est d'ores et déjà. Et les conséquences de ce risque ont pris une telle ampleur que sa gestion n'est plus un sujet technique relevant des seules directions informatiques. Il est devenu un enjeu de gouvernance. »*[308]

385. Les obligations résultant du règlement imposent implicitement aux acteurs du système de santé, à l'exclusion des professionnels exerçant individuellement ou au sein de structures de taille réduite (maisons de santé pluridisciplinaire, cabinet infirmier) la mise en place d'une gouvernance de la donnée.

[308] Rédaction Lextenso, « Assurer le risque cyber : quels enjeux ? », LPA 4 juill. 2018, n° 133137w0, p. 2.

386. Cette gouvernance vise à définir précisément les rôles et les responsabilités de chacun des acteurs impliqués dans les activités de traitements de données à caractère personnel (A), notamment en ce qui concerne la mise en œuvre de mesures appropriées ainsi que d'une organisation respectueuse des droits de la personne et permettant au(x) responsable(s) du traitement et au(x) sous-traitant(s) de garantir un niveau de sécurité adapté au risque pesant sur les données à caractère personnel notamment lorsqu'il s'agit de données de santé. Lorsque le traitement représente un risque particulier pour la vie privée des personnes. le responsable de traitement se trouve dans l'obligation de désigné un délégué à la protection des données (DPO). Ce DPO, en raison de ses fonctions, apparait comme un réel « chef d'orchestre » de la protection (B).

A. Une répartition des rôles et responsabilités entre les acteurs

387. **Une multiplicité d'acteurs.** Au sein de chaque région, plusieurs acteurs se sont regroupés afin de créer conjointement un Espace Numérique Régional de Santé.

388. Cet espace de services dématérialisés, porté institutionnellement par l'Agence Régionale de Santé (ARS) et piloté par une maîtrise d'ouvrage régionale, a vocation à *« assurer le développement des systèmes d'information dans le système de santé, en favorisant la coopération de l'ensemble des acteurs. Il joue un rôle essentiel dans la diffusion des normes, références, recommandations posées par les autorités compétentes, pour une utilisation convergente (…) de ces infrastructures »*.[309] Il vise à construire un espace de confiance au sein duquel la sécurité et l'interopérabilité doivent être garanties. Dans cet espace, peuvent être déployés des services régionaux et des services nationaux. Ainsi, en fonction des circonstances la maitrise d'ouvrage régionale, l'ARS ainsi que les établissements de santé et structures médico-sociales et d'une

[309] S. LANGARD, Approche juridique de la télémédecine – Entre Droit commun et règles spécifiques, Thèse, Nancy, 2012, p. 237.

manière générale, les membres de la maitrise d'ouvrage peuvent, selon les circonstances endosser le rôle de sous-traitant, de responsable mais aussi de coresponsable du traitement.

389. **Une coresponsabilité naissante.** La notion de coresponsabilité n'était pas mentionnée dans la convention 108. Elle a été introduite au sein de la directive de 1995[310] suite à un amendement proposé par le Parlement européen avant l'adoption du texte. Il résulte des différentes discussions menées au cours de la procédure législative, une modification de la proposition après avis de la Commission. Celle-ci intègre au sein de la directive la possibilité, pour un même traitement, d'avoir plusieurs coresponsables *« décidant conjointement de la finalité du traitement et des moyens à mettre en œuvre pour l'effectuer (…) dans un tel cas, chacun des coresponsables doit être considéré comme tenu au respect des obligations posées par la directive en vue de protéger les personnes physiques dont les données sont traitées. »*[311.]

390. Au regard de ces éléments de définition, le simple fait pour différents acteurs de santé de coopérer à la mise en œuvre d'un traitement de données à caractère personnel, ne signifie pas que ceux-ci sont coresponsables. En effet, ces acteurs peuvent être placés dans une relation ou (co)responsable du traitement et sous-traitant coexistent ou encore dans une chaîne consistant en un ensemble d'opérations reposant sur l'échange de données, sans partage ou définition commune des finalités ou des moyens.

391. **Des coresponsabilités variées.** Dans son avis du 16 février 2010, le G29 a mis en exergue le lien qui existe entre la définition extensive du traitement de données à caractère personnel et le nombre de personnes

[310] Dir. (UE). PE et Cons. UE 1995/46, 24 oct. 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, art. 2.

[311] Groupe de travail de l'article 29 (G29) sur la protection des données, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », Adopté le 16 février 2010, p. 19.

susceptibles de participer à la mise en œuvre d'un traitement. Il en résulte que la notion de coresponsabilité peut, au regard de la multiplicité des activités qui peuvent constituées à un traitement de données, faire intervenir un nombre considérable d'acteurs. Ces personnes peuvent participer *« à plusieurs opérations ou ensembles d'opérations appliquées à des données à caractère personnel. Ces opérations peuvent se dérouler simultanément ou en différentes étapes »*.

392. En ce sens, dans le cadre d'une coresponsabilité, la participation de chacune des parties à la détermination conjointe de la finalité et des moyens du traitement ne se réalise pas nécessairement sur un plan d'égalité. En conséquence, celle-ci peut revêtir différentes formes. Nous l'avons démontré, au regard de la multiplicité des activités susceptibles de constituer un traitement, le principe de coresponsabilité peut faire intervenir une multitude d'acteurs. Ceux-ci peuvent, par exemple, partager l'ensemble des finalités mais aussi des moyens d'un traitement ou, au contraire ne partager que quelques finalités et/ou moyens relatifs à une partie des opérations de traitement ou à l'ensemble du traitement. Du fait des raisons précédemment évoquées et de la variété de situations susceptibles de se présenter, il existe donc un large éventail de typologies de coresponsabilité.

393. **Un risque de dilution des responsabilités.** Afin de tenir compte de la réalité et de la variété de ces situations et de définir précisément les rôles et responsabilités de chacun des acteurs du traitement, un partage des responsabilités semble donc intéressant aussi bien dans une dimension théorique que pratique. Toutefois, les travaux du G29 démontrent les difficultés que représentent un tel exercice et les difficultés à en apprécier les conséquences juridiques. Cette situation peut être de nature à compromettre l'efficacité de la législation sur la protection des données. Appréhendant une dilution des responsabilités et une garantie partielle des droits de la personne concernant le traitement de ses données à caractère personnel, les parlementaires français ont donc écarté cette notion lors de l'adoption de la 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 transposant dans notre droit national les dispositions de la directive 95/46/CE.

394. Nous ne sommes pas favorable à ce parti pris car il méconnait la diversité des circonstances et des organisations relatives à la mise en œuvre d'un traitement. Ainsi, la loi de 1978 peut amener les acteurs d'un traitement à attribuer fictivement la responsabilité de celui-ci alors même que les opérations ont été définies conjointement dans le cadre d'instances opérationnelles et de concertation. *A contrario,* la loi Informatique et Libertés peut également amener chacun des acteurs d'un même traitement à se considérer, par le truchement d'une fiction juridique, individuellement responsable. Si l'ensemble des diligences sont mises en œuvre par les parties, cette dernière situation, représente un risque mineur pour les droits des personnes concernées.

395. Toutefois, dans le cadre d'un système reposant sur une déclaration préalable à la mise en œuvre d'un traitement, ce dernier cas de figure peut constituer un frein à l'exploitation des données et, le cas échéant aux soins. En tout état de cause, la notion de (co)responsable du traitement étant autonome et fonctionnelle, la Commission n'est pas tenue par la volonté des parties et, en cas de litige, se livre à une analyse factuelle notamment à partir des conditions définies par le G29. Ainsi, la désignation formelle d'un responsable du traitement dans un contrat ou, le cas échéant, un « cerfa » renseigné afin de satisfaire aux formalités préalables à la mise en œuvre des traitements[312], constituait et constitue un élément d'information intéressant sur la responsabilité d'une entité mais elle ne suffit pas à elle seule à lui attribuer le statut de responsable de traitement.

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

396. D**e la consécration de la notion de *« responsables conjoints de traitement »*.** Le règlement consacre cette notion et, du fait de sa nature, l'impose de manière immédiate, simultanée et uniforme à l'ensemble des États-membres de l'Union européenne. Ainsi, il dispose en son article 26 : *« Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement »*[313] Cette consécration ne constitue donc pas une innovation mais tient compte des recommandations issues de l'avis du G29. Ainsi, le règlement va au-delà des dispositions de la directive qui se restreignent à introduire la coresponsabilité dans la définition de la notion de responsable du traitement[314]. Le Parlement européen et le Conseil de l'Union européenne, afin de garantir le respect des règles de protection des données et éviter ainsi un affaiblissement résultant d'une dilution ou d'une mauvaise attribution des responsabilités entre les différents responsables du traitement intervenant dans un environnement complexe, ont confirmé le principe de responsabilité conjointe dégagée par le G29. Cette responsabilité conjointe permet à « *la personne concernée [d'] exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement »*[315] Ce faisant, le règlement ne diverge pas de notre droit national en matière de responsabilité conjointe.

397. Il nous parait regrettable que le Règlement général sur la protection des données écarte toute solidarité passive entre les responsables. Afin d'instaurer une véritable protection de la personne, il aurait été préférable que le Règlement laisse la possibilité, de recourir la solidarité passive au sens de l'article 1313 du Code civil.

[313] Règl. (UE). PE et Cons. UE 2016/679, préc., art. 26 (1).

[314] Dir. (UE). PE et Cons. UE 1995/46, préc. art. 2 (d).

[315] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 26 (3).

398. *« La solidarité entre les débiteurs oblige chacun d'eux à toute la dette. Le paiement fait par l'un d'eux les libère tous envers le créancier.*

399. *Le créancier peut demander le paiement au débiteur solidaire de son choix. Les poursuites exercées contre l'un des débiteurs solidaires n'empêchent pas le créancier d'en exercer de pareilles contre les autres. »*[316]

400. En effet, eu égard aux dispositions de l'article 82 qui pose le principe du droit à réparation, une personne qui aurait subi un dommage matériel ou moral consécutif à un manquement aux obligations résultant du règlement, ne pourrait agir qu'à l'encontre d'un des (co)débiteurs et lui demander réparation de l'intégralité de son préjudice. Afin de garantir un droit à réparation effectif à la personne concernée et éviter une dilution des responsabilités entre les coresponsables, il aurait été souhaitable que le règlement aille au-delà de la directive en retenant également la solidarité entre le(s) responsable(s) de traitement et le(s) sous-traitants(s) et en permettant ainsi à la personne lésée de demander réparation de l'intégralité du préjudice subi au sous-traitant.

401. *« Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi. (…) / 4. Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des paragraphes 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective. »*[317]

---

[316] C. civ., art. 1313.

[317] Règl. (UE) n° 2016/679, préc., art. 82 (1) et (4)..

402. Toutefois, la (co)responsabilité et la sous-traitance étant aménagées conventionnellement, il est envisageable que le ou les manquements aux obligations résultant du règlement qui seraient à l'origine du dommage ne soient pas imputables à l'un des (co)responsable ou au sous-traitant. Dans ce contexte et afin de s'exonérer de cette responsabilité le (co)responsable ou sous-traitant sont en droit de prouver que les faits qui ont provoqués le dommage ne leurs sont nullement imputables[318]..

403. Si chacun des acteurs est responsable du dommage dans son intégralité, le codébiteur solidaire qui aurait été tenu, au-delà de sa quote-part, de régler la dette en intégralité au créancier disposerait alors d'un recours subrogatoire, à l'encontre des autres codébiteurs afin de leur réclamer leur part. Toutefois, ce recours permettant *in fine* une répartition en fonction de la part de responsabilité de chaque acteur du traitement n'est possible qu'à la condition que le dommage subi par la personne concernée soit entièrement et effectivement réparé[319].

404. Ainsi, le (co)responsable ou le sous-traitant qui aurait indemnisé la personne concernée pourrait se retourner par la suite contre son partenaire contractuel en lui réclamant la part de la réparation correspondant à sa part de responsabilité dans le dommage.

405. *« Lorsqu'un responsable du traitement ou un sous-traitant a, conformément au paragraphe 4, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité*

[318] Règl. (UE) n° 2016/679, préc. art. 82 (3)..

[319] Règl. (UE). PE et Cons. UE 2016/679, préc. considérant 146.

dans le dommage, conformément aux conditions fixées au paragraphe 2. »[320]

406. Ce statut impose, à l'aune de la relation entre le responsable du traitement et du sous-traitant [321] à définir contractuellement *« leurs obligations respectives* » afin d'assurer le respect du règlement , notamment en ce qui concerne l'exercice des droits des personnes en attribuant, par exemple à l'un des coresponsables, la charge d'accomplir les obligations d'information et le cas échéant de recueil du consentement.

407. **De la relation entre le responsable du traitement et le sous-traitant**.

408. L'externalisation de la mise en œuvre d'un traitement de données à caractère personnel nécessite pour le responsable du traitement d'avoir recours aux services d'un ou plusieurs sous-traitants. Il peut s'agir de prestations d'hébergement de données de santé, de maintenance, de sécurité informatique, d'ingénierie en informatique, etc.

409. **Une harmonisation des obligations entre le sous-traitant et le responsable de traitement.** Nous remarquons que les définitions de « responsable du traitement » et de « sous-traitant » ne différent pas de la directive 95/46, 24 octobre 1995[322] au règlement 2016/679 du 27 avril 2016. De ce fait, à la différence du coresponsable, le sous-traitant est placé dans une relation de subordination. Le responsable du traitement est le commanditaire du traitement autrement dit, il en définit les moyens et objectifs c'est-à-dire les finalités. En qualité de donneur d'ordre, il contrôle la bonne réalisation des opérations de traitement, le respect de la réglementation ainsi que des normes professionnelles. En conséquence, le

[320] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 82 (5).

[321] Le règlement général sur la protection des données (RGPD) oblige tout responsable du traitement à désigner un sous-traitant, en signant avec ce dernier « un contrat ou un autre acte juridique [sous une forme écrite ou numérique] au titre du droit de l'Union ou du droit d'un État membre » Règl. (UE). PE et Cons. UE 2016/679, préc. art. 28 (3) et (9).

[322] Dir. (UE). PE et Cons. UE 1995/46, préc. art. 2 (e)..

sous-traitant agit pour le compte du responsable du traitement qui assume pour sa part la responsabilité de ce même traitement.

410. Toutefois, nous l'avons démontré précédemment, en ce qui concerne la responsabilité et les obligations du sous-traitant, le règlement innove. En raison des dispositions de l'article 82 du règlement relatif au droit à réparation et à la responsabilité, l'intérêt que représente la qualification de « sous-traitant » tend à disparaitre. Cette propension à l'harmonisation des obligations et responsabilités résulte de la volonté de garantir à la personne concernée par un traitement le respect de ses droits et l'indemnisation d'un éventuel préjudice résultant de leur méconnaissance, cela afin de faciliter la circulation des données au sein des États-membres de l'Union européenne dans le cadre du fonctionnement du marché intérieur.

411. Sans tenir compte de la liberté contractuelle par laquelle, le responsable de traitement, peux imposer un certain nombre d'obligations au sous-traitant notamment, au titre des dispositions de l'article 28 du règlement, le sous-traitant est le plus souvent placé dans une situation équivalente à celle du responsable du traitement. En effet, il est soumis, au même titre que celui-ci aux diverses obligations issues du règlement. De ce fait, au regard du principe d'*« accountability* », il doit être en mesure de rendre compte et d'expliquer, en toute transparence, à l'autorité de contrôle, les mesures qu'il met en œuvre afin de se conformer aux exigences issues du règlement. À ce titre, sur le fondement des dispositions du 2 de l'article30 du règlement il doit, à l'image du responsable du traitement, tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte de ce dernier. De la même manière le sous-traitant doit, en amont de tout contrôle, définir et mettre en œuvre les procédures nécessaires et ainsi faciliter l'exécution des opérations de contrôle de la Commission nationale avec laquelle il doit coopérer[323].

[323] Règl. (UE). PE et Cons. UE 2016/679, préc. considérant 31.

412. *« Chaque responsable du traitement et sous-traitant devrait être tenu de coopérer avec l'autorité de contrôle et de mettre ces registres à la disposition de celle-ci, sur demande, pour qu'ils servent au contrôle des opérations de traitement. »*[324]

413. Enfin, le sous-traitant doit, comme le responsable du traitement, coopérer avec l'autorité de contrôle dans le but de faciliter l'exécution des opérations de contrôle qu'elle réalise.

414. **Le sous-traitant concerné par la désignation d'un DPO.** Comme nous l'avons auparavant mentionné, eu égard aux dispositions de l'article 37 du règlement2016/679, le sous-traitant peut également se trouver dans l'obligation de désigner un délégué à la protection des données selon les mêmes termes que le responsable du traitement. Enfin, en ce qui concerne la sécurité du traitement, il est également dans l'obligation de mettre en œuvre, avec le responsable du traitement *« les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque »* en tenant compte *« des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques »*[325].

415. **Le sous-traitant soumis à un devoir de suppléance et d'information.** Corrélativement à la responsabilité conjointe, ces obligations analogues ont vocation à couvrir l'intégralité des risques pesant sur le traitement. Ainsi, si l'une des parties vient à manquer à ses obligations, les mesures mises en œuvre par l'autre partie permettent de pallier aux risques susceptibles de peser sur les données. Il s'agit surtout ici de faire assumer au sous-traitant la responsabilité de suppléer aux défaillances d'un responsable de traitement non consciencieux. Dans ce cadre, le sous-traitant est également tenu d'informer, immédiatement, le responsable du traitement si, selon lui, ses instructions constituent *« une*

[324] Règl. (UE). PE et Cons. UE 2016/679, préc. considérant 82.

[325] Règl. (UE). PE et Cons. 2016/679, préc. art. 38.

violation du règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données »[326].

416. **Le responsable de traitement seul responsable de l'effectivité des droits de la personne.** Toutefois, ces mesures concernent essentiellement la sécurité des données et la confidentialité des informations[327]. Ainsi, bien que le sous-traitant puisse, de sa propre initiative, nommer un délégué à la protection des données ou y être contraint du fait de la satisfaction des conditions de l'article 37 précitées, il appartient toujours au responsable du traitement, de mettre en œuvre une organisation, ainsi que des processus de nature à permettre à la personne d'exercer effectivement ses droits.

417. **Le sous-traitant confronté à une obligation de collaboration.** Cette affirmation doit être nuancée. En effet, en matière d'hébergement de données de santé le sous-traitant est tenu dans le cadre la procédure d'agrément, de transmettre les modèles de contrats et une présentation de sa politique de sécurité et de confidentialité. Il ressort des dispositions des articles R. 1111-3 et R. 1111-4 du Code de la santé publique que ces documents, doivent comporter les modalités de recueil du consentement de la personne concernée ainsi que, les conditions dans lesquelles sont présentées et prises en compte les éventuelles demandes de rectification des données hébergées et les moyens mis en œuvre pour assurer le respect des dispositions de l'article L. 1111-7 relatif à l'accès des personnes à leurs informations de santé, notamment en termes de délais et de modalités de consultation.

418. Pour autant, la loi de n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé substitue, en son article 204, 5° (c), à l'ancienne procédure d'agrément une procédure de certification. L'appréciation des conditions requises pour bénéficier de cette

---

[326] Règl. (UE). PE et Cons. 2016/679, préc. art. 28 (3).

[327] C. santé publ art. L. 1110-4 et L. 1111-8.

autorisation est réalisée par un organisme certificateur accrédité par le comité français de certification (Cofrac).

419. Cette évaluation est effectuée à partir du référentiel de certification Hébergeur de Données de Santé (HDS) élaboré et publié par l'Agence des systèmes d'information partagés de santé (ASIP Santé). Celui-ci comporte notamment comme prérequis spécifique au secteur santé, l'obligation, pour le candidat à la certification, de coopérer en ce qui concerne les droits de la personne. Cette coopération nécessite pour l'hébergeur de mettre en œuvre, conformément à la norme ISO/CEI 27018:2014[328], à laquelle le référentiel fait référence, des mesures de nature à permettre au responsable de traitement de respecter ses obligations vis-à-vis des personnes concernées par le traitement de leurs données à caractère personnel. Il s'agit en outre de permettre au responsable de traitement de pouvoir répondre positivement et dans les délais aux demandes de droit d'accès, de rectification et de suppression qui lui seraient adressées par un patient.

420. Il en résulte que le sous-traitant qui fournit un service d'hébergement de données de santé doit, à l'instar du responsable du traitement, déterminer les modalités d'exercice des droits de la personne pour le périmètre dont il a la maitrise. Cela peut, par exemple, consister en la définition de processus de réception de contrôle et de validation des demandes émanant du responsable du traitement ou de la personne concernée, en la mise à disposition de ressources humaines dédiées à la gestion de ces sollicitations ou en la création de comptes d'accès pour des membres de son personnel qui seraient chargés de gérer ces demandes d'accès. Celui-ci est soumis a minima à l'obligation de collaborer avec le

[328] Il s'agit d'une norme de bonnes pratiques pour la protection des données à caractère personnel et le respect de la vie privée dans les services de *Cloud Computing* (ou informatique en nuage.)..

responsable de traitement afin de lui permettre de répondre favorablement aux demandes de la personne concernée.

421. **Le sous-traitant gardien de la licéité du traitement**. Afin de garantir la protection des données à caractère personnel ainsi que le respect des droits de la personne, le règlement fait peser la responsabilité du contrôle de la licéité des traitements mis en œuvre par le responsable de traitement sur les épaules de son sous-traitant[329].

422. *« Le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre. »*[330]

423. Si le sous-traitant souhaite prouver que *« le fait qui a provoqué le dommage ne lui est nullement imputable »*[331] , il est important qu'il exige contractuellement du responsable de traitement, de rédiger et de documenter consciencieusement ses instructions. Le sous-traitant est ainsi encourager à signale formellement toute instruction qui lui semblerait illicite. *A contrario*, s'agissant d'obligations similaires, ce dernier serait confronté à la difficulté de démontrer que le manquement est imputable au responsable du traitement. Il pourrait également être tenu pour responsable, pour ne pas l'avoir alerté du caractère illicite de son instruction et, d'autre part, pour y avoir obéi. Cette lecture, est particulièrement défavorable aux prestataires d'hébergement de données de santé qui, en pratique, ne sont pas toujours en mesure de satisfaire cette obligation.

---

[329] Règl. (UE). PE et Cons. 2016/679, préc. art. 32 §4.

[330] Règl. (UE). PE et Cons. 2016/679, préc. art. 29.

[331] Règl. (UE). PE et Cons. 2016/679, préc. art. 82 (3).

B. Le Délégué à la protection des données, chef d'orchestre de la protection

424. L'obligation de désigner un délégué à la protection des données. Le Délégué à la protection des données (DPD) ou Data protection officer (DPO) est une évolution du Correspondant à la protection des données à caractère personnel plus connu sous l'appellation de Correspondant Informatique et Libertés (CIL) dont la fonction est définie dans le titre III aux articles 42 à 55 du décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

425. Le règlement prévoit la possibilité pour le(s) responsable(s) de traitement(s) et sous-traitant de désigner un DPD. Cependant, l'article 37 du règlement du 27 avril 2016 contraint sous certaines conditions les responsables de traitements ainsi que les sous-traitants à désigner un délégué à la protection des données ou DPD.

426. Ainsi, sont tenus en tout état de cause de désigner un DPD les responsables de traitements ou sous-traitants lorsque :

427. *« a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;*

428. *b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou*

429. *c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. »*

430. Le règlement ne définit pas ce qu'est une autorité ou un organisme public. Ainsi, il appartient aux États-membres de déterminer au moyen de leur législation nationale cette notion. Il ressort toutefois des travaux du G29 que les autorités ou organismes publics devraient comprendre les autorités nationales, régionales ou locales et, le cas échéant, d'autres organismes de droit public. Au vu de ces éléments, la Caisse nationale de l'assurance maladie des travailleurs salariés qui dans le cadre de ses activités traite des données à caractère personnel relatives à la santé serait dans l'obligation de désigner un DPD. En ce qui concerne les autres acteurs de santé, le règlement ne fait aucunement référence aux organismes de droit privé poursuivant une mission de service public, de ce fait, ceux-ci ne sont pas soumis à l'obligation de désigner un DPD sur ce fondement. Toutefois, les États-membres pourraient ultérieurement décider d'impliquer dans leur législation nationale ces organismes au même titre que les établissements de santé public.

431. Si nous considérons les autres dispositions de l'article 37, celles-ci décrivent deux cas comportant chacun trois conditions cumulatives. Ces deux cas partagent des conditions communes ainsi que des conditions particulières. Le premier critère commun à trait aux activités du responsable du traitement ou du sous-traitant. Ces activités, doivent être considérées comme les activités principales et non comme de simples activités auxiliaires, *« les activités de base d'un responsable du traitement ont trait à ses activités principales et ne concernent pas le traitement des données à caractère personnel en tant qu'activité auxiliaire »* [332] . Toutefois, le G29 sur la protection des données a adopté, lors de sa séance plénière des 12 et 13 décembre 2016, plusieurs lignes directrices permettant d'apprécier les dispositions de l'article 37, notamment en ce qui concerne l'obligation de procéder à la désignation d'un DPD[333]. Il

[332] Règl. (UE). PE et Cons. 2016/679, préc. considérant 97.

[333] Groupe de travail de l'article 29 (G29) sur la protection des données, *« Guidelines on Data Protection Officers ('DPOs') »*, adopté le 13 décembre 2016.

résulte de ces travaux que les activités indispensables à la réalisation des missions du responsable du traitement ou du sous-traitant doivent être considérées comme constituant des activités de base. En conséquence, il s'agit pour le responsable du traitement ainsi que pour le sous-traitant d'opérations clés qui sont nécessaires pour atteindre leurs objectifs, *« 'core activities' can be considered as the key operations necessary to achieve the controller's or processor's goals »*[334].

432. Au regard de ces éléments, l'on peut en déduire qu'un *« hôpital ne pourrait pas fournir des services médicaux sans risque et efficacement sans traiter des données de santé, comme les dossiers médicaux des patients. Par conséquent, on devrait considérer que le traitement de données de santé est une des activités principales de n'importe quel hôpital et les hôpitaux devraient donc désigner des DPO »*[335].

433. Le second critère commun concerne aux deux dernières situations décrites se rapporte à la dimension de ces activités. Celles-ci doivent nécessiter un suivi à grande échelle ou consister en un traitement à grande échelle. Le règlement 2016/679 ne précise aucun seuil et ne donne aucun élément d'appréciation afin de déterminer à quoi correspondent de tels traitements. Au regard des éléments dégagés par le G29, il convient de considérer différents critères. Ainsi, l'échelle examinée peut-être appréciée au regard du volume de données ou du nombre de personnes concernées. Il peut également s'agir de l'étendue géographique du traitement ou encore de sa durée.

434. Au regard de ces éléments, ne constitue par un traitement à grande échelle, le traitement mis en œuvre par un médecin et qui concernerait les données de ses patients. *A contrario*, le traitement de données de santé des patients d'un établissement de santé public ou privé réalisé dans le cadre de ses activités habituelles, constituerait un traitement à grande échelle

---

[334] *Ibid.*, p. 6.

[335] *Ibid.*, p. 60 (Traduit de l'anglais).

obligeant l'établissement ou le groupe à désigner un délégué à la protection des données.

435. En ce qui concerne les caractéristiques particulières de ces traitements à grande échelle, pour imposer la désignation d'un DPD, les opérations de traitement doivent soit exiger un suivi régulier et systématique, c'est-à-dire qu'elles doivent être réalisées de manière organisée et répétée le plus souvent à des intervalles particuliers et pour une période donnée, soit celles-ci doivent porter sur des catégories particulières de données personnelles et de données telles que les données relatives à la santé. Ainsi, les données collectées ou produites par les applications mobiles de bien-être, de m-santé ou par des dispositifs médicaux qui traitent également des données de localisation des personnes peuvent intégrer la liste des traitements obligeant les responsables et sous-traitants à désigner un délégué.

436. L'ensemble de ces critères étant cumulatifs, si les trois critères de l'un des deux cas décris sont remplis, alors le responsable du traitement et/ou le cas échéant le sous-traitant, devront désigner un DPD qui sera alors chargé de la conformité des traitements mis en œuvre par l'organisme.

437. Nous constatons, en ce qui concerne le ou les ensembles présentant une organisation formalisée décrites à l'article L. 1110-12, 3 du Code de la santé publique, qu'ils ne sont pas organisés autour d'une personne morale mais sur la collaboration de plusieurs personnes physiques et morales. Dans ce contexte, les décisions relatives aux modalités de traitements sont prises collégialement, par les différents acteurs et, le plus souvent avec le concours des représentants des Conseils départementaux et des chargés de missions des Agences régionales de santé. En conséquence, les traitements mis en œuvre par ces organisations, relèvent le plus souvent d'une coresponsabilité. Au-delà de la question de la création de structures ad hoc, il convient donc de s'interroger sur l'obligation pour chacun des coresponsables de désigner un sous-traitant

et, sur l'efficacité de la démarche qui consisterait à solliciter chacun de ces DPD des parties prenantes.

438. La désignation d'un DPD au sein des structures du secteur médico-social n'est également pas sans difficultés. Ces structures sont le plus souvent en cours d'informatisation et ne bénéficient pas de moyens financiers, matériels et humains suffisant[336].

439. Ainsi, pour ce secteur, le sujet est d'autant plus complexe que les questions relatives à la sécurité ne sont pas toujours incluses ou les ressources ne sont pas toujours impliquées dans les projets d'informatisation. Par ailleurs, les Établissements et services sociaux et médico-sociaux (ESMS), Groupements de coopération sociale ou médicosociale (GCSMS[337]), associations, etc. ne sont pas suffisamment dimensionnées ou acculturées pour bénéficier d'une politique de sécurité ainsi que de ressources humaines chargées de la sécurité des systèmes d'information (SSI).

440. Le DPD, incarnation de la conformité. La fonction de DPD est définie dans le RGPD 2016/679 du 27 avril 2016, principalement par le considérant 97 et par la section 4. Les articles 38 et 39 du règlement décrivent ses fonctions et missions.

441. Au regard de ces dispositions, la mission principale d'un délégué consiste à garantir la protection des données à caractère personnel en faisant en sorte que l'organisme qui a procédé à sa désignation soit en conformité avec la réglementation relative aux données à caractère personnel ainsi que les exigences sectorielles.

---

[336] C'est le constat réalisé par différentes Agences régionales de santé et notamment celle du Grand Est qui ont lancé différents appels à candidature et versé plusieurs subventions afin d'aider les établissements et services médico-sociaux (ESMS) à s'informatiser. Le dernier appel à candidatures pour la région Grand Est date du 19 juillet 2017. Il concernait les départements des Ardennes, de l'Aube, de la Marne, et de la Haute Marne.

[337] CASF, art. L. 312-7.

442. Cette fonction témoigne de l'esprit du règlement en ce qu'elle s'inscrit dans une logique consistant à doter les responsables de traitement et sous-traitants de moyens de nature à leur permettre de procéder à une autorégulation par la pratique.

443. De ce fait, l'objectif consistant à garantir un niveau de protection adéquat de la donnée à caractère personnel protégée est atteint au travers les missions du délégué. En raison de ses responsabilités, ce dernier est le gardien du respect de la règlementation relative à la protection des données au sein de l'organisme. Pour ce faire, il dispose de solides connaissances en droit, en technologies de l'information et en gestion de risques, afin de pouvoir interagir avec l'ensemble des interlocuteurs notamment les informaticiens et professionnels de la SSI. Il bénéficie, par ailleurs, de l'ensemble des informations nécessaires à l'accomplissement de ses fonctions et dispose des moyens humains, matériels et financiers adaptés.

444. Par souci de rendre efficace les mesures arbitrées par la direction générale et de garantir la protection des données, ses missions d'analyse, de conseil mais aussi de contrôle s'étendent aux sous-traitants prenant part aux traitements.

445. Dans le but de garantir son indépendance ainsi que l'effectivité de ses missions, le délégué n'a pas, dans l'exercice de ses fonctions, à recevoir ou donner aux autres acteurs des instructions impératives. De ce fait, il doit faire directement rapport au niveau le plus élevé de décision[338]. Au sein d'un établissement de santé, le DPD doit donc pouvoir s'adresser à la direction générale. Il doit travailler en étroite collaboration avec l'ensemble des acteurs accédant ou intervenant sur les données et porter conseil auprès des différentes directions métiers et, si cela s'avère nécessaire, auprès de la Direction générale. Ainsi, afin de pouvoir formuler des recommandations au responsable du traitement, il est obligatoirement consulté préalablement à toute modification substantielle d'un traitement

[338] Règl. (UE). PE et Cons. UE 2016/679, préc., art. 38 (3)..

en cours et, est pleinement associé à la conception de tout nouveau traitement.

446. Sous peine de sanctions, il veille en toute indépendance au respect des dispositions applicables, aux règles sectorielles mais aussi aux règles internes du responsable du traitement et, le cas échéant, du sous-traitant ainsi qu'au respect de la répartition des responsabilités entre les différents protagonistes.

447. Afin de garantir que l'organisme qui l'a désigné présente un niveau de maturité suffisant et afin d'impliquer l'ensemble des personnels dans la protection des données, le délégué exerce des missions d'information et de sensibilisation. En fonction de la taille et de l'organisation de l'organisme qui l'a désigné, il pilote et, le cas échéant, mène des actions destinées à former et sensibiliser les personnels et collaborateurs participant aux opérations de traitement ainsi qu'à la SSI de santé mais aussi les équipes de direction. Ces campagnes d'information et de sensibilisation consistent à vulgariser les notions et obligations incombant au responsable du traitement et sous-traitants mais aussi à diffuser les bonnes pratiques et concourent à l'implication de chacun. Elles contribuent à la conduite du changement en présentant les travaux de mise en conformité sous un angle positif et non comme de simples contraintes.

448. Dans le cadre de ses missions d'analyse, d'investigation, d'audit et de contrôle, le délégué met en œuvre de manière indépendante toutes les actions qui lui permettent d'apprécier le degré de conformité de l'organisme et ainsi de mettre en évidence d'éventuelles non-conformités à la réglementation, aux règles de bonne conduite ainsi qu'aux méthodes et procédure relatives à la protection des données à caractère personnel. Lorsque des irrégularités sont constatées, il en informe directement et de manière formalisée le responsable du traitement.

449. Le délégué à la protection des données est tenu auprès du responsable du traitement ou du sous-traitant à une mission de

responsabilisation et d'alerte. Ainsi, lorsqu'il est amené à constater, dans le cadre de ses fonctions, des risques concernant la sécurité des données et qui résulteraient du non-respect de ses recommandations, ou de mésusages, il en informe sans délai le responsable du traitement. De manière générale, malgré son rôle et ses responsabilités, le DPD n'est pas personnellement responsable de la non-conformité des traitements mis en œuvre par l'organisme qui l'a désigné. Le délégué ne fait qu'incarner la protection des données en formulant des recommandations et en veillant au respect de la réglementation ainsi que de la bonne application des méthodes, consignes et procédures à la définition desquelles il a participé. Toutefois, il appartient *in fine* à l'organisme, de prendre la responsabilité de mettre en œuvre un traitement respectueux des recommandations du DPD et du règlement.

450. Le délégué occupe également sur les questions relatives au traitement, une fonction de médiation entre la personne concernée ou encore l'autorité de contrôle et le responsable du traitement ou le sous-traitant. Dans ce cadre, vis-à-vis de la personne concernée, il veille au respect de ses droits. Ainsi, il reçoit les réclamations et plaintes adressées au responsable du traitement et met en œuvre les procédures adéquates afin d'y apporter une réponse appropriée.

451. De la même manière que le délégué à la protection des données joue un rôle de médiation entre la personne concernée et le responsable du traitement, il est l'interlocuteur privilégié de la CNIL sur les questions relatives aux traitements[339]. Dans ce but, il intervient lorsqu'il est nécessaire de procéder à une consultation préalable[340] de l'autorité de contrôle mais également lorsque l'organisme fait l'objet d'un contrôle. Afin d'être en mesure de démontrer que le responsable du traitement respecte les obligations découlant du règlement, le délégué constitue et

[339] Règl. (UE). PE et Cons. UE 2016/679, préc. art., article 39 (e).

[340] Règl. (UE). PE et Cons. UE 2016/679, préc. art., article 36.

maintient la documentation [341] des traitements de données à caractère personnel et s'assure que l'autorité de contrôle puisse en disposer[342].

452. Une ressource indépendante et préservée des conflits d'intérêts. Nous l'avons précédemment évoqué, la nomination d'un délégué à la protection des données n'est obligatoire que sous certaines conditions. Toutefois, eu égard aux responsabilités dévolues aux (co)responsables de traitements et aux sous-traitants et compte tenu des exigences et risques associés aux traitements de données à caractère personnel relatives à la santé, les organismes de soins et leurs prestataires informatique sont *de facto* dans l'obligation de désigner un DPD afin de s'assurer de la conformité des traitements qu'ils mettent en œuvre ou auxquels ils contribuent.

453. Qu'ils soient de droit public ou de droit privé ces organismes se trouvent confrontés, du fait du règlement général, à l'impératif ou à la nécessité de désigner un délégué chargé de personnifier la protection des données à caractère personnel. Qu'il s'agisse de petites organisations ou d'établissements guidés par un souci de réduction des dépenses, ils peuvent préférer à la création d'une nouvelle responsabilité l'alternative de confier cette activité à un prestataire, au moyen d'un contrat de services ou à un autre professionnel occupant déjà, en leur sein, des fonctions en lien avec les systèmes d'information ou la sécurité.

454. Cette dernière solution ne nous paraît pas nécessairement la plus appropriée. En effet, si le règlement permet au délégué à la protection des données d'exécuter d'autres missions et tâches, l'organisme qui souhaite désigner l'un des membres de son personnel doit toutefois veiller à ce que ses autres fonctions n'emportent pas de conflit d'intérêts[343]. Ainsi, le G29 a mis en évidence, au cours de ses travaux portant sur le statut du

[341] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 30 et 35.

[342] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 31.

[343] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 26 (3).)

délégué[344], que celui-ci doit pouvoir agir de manière indépendante par rapport à l'organisme qui l'a désigné. A ce titre, il doit, par exemple, être en capacité d Toute sembler avoir d'empêchement à ce qu'il occupe en sus de cette activité des fonctions de direction. Toutefois, cela pourrait le conduire à privilégier à la protection des données les intérêts propres à l'organisme notamment lorsque des arbitrages doivent être réalisés entre la nécessité de mettre en œuvre des mesures de sécurité complémentaires et la facilitation des accès en vue de favoriser l'activité. D'une manière générale, les autres fonctions occupées par le délégué ne doivent pas le conduire à influer sur les principaux critères de sécurité de l'information (disponibilité, intégrité, confidentialité et traçabilité) ou à participer à la détermination des finalités et des moyens d'un traitement de données à caractère personnel. Ainsi, le délégué ne peut, à titre d'exemple, occupé les fonctions de direction des ressources humaines (DRH), de direction des services informatiques (DSI) ou de direction administrative et financière (DAF).

455. Chez nos voisins Allemand, la *« Federal Data Protection Act »* promulguée le 14 janvier 2003 et modifiée par la loi du 14 août 2009[345] oblige, dès à présent, les organismes à désigner un délégué. Son statut est similaire à celui défini au sein du règlement. En effet, on retrouve dans les deux textes la volonté de garantir l'indépendance du délégué et de le préserver de toute contrainte et garantir ainsi l'effectivité de ses missions. Dans ce cadre, pour l'autorité de contrôle nationale allemande, la Bayerisches Landesamt für Datenschutzaufsicht, « autorité bavaroise de protection des données » ou « BayLDA »[346], les fonctions de directeur

[344] Groupe de travail de 29 (G29) sur la protection des données, *« Guidelines on Data Protection Officers ('DPOs') »*, Adopté le 13 décembre 2016.

[345] Federal Data Protection Act, 14 janv. 2003 (Federal Law Gazette I p. 66), modifié par l'art. 1 de l'Act of 14 August 2009 (Federal Law Gazette I p. 2814).)

[346] Voir notamment communiqué de presse du 20 octobre 2016 de l'Office d'Etat de Bavière pour le contrôle de la protection des données. Consultable à l'adresse suivante : https://www.lda.bayern.de/media/pm2016_08.pdf

informatique est de DPD étant distinctes et le délégué étant amené dans le cadre de ses missions, à apprécier les mesures, notamment techniques, mises en œuvre par le directeur informatique, cette indépendance aboutie à rejeter le cumul de ces fonctions afin d'éviter qu'il ne soit juge et partie.

456. DPD et RSSI une symbiose à concevoir. Les données des personnes prises en charge par les structures de soins, sont traitées au sein d'un système d'information dont la sécurité est confiée à plusieurs acteurs. Le délégué à la protection des données ne peut donc garantir à lui seul leur disponibilité et intégrité ainsi que le respect de la confidentialité.

457. Les missions du délégué se rapportent à la conformité des traitements de données à caractère personnel à la réglementation, à la sécurité des données et à la protection des droits des personnes concernées par le traitement. Le responsable de la sécurité des systèmes d'information (RSSI) quant à lui est un expert de la SSI. Ses tâches sont similaires à celles du délégué en ce qu'il a pour rôle, en sus de sa mission de SSI, d'assister, d'informer, de conseiller et d'alerter le responsable de traitement. Cependant, bien qu'il soit un expert dans son domaine et qu'il est des connaissances en droit, son cœur de métier demeure la sécurité logique et physique du système d'information dans son ensemble.

458. De prime abord, la fonction de RSSI peut sembler compatible avec celle de délégué. Toutefois, bien que ce dernier doive disposer de solides connaissances en sécurité et en systèmes d'information, la fonction de délégué dépasse le cadre d'une approche technique axée sur la maitrise du risque. Elle suppose également de solides connaissances de l'organisation, mais une véritable expertise en droit, des compétences en management, en conduite du changement etc.

459. Par ailleurs, dans l'éventualité où un organisme souhaiterait privilégier la promotion de compétences internes, il serait souhaitable qu'il se livre, au préalable, à une analyse afin de déterminer s'il existe des incompatibilités avec les responsabilités envisagées. En effet, le RSSI est,

le plus souvent, placé sous l'autorité de la direction des systèmes d'information ou encore de la direction des affaires financières. Ces organisations sont incompatibles avec la fonction de délégué à la protection des données qui, nous l'avons vu, nécessite des garanties d'indépendance et l'éviction de tout conflit d'intérêt. Il convient donc d'apprécier, au cas par cas si le RSSI est, de par ses compétences et du fait de l'organisation du responsable de traitement en capacité de revêtir le rôle de délégué.

460. Les fonctions de DPD et de RSSI ainsi que leurs rôles respectifs concernant la conformité des traitements de données à caractère personnel doivent donc être considérés comme étant complémentaires. En conséquence, lorsqu'il exerce au sein d'un établissement de santé, la mission principale du délégué consiste à travailler de concert avec le RSSI afin de faire évoluer les pratiques et organisations et de peser auprès des différentes instances, directions et membres du personnel le composant.

461. Afin de mener à bien leurs missions, le délégué et le RSSI doivent travailler chacun dans la limite de leur compétence au développement d'outils communs, notamment en matière d'analyse de risque. Ils doivent collaborer dans le développement de la Politique de Sécurité des Systèmes d'Information (PSSI) déclinée au sein d'une charte informatique en tenant compte de normes et méthodes professionnelles et dans le respect de la norme juridique. Le cas échéant travailler avec l'appui d'un qualiticien à la formalisation de recommandations en faveur d'une organisation repensée et respectueuse des droits de la personne et notamment de la protection de la vie privée et ainsi, soumettre leurs conseils à l'arbitrage de la direction générale.

462. De manière plus spécifique, le délégué et le RSSI doivent dialoguer avec la Direction des systèmes d'information (DSI) afin de mettre en œuvre de manière coordonnée des procédures conjointes

permettant une protection intégrée de la vie privée[347] et de la sécurité. Ces procédure et méthodes doivent consister en un paradigme à somme positive permettant de mettre fin à cette dichotomie désuète consistant à opposer les besoins et la stratégie de l'établissement et le respect des droits de la personne. Ainsi, leur rapprochement doit aboutir à la mise en œuvre, d'un système d'information garant, du respect des exigences résultant du règlement. Cela passe notamment par l'adoption au sein du pôle système d'information de méthode et processus visant à garantir le respect, par défaut, des exigences résultant du règlement lors du choix de solutions ou lors de leur conception.

463. Le délégué et le RSSI doivent également conseiller le directeur de l'information médicale dans la définition et la mise en œuvre de dispositions relatives à la protection des données médicales nominatives des patients afin de préserver la confidentialité de ces données. *« Ces dispositions concernent notamment l'étendue, les modalités d'attribution et de contrôle des autorisations d'accès ainsi que l'enregistrement des accès »*[348] et la traçabilité des actions menées sur ses données.

464. Ils doivent également intervenir auprès de la commission médicale d'établissement (CME), essentiellement à des fins de consultation ou d'information portant sur les modifications opérées dans le règlement intérieur ou au sein de la politique de SSI qui y est annexée. La CME peut être également consultée et informée par le RSSI et le DPD des modifications que la mise en conformité de l'organisme pourrait induire vis-à-vis de l'organisation de l'activité médicale notamment dans le cadre du processus de gestion de l'information et du recueil de consentement, les procédures de gestion des accès ou encore l'introduction de comptes individuels d'accès aux membres du personnel, etc.

[347] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 25.

[348] C. santé publ, art. R. 6113-6.

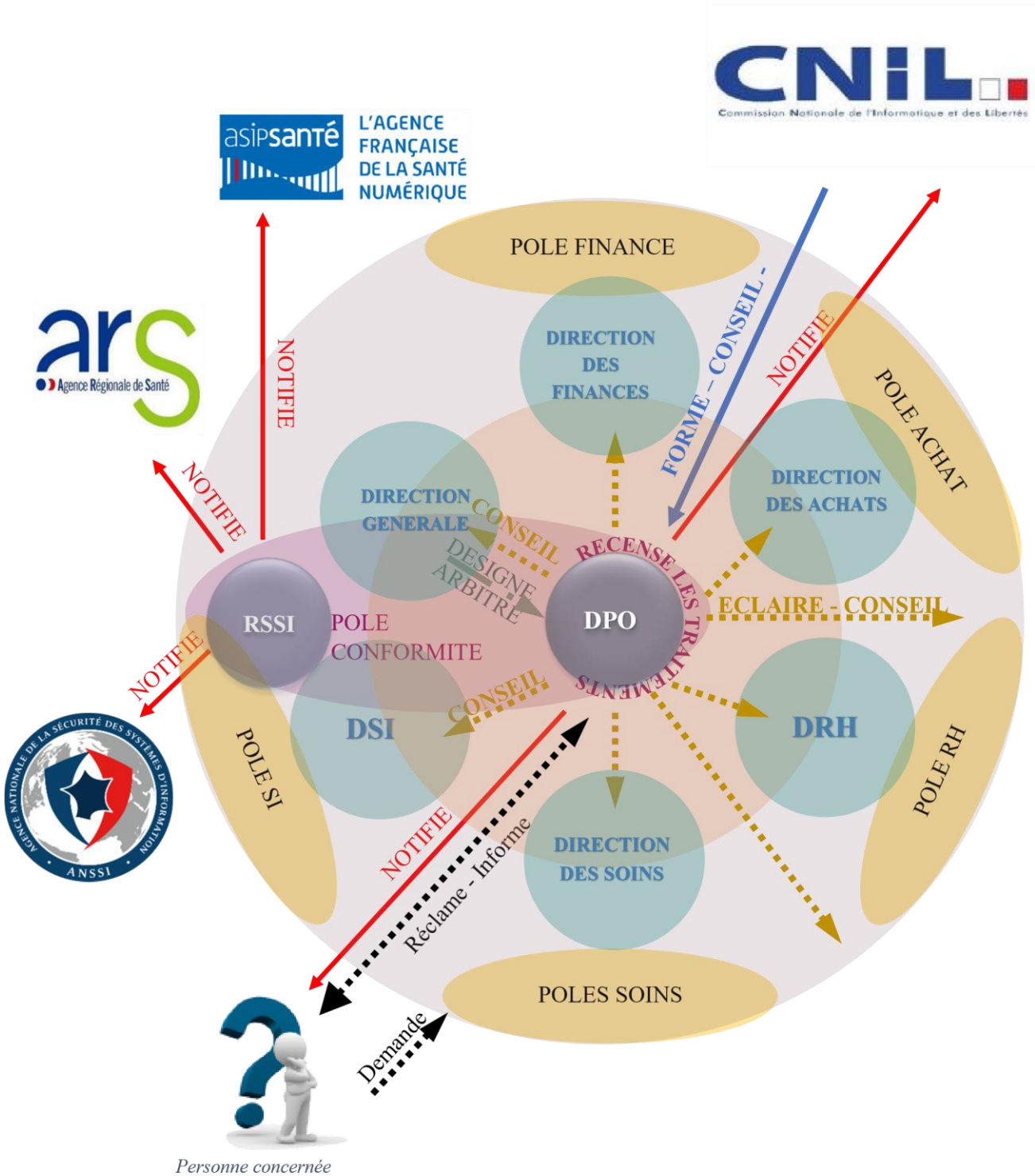
465. En ce qui concerne les activités de recherche menées au sein de l'établissement, le délégué à la protection des données ainsi que le RSSI peuvent également être amenés à intervenir auprès de la direction de la recherche.

466. Ainsi, le délégué peut assister et contrôler que les études ou évaluations qui impliquent ou non la personne humaine admettent, lorsque cela est nécessaire, l'existence de procédures d'information et de consentement et garantissent la confidentialité des données du patient. Pour chaque nouveau projet de recherche le délégué peut également accompagner les membres du pôle dans l'appréciation des critères fixés par les méthodologies de référence [349] et ainsi déterminer que les traitements qu'ils projettent de mettre en œuvre respectent parfaitement l'une de ces méthodologies. *A contrario*, le RSSI et le délégué peuvent, chacun dans leur domaine de compétence, les accompagner dans la constitution des dossiers de demande d'autorisation et d'avis selon les critères fixés par le Chapitre IX de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

467. Le RGPD impose donc aux établissements de travailler en amont sur la gouvernance de la conformité, sur une répartition des rôles et responsabilités entre les acteurs susceptibles d'intervenir quant aux traitements ou quant à leur conformité. S'il souhaite associer les fonctions de RSSI et de délégué ou simplement organiser leur collaboration, le responsable du traitement est donc dans l'obligation de procéder au préalable à une modification de son organisation, plus particulièrement en ce qui concerne les relations hiérarchiques, les fonctions dévolues au RSSI

[349] La CNIL a adopté des méthodologies de référence (MR 001, MR 002 ou encore MR 003) afin de simplifier les modalités déclaratives de traitements qui sont nécessaires à la conduite des recherches visées et encadrées par le Code de la santé publique. Dans ce cadre, elle a défini précisément la nature des données collectées et les modalités de conduite et d'analyse de ces études. Ainsi, les responsables de traitement qui souhaiteraient mettre en œuvre un traitement de données à caractère personnel relatives à la santé relevant de l'une de ces principales catégories de recherche peuvent dorénavant se limiter à la réalisation d'un engagement de conformité auprès de la CNIL.

au moyen de son contrat de travail afin de garantir l'indépendance du DPD et de le préserver de tout conflit d'intérêts.



Personne concernée

§ 2. La mise en œuvre de mesures de sécurité

469. **La sécurité et le risque.** « La sécurité » et « le risque » sont des vocables distincts mais ils constituent des notions conceptuelles de référence dans de nombreux domaines, tel que l'assurance, le droit, les systèmes d'information.

470. Malgré les distinctions entre ces différentes notions, les mesures de gestion du risque tendent aujourd'hui à les rapprocher, si bien que la maitrise du risque et la sécurité sont souvent confondus[350]. C'est en particulier le cas en matière de sécurité informatique ce rapprochement étant effectué au moyen de la gestion des risques qui prend donc la suite de la perspective plus générale de la sécurité des systèmes d'information. La notion de « sécurité » exprime l'utopie de la protection, la fiabilité au regard de multiples vulnérabilités existantes dans d'un domaine d'activité considéré *« d'un point de vue processuel, il est question de sécuriser »*[351] c'est-à-dire d'adopter une approche qui se situe entre la prévention et la maîtrise.

471. **La sécurité des systèmes d'information.** Directive de 2016 relative à la cyber-sécurité appelée directive sur la Sécurité des Réseaux Informatiques (SRI) ou encore directive NIS pour *« Network Information Security »* définie en son article 4 le concept de sécurité des systèmes d'information comme *« la capacité (…) des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité*[352]*, l'intégrité ou la confidentialité de*

[350] Y. PESQUEUX, *« Pesqueux. Sécurité, fiabilité et risque »*, 2015. Disponible à l'adresse suivante : https://halshs.archives-ouvertes.fr/halshs-01236503

[351] *Ibid.*

[352] L'authenticité repose sur les concepts d'imputabilité et de non-répudiation, elle nécessite l'identification et l'authentification des entités habilitées à réaliser une ou plusieurs actions sur le système ou la donnée. Elle permet ainsi la traçabilité des événements et ainsi l'établissement de la responsabilité d'une personne vis-à-vis d'un acte. Sans ces conditions, les éléments produits ne

données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles »[353].

472. La sécurité des systèmes d'information s'inscrit *« dans un cadre institutionnel évolutif mais déjà relativement structuré. Dès lors que le droit donne une définition circonstancielle de la sécurité, celui-ci intervient pour accompagner la définition et la mise en place des actions de sécurité. Bien entendu, le droit traite également des conséquences préjudiciables des sinistres notamment au titre de la recherche d'éventuelles responsabilités »*[354].

473. **Le risque un objet frontière.** En ce qui concerne la notion de risque[355] elle constitue un - objet frontière –[356]. Il s'agit en effet d'une notion de référence qui est utilisée dans plusieurs domaines d'activités sans pour autant recouvrir les mêmes « réalités ». Cette notion n'est pour autant pas disjonctive car elle conserve un sens commun quel que soit le champ d'activité considéré. Le risque est ainsi indéfini en lui-même. Il peut donc être apprécié au moyen d'une approche rationnelle et ainsi être envisagé de manière objective mais il peut également s'apprécié de

sauraient être fiables et ne pourraient ainsi que constituer un moyen de preuve contestable.

[353] Dir. (UE) PE et Cons. 2016/11481148, 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. En ce sens, se référer également au considérant 49 du RGPD

[354] A. TESSALONIKOS, A. BENSOUSSAN, « Bensoussan, *Risque informatique et sécurité juridique* », *Gaz. pal*., n° 128, 18 avril 2002, p. 12.

[355] Le risque peut être exprimé de la manière suivante : aléa * vulnérabilité.

[356] Il s'agit d'un objet et par analogie d'une notion *« suffisamment plastique pour s'adapter aux besoins locaux et aux contraintes des divers groupes qui l'utilisent, tout en étant suffisamment robuste pour maintenir une identité commune d'un site à l'autre »* (S. L. STAR, J. R. GRIESEMER, *« Griesemer. Institutionnal ecology, 'Translations' and Boundary objects: amateurs and professionals on Berkeley's museum of vertrebate zoology »*, Social Studies of Science, vol. 19, n° 3, 1989. p. 393)..

manière subjective, c'est-à-dire interprétative, et ainsi dépendre de la perception ou l'exposition de l'individu supportant le risque.

474. Quelle que soit l'approche adoptée, cette notion est associée à un phénomène négatif pouvant résulter d'un incident ou d'un acte à caractère malveillant. Cet évènement indésirable est le plus souvent envisagé comme étant susceptible de présenter un caractère irréversible. Ainsi il exprime la crainte de se retrouver dans l'incapacité de revenir à la situation initiale où le dispositif considéré, accomplis la fonction requise dans des conditions déterminées pendant une durée donnée[357]. De ce fait, le risque est considéré par les acteurs de la sécurité des systèmes d'information de manière rationnelle au moyen d'outils de diagnostic et d'audit. Ces outils sont construits à partir d'une codification des incidents préalablement identifiés et assortie d'une échelle de gravité et de mesures de corrections. Ces dispositifs permettent ainsi de considérer les risques à travers la mise en œuvre de procédures destinées à les maitriser, à les réduire à une variable acceptable. Par cette approche similaire, par bien des aspects, à l'approche déclinée en matière de qualité, on entrevoit un système organisé autour du principe de prévention du risque afin de tendre vers le « risque zéro » qui constitue un objectif ultime inatteignable en matière de sécurité des systèmes d'information.

475. Dans ce domaine, « le risque correspond à la probabilité plus ou moins grande de perte résultant d'une organisation inadéquate, d'un défaut de fonctionnement, ou d'une insuffisante sécurité du système d'information, entendu comme l'ensemble des équipements systèmes et réseaux et des moyens humains destinés au traitement de l'information de l'institution »[358].

---

[357] P-G. FONTOLLIET, *Systèmes de télécommunications*. Nouvelle édition, revue et augmentée. Vol. XVIII. Presses Polytechniques et Universitaires Romandes, 1996, p. 53.

[358] « Réflexion sur le risque informatique », *RGDA*, n° 4, 1er. 1 avril 2018, p. 6.

476. Ainsi, la notion de risque peut être synthétisée de la manière suivante : [risque = (Menace*vulnérabilité)/contre-mesure.] Notons que les risques informatiques peuvent être d'origine naturelle ou humaine, accidentelle ou intentionnelle.

477. **Le risque - en perpétuelle mutation**. « Il évolue au rythme des technologies des systèmes informatiques et électroniques, mais aussi des capacités techniques des individus et des organisations dédiées à la cyber-malveillance. »[359]

478. Cette impermanence du risque peut également être de nature à ne pas préserver la confiance des usagers et patients dans les systèmes d'information de santé. C'est pourquoi, elle nécessite que la réglementation soit agnostique de la technologie afin qu'elle puisse demeurer effective face aux nouveaux risques et ce, quel que soit le degré de maturité technologique. Cet agnosticisme était déjà présent au sein de la loi de 1978, ces modifications ne correspondant pas uniquement aux nouvelles technologies mais à l'évolution du regard de notre société vis-à-vis des droits de la personne, de sa vie privée et de la protection de ses données.

479. La sécurité sanitaire fait essentiellement référence au principe de précaution, en raison de l'existence d'une incertitude scientifique qui pèse sur la réalisation du dommage et de son caractère irréversible. En revanche, la sécurité des systèmes d'information de santé fait, quant à elle, référence au principe de prévention en raison du fait qu'il n'existe pas, en la matière, d'incertitude scientifique quant à l'existence d'un risque ou à la réalisation d'un dommage. En effet, dans ce domaine, les risques et éventuels dommages sont connus et leurs effets sont évalués ou évaluables.

480. En outre, dans le domaine de l'informatique, le dommage résultant d'une faute qu'il s'agisse d'une omission, d'une négligence ou

[359] Rédaction Lextenso, « Assurer le risque cyber : quels enjeux ? »,?, préc. p. 2.

que cette faute constitue un manquement, intentionnel, ne présente pas nécessairement un caractère irréversible vis-à-vis des droits de la personne, du système d'information ou, plus spécifiquement, de l'information elle-même.

481. Toutefois, à l'égard des patients et usagers, sa réalisation, voir sa probabilité, est susceptible d'entrainer une perte de confiance définitive vis-à-vis de l'outil numérique et du système de santé avec lequel il finit par se confondre. Cette perte de confiance se traduit par des comportements pouvant aller du maintien du silence à l'égard du professionnel de soins, à l'opposition à tout traitement de données. Ces postures sont préjudiciables à l'économie et au fonctionnement du système de santé mais aussi à la qualité de la prise en charge et des soins qui s'en trouvent dégradés. Qu'il s'agisse ou non d'un service public, les professionnels sont toutefois dans l'obligation d'assurer la continuité des soins. C'est à dire que les professionnels doivent s'efforcer de maintenir la prise en charge en manquant de moyens complets et fiables. *In fine*, cette situation amène, le plus souvent, les acteurs du soin à revenir à une prise en charge plus conventionnelle dans laquelle la confidentialité, la disponibilité, l'intégrité de l'information et la traçabilité des actions sont en définitive altérées par rapport à la dispensation de soins reposant sur l'utilisation de l'outil informatique.

482. *« Le droit fondamental à la protection de la santé doit être mis en œuvre par tous moyens disponibles au bénéfice de toute personne. Les professionnels, les établissements et réseaux de santé, les organismes d'assurance maladie ou tous autres organismes participant à la prévention et aux soins, et les autorités sanitaires contribuent, avec les usagers, à développer la prévention, garantir l'égal accès de chaque personne aux soins nécessités par son état de santé et assurer la continuité des soins et la meilleure sécurité sanitaire possible. »*[360]

[360] C. santé publ, art. L. 1110-1. Se référer également aux dispositions de l'art. R. 4127-47 *« Quelles que soient les circonstances, la continuité des soins aux malades doit*

483. Au regard de ce qui précède, l'obligation de SSI de santé résultant des dispositions des articles L. 1110-4-1 du Code de la santé publique, 32 paragraphe 1 du Règlement et 34 de la loi de 1978 modifiée par la loi du 20 juin 2018[361], peut, parfois, être considérée comme une déclinaison « moderne » du principe de secret professionnel. Assurément, c'est deux obligations constituent un moyen de prévention destiné à préserver la confiance dans un système de santé désormais fondé sur le partage d'information à des fins de soins, de prévention et subsidiairement de recherche. Toutefois, l'article 226-17 du Code pénal est d'une autre nature de celle de l'article 226-13 du Code pénal puisque les dispositions précitées renvoient aux mesures prescrites à l'article 34 de la loi relative à l'informatique, aux fichiers et aux libertés[362]. Celles-ci ne sont pas uniquement dédiées à la préservation de la confidentialité l'information mais concernent également la préservation de l'intégrité de l'information mais aussi de sa disponibilité[363]. Cette infraction d'omission constitue par ailleurs un délit plus sévèrement réprimé en raison de l'aggravation des conséquences dommageables pouvant résulter de l'utilisation de l'outil informatique. Elle est ainsi sanctionnée d'une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende au visa de l'article 226-17 du Code pénal.

être assurée. Hors le cas d'urgence et celui où il manquerait à ses devoirs d'humanité, un médecin a le droit de refuser ses soins pour des raisons professionnelles ou personnelles. S'il se dégage de sa mission, il doit alors en avertir le patient et transmettre au médecin désigné par celui-ci les informations utiles à la poursuite des soins. »

361 Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

362 Le terme est ici employé dans un sens commun, en ce sens que l'information ne doit pas être portée à la connaissance de personnes non autorisées et ce indépendamment du mode d'appropriation du contenu informationnel, que celui-ci résulte d'une divulgation ou d'un accès illicite.

363 L'art. 226-17 du Code pénal dontdonc la qualité rédactionnelle est, au regard du principe de légalité criminelle, discutable, renvoie renvoi aux dispositions de l'art. 34 de la loi de 1978 qui emploie le terme « notamment », ce qui laisse supposer que la non mise en œuvre des mesures prescrites à l'art. 34 comprend également la disponibilité de l'information.

484. Elle constitue toutefois un moyen de protection supplémentaire de l'information qui vient parfaire l'inventaire des infractions pénales permettant de protéger les atteintes à la vie privée, au secret ou aux systèmes de traitement automatisé de données.

485. De manière générale, on constate que le risque est les plus souvent assimilé à la notion de perte qu'à celle de probabilité et encore plus rarement au gain, à la bonne fortune. Toutefois, si nous adoptons une perception différente du risque et de sa gestion, notre analyse diverge. Dans la pratique entrepreneuriale, le risque est assimilé à l'essai, l'expérimentation, le fait d'éprouver. Ainsi il permet la mise en perspective des concepts de profits, et d'intérêt. Il peut prendre dans cette approche la forme d'un risque humain ou technique. Ainsi les risques sont définis, appréciés, scindés, catégorisés pour aboutir au concept de bénéfice-risque.

486. Dans cette acceptation, le bénéfice escompté peut être apprécié par rapport aux responsabilités susceptibles d'être engagées, au critère indemnitaire, aux autres conséquences telles que la perte en terme d'image, de considération, de probité, etc.

487. Afin d'apprécier plus finement le risque et de conserver ainsi une certaine souplesse quant à l'appréciation des risques et mesures correctives, les acteurs de la sécurité sont allé jusqu'à apprécier le degré de gravité du risque. Ils ont ainsi opéré une distinction entre « le risque avéré », pour lequel le responsable de la sécurité est en capacité de mesurer la probabilité de sa réalisation et d'en apprécier les conséquences, et le « risque potentiel » pour lequel le responsable de la sécurité ne peut définir la liste des conséquences susceptibles de se produire, ou n'est pas mesure de déterminer de probabilité de réalisation des conséquences préalablement identifiés.

488. Il en va ainsi de la gestion des risques liés à la sécurité de l'information [364] qui repose sur la mise en perspective de mesures de traitement de risques et des bénéfices potentiels attendus dans la perspective d'équilibrer les risques et les incitations. Il s'agit de maitriser et d'assumer activement l'occurrence des dangers futurs[365]. Cette seconde approche est essentiellement considérée dans le choix des mesures destinées au maintien et à la restauration de la sécurité des systèmes.

489. Ainsi, le RGPD et la loi Informatique et Libertés modifiées n'imposent pas la mise en œuvre de mesures spécifiques de sécurité des systèmes d'information afin de gérer les risques pesant sur le système d'information et les données. Elles prescrivent de simples recommandations mais laisse le soin au responsable de traitement de déterminer les mesures à prendre.

490. Les dispositions de la loi et du Règlement opèrent, en conséquence, une distinction. Ainsi, le RGPD reprend les principes et droits fondamentaux antérieurement reconnus par la Directive. Ces principes et droits demeurent intangibles et doivent être assurément respectés. Ils ne peuvent faire l'objet d'aucune inflexion. D'autre part, le Règlement développe les dispositions relatives à la gestion des risques, y compris sur la vie privée des personnes concernées. Par ces nouvelles dispositions, le Règlement octroie, compte tenu de la nature des risques, de leur capacité à évoluer ainsi que de l'obsolescence des technologies, une relative souplesse aux responsables de traitements mais aussi aux sous-traitants. Cette capacité de gestion leur permet de déterminer en fonction de la nature, la gravité et la des risques encourus les mesures techniques, organisationnelles mais aussi juridiques appropriées [366] qui

[364] Se référer désormais à la norme ISO/IEC 27005:2018 anciennement ISO/CEI 27005:2011.2011 publiée au cours du mois de juillet 2018

[365] Il s'agit, en l'espèce, d'une matérialisation du principe de l'aléa.

[366] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 5 (1) (f).

doivent être mises en œuvre pour protéger le système ainsi que les données à caractère personnel relatives à la santé.

491. Pour autant, s'ils ne souhaitent pas voir leur responsabilité engagée, les responsables de traitements doivent tenir compte, lorsqu'ils se livrent à cette appréciation, *« de l'état des connaissances, des coûts de mise en œuvre et de la nature et de la portée, du contexte et des finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes »*[367] concernées.

492. *« Les hommes, en règle générale, répugnent à assumer des risques*[368]*, car, à leurs yeux, l'utilité marginale des dollars qu'ils gagnent est inférieure à celle des dollars qu'ils perdent (…). Par suite, les activités économiques qui comportent beaucoup d'incertitudes et de grands risques assumés par les personnes qui s'y consacrent doivent obligatoirement, sous l'influence des arrivées et des départs, déterminés par la concurrence, des porteurs de risques, assurer à ces derniers, à long terme, un profit, en tant que prime positive destinée à neutraliser leur aversion normale pour le risque. »*[369]

493. Cette appréciation des risques et des mesures, devant être mises en œuvre pour parvenir à un niveau de sécurité approprié à l'information traitée s'avère être difficile. En effet, du fait de la combinaison de l'instabilité et de l'inflation législative, les responsables de traitement et experts en sécurité arrivent, difficultueusement, à suivre l'état de l'art. *In fine*, c'est la qualité de la loi et son effectivité même qui sont en cause. Celles-ci ont également une incidence sur l'effectivité et la qualité des référentiels et normes professionnelles ainsi que sur leur opposabilité.

---

[367] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 32.

[368] P. A. SAMUELSON, L'Economique, tome II, Armand Colin, Paris, 1973, p. 355.

[369] *Ibid.*

494. En ce sens, C. Zorn conclue, à propos des dispositions de la loi du 4 mars 2002 et des référentiels relatifs à l'hébergement des données de santé, que *« les textes se sont ainsi multipliés négligeant la nécessaire clarté que l'environnement technique impose. La précipitation dans leur rédaction contrastant avec la lenteur de publication de référentiels très attendus, le contexte juridique est devenu extrêmement compliqué pour les acteurs du monde de la santé en général, comme pour les juristes »*[370].

495. Sécurité des systèmes d'information de santé et état de l'art. Depuis les années 2000 on constate une forte inflation normative qui témoigne d'une emprise croissante de l'État sur l'ensemble de notre société[371]. La France comptait ainsi, à la fin de l'année 2010, deux-mille-seize lois, six-cents ordonnances, vingt-six mille cent quatre-vingt-dix-huit décrets et cinquante-huit codes[372]. Avec les normes communautaires, la densification de l'arsenal juridique s'est poursuivie, on décomptait ainsi en 2009, en plus des nombres précités, sept-mille quatre-cents traités et dix-sept mille textes communautaires[373]. Les textes sur lesquels repose la stratégie de sécurisation des systèmes d'information en santé se sont également multipliés, ces dernières années[374].

496. *« On assiste à la multiplication de textes dans le domaine des systèmes d'information en santé. C'est en réalité la qualité de ces textes qui est en cause. Ces "bouts de loi" à la rédaction*

---

[370] C. ZORN, *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé*, avant-propos B. Py, préf. I. de Lamberterie, PUN, 2010, p. 254-255, n° 292.

[371] Conseil d'Etat, Rapport public 2006 – Jurisprudence et avis de 2005 – Sécurité juridique et complexité du droit, Paris, La Documentation française, 2006, p. 84.

[372] Secrétariat général du gouvernement, Loi et règlements en vigueur, *A*pproche statistique, janvier 2011, p. 2.

[373] Voir notamment F. ROUVILLOIS, *Libertés fondamentales*, Flammarion, coll. « Champs Université », 2e éd., 2016 ; M. GAY, F. CROTTA, *Les dessous des affaires judiciaires*, Max Milo éditions, coll. Essais-documents, document »,2014 ; G. ADREANI, R. BISMUTH, *Méthodologie de la recherche documentaire juridique*, Larcier, coll. Paradigme, 2014.

[374] Gaz. Pal. 22 janv. 2008, n° GP20080122003. p. 10

hasardeuse ne sont pas neutres vis-à-vis de leur environnement juridique global. Tel les dominos, chaque modification, aussi anodine puisse-t-elle paraître, provoque des répercussions qui peuvent être profondes. »[375]

497. Ce phénomène de prolifération des normes n'a donc pas épargné le domaine de la technique et de la SSI. En effet, l'interpénétration de la technique et du droit à, dans un premier temps, contribuée à alimenter l'instabilité de la règle de droit et à poursuivre ainsi ce phénomène de dégradation de la qualité des normes juridiques. De ce fait, la multiplication des sources et normes professionnelles, des recommandations techniques, des méthodologies professionnelles ont aboutie à l'accroissement du nombre de textes nationaux et communautaires. *« Des textes se sont ainsi multipliés négligeant la nécessaire clarté que l'environnement technique impose. »*[376]

[375] C. ZORN, *op. cit*. p. 284

[376] *Ibid*., p. 209. *Ibid*., p. 209. *Ibid*., p. 209.

498.

499. Schéma : Représentation non exhaustive de l'inflation normative

500. Cette situation est favorable à la multiplication des « conflits verticaux » entre normes de valeurs ou d'ordres juridiques différents, ainsi que des « conflits horizontaux » entre normes de même valeur et d'une manière générale nuit à l'intelligibilité du droit. Bien qu'en raison du caractère moniste de notre système juridique, un conflit vertical puisse être résolu aisément, ce pluralisme de sources et de textes fait qu'une même problématique peut accepter des réponses différentes selon la règle de droit considérée. Il existe des antinomies entre les dispositions de ces normes, contradictions substantielles qui résident dans le contenu des normes, il faut alors déterminer laquelle est applicable. Aussi, connaître et savoir interpréter les nombreuses normes des différents domaines du droit des systèmes d'information et des différents ordres (national, européen et international) pour déterminer comment elles doivent être appliquées et interprétés n'est pas à la portée des néophytes. Il est donc difficile même pour des experts du droit et de la sécurité de conserver des repères dans cet environnement normatif.

501. Toutefois, depuis 2016, la prise en compte des normes professionnelles a également contribuée à la limitation de cette prolifération. Ainsi, les normes techniques et professionnelles ont complétées voir se sont, pour partie, substituées aux normes juridiques nationales, les dispositions législatives n'y faisant qu'une simple référence et laissant le soin à des normes de valeur inférieure d'en préciser les conditions.

502. Elles sont désormais considérées par le droit comme un moyen de mise en œuvre ou de garantie du respect de la norme juridique et des droits et libertés de la personne concernée par le traitement de ses données. De ce fait, ces règles qui constituent l'état de l'art ont rapidement atténuées la

frontière entre le droit souple, encore appelé « droit flou »[377] ou *soft law*[378] et les normes impératives en se trouvant imposées progressivement par des dispositions législatives et réglementaires.

503. En ce sens, la loi de modernisation de notre système de santé[379] a reconnu aux référentiels de sécurité et d'interopérabilité[380], une assise législative unique au sein du Code de la santé publique au moyen de l'article L. 1110-4-1.

504. *« Afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, les professionnels de santé, 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 par le groupement d'intérêt public mentionné à l'article L. 1111-24. Ces référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés. »*[381]

---

[377] J. LEONHARD, Etude sur la pornographie pénalement prohibée, Thèse, Nancy, 2011, p. 60.

[378] Les normes constituant la soft law peuvent être considérées comme des recommandations, « *bien souvent, ces normes sont prises précisément pour éviter une quelconque « sanction » juridictionnelle, et leur caractère non obligatoire suppose qu'elles échappent à tout contrôle. Comment en effet sanctionner un comportement à l'aune d'une norme qui n'impose pas d'agir dans un sens déterminé ? »* (B. LAVERGNE, *Recherche sur la soft law en droit public français*, Thèse, Toulouse, 2011, p. 309)

[379] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

[380] Référentiel introduit par la Loi n° 2009-879 du 21 juillet 2009 dite loi HPST, dont l'élaboration a été confiée à l'Asip Santé par les dispositions de l'article L. 1111-8 alinéa 4 du Code de la santé publique...)...

[381] C. santé publ, art. L. 1110-4-1.

505. Figurent parmi ces documents de la Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) les référentiels techniques d'identification des acteurs sanitaires et médico-sociaux, d'authentification des acteurs de santé, le référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé ainsi que le référentiel d'imputabilité[382]. Leur élaboration résulte de la collaboration de l'Agence des systèmes d'information partagés de santé (ASIP Santé), de la délégation à la stratégie des systèmes d'information en santé (DSSIS) [383] et du fonctionnaire de la sécurité des systèmes d'information[384].

506. La PGSSI-S appartient à une série de politiques de sécurité des systèmes d'information dont la politique générale de sécurité des systèmes d'information de l'État (PGSSI-E)[385]. Cette politique définie les règles de protection applicables aux systèmes d'information des administrations de l'État composées des différents ministères et des établissements publics sous leur tutelle, des services déconcentrés de l'État ainsi que des autorités administratives indépendantes comme la CNIL[386]. Celle-ci fait l'objet

[382] Aujourd'hui, ces référentiels sont au nombre de quatre. Ils sont constitués du référentiel d'identification des acteurs sanitaires et médico-sociaux, du référentiel d'authentification des acteurs de santé, du référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé, du référentiel d'imputabilité. Les différents guides et référentiels élaborés par l'ASIP Santé sont disponibles à l'adresse suivante : http://esante.gouv.fr/services.

[383] La DSSIS est une délégation qui a pour objet de « favoriser le développement des usages des technologies numériques (…) dans l'ensemble du champ sanitaire et médico-social, afin d'optimiser la prise en charge des patients et d'améliorer la qualité des soins. » Placée sous l'autorité du secrétariat général du ministère chargé des affaires sociales (SGMAS), elle s'appuie, dans le cadre de ses missions de pilotage et de coordination des orientations nationales de la e-santé sur l'Asip Santé. Voir notamment : http://solidarites-sante.gouv.fr

[384] Le fonctionnaire de la sécurité des systèmes d'information (FSSI) est nommé par le Haut fonctionnaire de défense et de sécurité (HFDS) qui est lui-même nommé par le Ministre des Solidarités et de la Santé : C. défense, art. R. 1143-1. Le FSSI assiste le HFDS dans ses missions et participe à l'élaboration de la réglementation ministérielle et le contrôle de son application.

[385] La PGSSI-E a été élaborée par l'ANSSI et portée par la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014, elle est entrée en vigueur le 29 août 2014.

[386] PGSSI-E, art. 2.

d'une déclinaison propre aux ministères chargés des affaires sociales (MCAS) au moyen du politique de sécurité dédiée approuvée en 2015[387]. Ainsi, la politique de sécurité consacrée aux systèmes d'information de santé ne constitue pas une exception aux dispositions des autres politiques avec lesquelles elle demeure en cohérence. Elle peut simplement être assimilée à l'application de dispositions spécifiques relatives aux systèmes d'information (SI) utilisés dans le champ sanitaire et médico-social et traitant des données relatives à la santé que celles-ci soient à caractère personnel ou qu'elles soient anonymes.

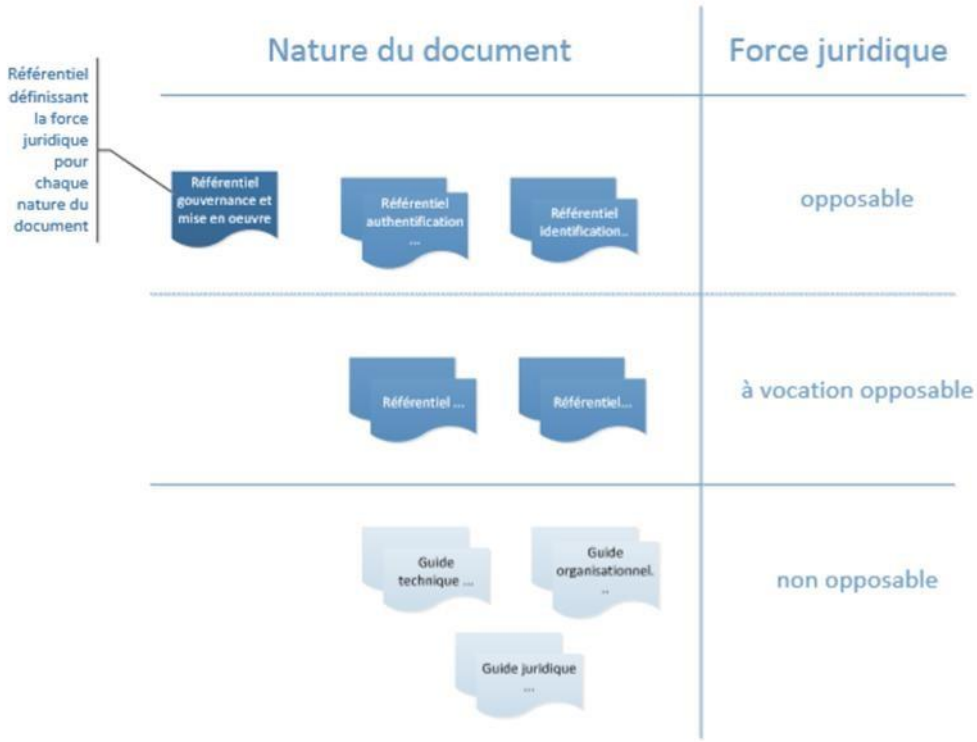
507. Elle constitue *de facto* une codification des règles de l'art et des usages qui, lorsqu'ils sont « approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés » [388] et publiés au Journal Officiel (JORF) deviennent *de jure* opposables. C'est-à-dire qu'ils acquièrent force obligatoire et ainsi disposent d'une valeur, non plus simplement déclarative mais contraignante, permettant aux justiciables de s'en prévaloir. C'est référentiels ne font pas tous, à ce jour, l'objet d'un arrêté et il reste à espérer que cette formalité sera, à l'avenir, plus aisément réalisée.

508. L'ASIP Santé a élaboré, en complément de ces référentiels, différents guides relatifs à la sécurité des systèmes d'information de santé qui, bien qu'ils n'aient pas force obligatoire, ne sont pas dépourvus d'effet juridique[389].

[387] Arrêté du 1er octobre 2015 portant approbation de la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales.

[388] C. santé publ, art. L. 1110-4-1.

[389] Voir notamment S. ROZENFELDRozenfeld, *« La donnée au* cœur *de l'e-santé », R*evue Expertises des systèmes d'information, 1er1 déc. 2016, p. 405.



510.

511. *Figure 5: Force juridique des documents*[390]

512. Ces guides, *« face aux nouvelles situations suscitées par le développement des technologies appliquées à la santé, constituent une réponse à la volatilité et la vélocité des nouvelles technologies »*[391]. Ils permettent, de par leur caractère non contraignant, de diffuser les bonnes pratiques et ainsi de favoriser leur application par les acteurs de la santé et du numérique. Ces pratiques constituent un standard de référence auquel peuvent avoir recours les Directeurs (DSI) et responsables de la sécurité des systèmes d'information de santé (RSSI) ainsi que les autres acteurs du monde de la santé afin de déterminer les conditions d'application et de mise en œuvre des différents référentiels. À l'aune de l'analyse réalisée par les juges concernant l'application, par les professionnels de santé, des

[390] Référentiel de gouvernance et de mise en œuvre de la PGSSI-S, 15 février 2017, p. 9.

[391] PGSSI-S, disponible à l'adresse suivante : http://esante.gouv.fr/

recommandations de bonnes pratiques de la HAS, le juge va se référer, le cas échéant, aux rapports d'expertise et par ce moyen appréhender les différentes sources, guides et référentiels[392]. Ainsi, il va pouvoir apprécier le respect de ces préconisations non contraignantes et, le cas échéant, retenir la responsabilité des professionnels (hébergeurs de données de santé, direction d'établissement ou de structure, professionnels de santé libéraux, etc.) si leurs comportements s'en écartent.

513. Le RGPD apporte également quelques précisions en la matière. Il énonce ainsi aux considérants 39, 78, 81, 83, aux articles 30 et 32 à 34 de sa section 2 ainsi qu'au sein de ses articles 40 et 47 des indications quant aux mesures organisationnelles, techniques et juridiques qui sont attendues du responsable de traitements en matière de sécurité. Ces dispositions ne sont circonscrites qu'aux grands principes gouvernant la sécurité des systèmes d'information. En effet, le Règlement n'édicte pas de mesures de sécurité de nature impératives. Elles ont pour principale vertu d'être pédagogiques en permettant de porter à la connaissance des responsables de traitements et sous-traitant non aguerris les moyens dont ils disposent pour assurer la sécurité des traitements qu'ils mettent en œuvre et garantie ainsi les biens essentiels[393] mais aussi les droits des personnes concernées par le traitement de leurs données à caractère personnel.

514. Il ne s'agit pas de se livrer à un « inventaire » à la Prévert mais d'observer que le responsable de traitements ainsi que le sous-traitant se trouvent également dans l'obligation d'adopter « *des mesures techniques et organisationnelles appropriées* »[394], « *de manière à garantir une sécurité et une confidentialité appropriées, y compris pour prévenir*

[392] Le juge qui ne dispose pas d'éléments suffisants pour statuer peut commettre, sur le fondement de l'art. 232 du Code de procédure civile, *« toute personne de son choix pour l'éclairer par des constatations, par une consultation ou par une expertise sur une question de fait qui requiert les lumières d'un technicien* ».»

[393] La notion de bien essentiel est définie au sein de la norme ISO 27001 et de la méthodologie EBIOS comme une information ou un processus jugé comme important pour l'organisme.

[394] Règl. (UE). PE et Cons. 2016/679, préc. considérant 78.

l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement »[395].

515. Les mesures prises doivent être de nature à assurer « un niveau de sécurité approprié, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger »[396].

516. Ces mesures peuvent, lorsque cela est nécessaire consister en la pseudonymisation des données. Elles peuvent également consister en l'introduction de clauses dans les contrats et marchés publics afin d'imposer aux prestataires et sous-traitants, la fourniture de services et produits conformes aux normes de sécurité, de protection des données par défaut et des droits de la personne dès leur conception.

517. Ces clauses peuvent prendre la forme d'incitations à l'égard des fabricants de produits, des prestataires de services et des producteurs d'applications afin que ces derniers prennent en compte *« le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications » compte tenu de l'état des connaissances »*[397].

518. Il peut également s'agir de règles internes qui peuvent être des règles d'entreprise contraignantes notamment appelées *Binding Corporate Rules* (BCR) afin d'uniformiser les pratiques relatives à la protection des données personnelles, de prévenir les risques, de communiquer sur sa politique d'entreprise en matière de protection des données à caractère

[395] Règl. (UE). PE et Cons. 2016/679, préc. considérant 39.

[396] Règl. (UE). PE et Cons. 2016/679, préc. considérant 83.

[397] Règl. (UE). PE et Cons. 2016/679, préc. considérant 78.

personnel auprès des membres des personnels, des sous-traitants, clients et partenaires mais surtout de la personne concernée par le traitement de ses données. Il peut également s'agir de l'application par un sous-traitant *« d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir à démontrer le respect des obligations incombant au responsable du traitement* », la conclusion de contrats spécifiques entre les responsables de traitement et les sous-traitants définissant les modalités du traitement et « *tenant compte des tâches et responsabilités spécifiques du sous-traitant dans le cadre du traitement à effectuer et du risque pour les droits et libertés de la personne concernée* ».

519. La CNIL dans l'exercice de ses missions, s'assure 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 »*[398].

520. En mai, juin et juillet 2018, la CNIL, s'est livrée à une appréciation des mesures de sécurité mises en œuvre par trois responsables de traitements afin de déterminer si celles-ci étaient conforme à l'état de l'art. Pour chacun des traitements de données examinées, la CNIL a considéré que ceux-ci avaient manqué aux obligations leur incombant au visa de l'article 34 de la loi relative à l'information, aux fichiers et aux libertés, modifiée.

521. Dans le premier cas d'espèce, des données sensibles constituées d'informations relatives à la correction ophtalmologique ainsi que du numéro d'inscription au répertoire de clients de la société Optical center avaient été rendus librement accessibles sur internet. La formation restreinte de la Commission a rappelé, à cette occasion, que de manière générale, l'exposition de ressources sans contrôle d'accès préalable, est identifiée depuis de nombreuses années comme faisant partie des failles de sécurité devant faire l'objet d'une surveillance particulière et doit, en

[398] *Ibid.*

conséquence, faire l'objet de vérifications notamment dans le cadre d'audits de sécurité.

522. Après constatation et instruction, la formation restreinte de la CNIL a relevé que les mesures élémentaires de sécurité, *« correspondant à l'état de l'art »* n'avaient pas été mises en place en amont de la mise en production d'une nouvelle fonctionnalité.

523. Elle a rappelé à cette occasion, que s'agissant d'informations relevant de la vie privée des personnes et, au regard de leur nature particulière, ces données auraient dû faire l'objet de garanties de sécurité renforcées indépendamment du volume de données concernées. Ainsi eu regard de la nature sensible des données traitées, elle a considéré, que la société aurait du « mettre en œuvre des moyens propres à assurer la sécurité des données à caractère personnel […] afin que ces données ne soient pas accessibles à des tiers non autorisés »[399].

524. La Commission a ainsi condamnée la société sur le fondement de l'article 34 de la loi du 6 janvier 1978 modifiée à une sanction pécuniaire d'un montant de deux cent cinquante mille euros d'amende.

525. Dans une autre décision du 24 juillet 2018[400], la Commission a été amenée à connaitre de faits relatifs à un incident de sécurité résultant d'une attaque en plusieurs étapes menée par « des délinquants informatiques chevronnés » au terme d'une démarche coordonnée sur plusieurs mois. Cette attaque a conduit au détournement d'un compte d'administration en vue de la propagation de l'intrusion vers les données et ce, sans que les auteurs ne puissent être identifiés.

[399] CNIL, délib., 7 mai 2018, n° SAN-2018-002, prononçant une sanction pécuniaire à l'encontre de la société OPTICAL CENTER.

[400] CNIL, délib. 24 juill. 2018, n° SAN-2018-008 prononçant une sanction pécuniaire à l'encontre de la société DAILYMOTION.

526. La société arguait qu'eu égard à la sophistication de l'attaque, l'atteinte à la confidentialité ne résultait pas de l'insuffisance des mesures qu'elle aurait prises en matière de sécurité. La formation restreinte a considéré que l'article 34 précité mettait à la charge du responsable de traitement l'obligation de mettre en œuvre des moyens propres à assurer la sécurité des données à caractère personnel contenues dans son système d'information, notamment afin que ces données ne soient pas accessibles à des tiers non autorisés.

527. *In casu*, le mot de passe du compte d'un compte de service était présent au sein du code source afin de simuler un administrateur dans le but de tester les fonctionnalités d'administration. La formation restreinte s'est livrée *de facto* à une appréciation de la technique employée au regard de l'état de l'art et a estimé que celle-ci était conforme. Elle a toutefois précisé qu'en matière d'authentification, il était important de veiller à ce qu'un mot de passe ne soit pas divulgué et par conséquent, qu'il ne soit pas stocké dans un fichier qui ne serait pas protégé. Elle a rappelé à cette occasion que s'il est admissible, pour le bon déroulement de tests relatifs au compte de service, le mot de passe associé à ce compte pouvait être inscrit, en clair, dans le code source, cette circonstance ne saurait toutefois, justifier, la présence constante du mot de passe dans le code source.

528. Elle a ainsi analysé le procédé employé pour en déduire que l'utilisation de cette méthode n'était pas de nature à permettre la sécurisation de la connexion distante et, à juste titre, a considéré que cette précaution élémentaire indispensable à la préservation de l'intégrité du réseau n'était pas remplie.

529. Si la formation restreinte admet, dans sa délibération, que la réussite de l'attaque résulte bien de la conjonction de plusieurs facteurs dont certains ne sont pas imputables à la société, elle considère toutefois que celle-ci a fait preuve de négligence en retenant que cette attaque n'aurait pas pu aboutie si des mesures appropriées avait été prises par la société.

530. Ce qui est intéressant dans ce cas d'espèce c'est que la société a soulevé que l'article 34 de la loi Informatique et Libertés était lacunaire s'agissant du type de mesures à prendre par le responsable de traitement et qu'il méconnaissait ainsi le principe de légalité des délits et des peines qui impose de définir, dans des termes suffisamment clairs et précis, les éléments constitutifs d'une infraction.

531. À cette occasion, la formation restreinte a rappelé que le législateur a confié au responsable de traitement le choix des mesures précises à mettre en place pour respecter l'obligation générale tirée de l'article 34 précité. En conséquence, le texte n'est pas prescriptif quant aux mesures à déployer pour garantir la sécurité d'un traitement, tant que l'obligation est, *in fine*, respectée. Elle confirme ainsi, le moyen de droit invoqué mais n'en tire pas les conclusions nécessaires en considérant qu'il s'agissait de la volonté du législateur de laisser au responsable de traitement la liberté de déterminer compte tenu des risques et de la nature des données, les mesures appropriées. Elle se situe sur une obligation de résultat dont l'objet et mixte puisque cette obligation porte sur les moyens mis en œuvre mais aussi sur la réalisation de l'atteinte.

532. Il convient donc de s'interroger sur le fait que l'obligation de sécurité serait devenue une obligation de résultat.

533. Par ailleurs, nonobstant les catégories de données concernées, la formation restreinte relève que la société n'apporte aucun élément permettant de minimiser significativement le nombre de 82,5 millions d'adresses électroniques. Elle estime donc que le volume de données impactées par la violation est considérable.

534. Dans la dernière affaire[401], la CNIL a été alertée de l'existence d'un défaut de sécurité permettant d'accéder aux documents officiels, dans leur intégralité, tels que *« des justificatifs d'identité (passeports, titres de*

[401] CNIL, délib. 21 juin 2018, n° SAN-2018-003 prononçant une sanction pécuniaire à l'encontre de l'Association pour le Développement des Foyers.

séjour et cartes d'identité), des bulletins de salaire, des avis d'imposition ou encore des attestations de paiement de la Caisse d'allocations familiales » de bénéficiaires de l'association pour le Développement des Foyers. En outre, ces documents contenaient *« une multitude de données d'identification des utilisateurs du site web telles que des noms, prénoms, dates de naissance, coordonnées postales, numéro d'inscription au répertoire national d'identification des personnes physiques ou IBAN »*[402].

535. En application de la décision n° 2017-147C de la Présidente de la Commission du 12 juin 2017, une délégation de la CNIL a procédé à une mission de contrôle en ligne le 15 juin suivant sur les traitements mis en œuvre par l'association. Le procès-verbal de constat n°2017-147/1 dressé à l'issue de cette mission, a été adressé à l'association par courrier électronique (courriel) et par courrier le 20 juin 2017.

536. Au cours d'une opération de contrôle en ligne[403], la délégation a constaté qu'une modification du chemin de l'URL affichée dans le navigateur permettait d'accéder aux documents enregistrés par d'autres demandeurs.

537. *« La formation restreinte rappelle en outre que, de manière générale, l'exposition de données à caractère personnel sans contrôle d'accès préalable, est identifiée comme faisant partie des failles de sécurité pour lesquelles une surveillance particulière s'impose et doit, en conséquence, faire l'objet de vérifications notamment dans le cadre d'audits de sécurité. À cet égard, la formation restreinte souligne l'importance de procéder à un protocole complet de test en amont de la mise en production d'un site internet. Il apparaît également que l'association n'a pas*

[402] Certaines des informations accessibles relevaient de la vie privée dès lors que les documents permettaient de connaître « le salaire des personnes, leur revenu fiscal de référence, leur statut marital ou leur nombre d'enfants et de savoir si elles percevaient l'aide personnalisée au logement »..

[403] Ces opérations sont menées en application de la décision n° 2017-147C de la Présidente de la Commission du 12 juin 2017.

procédé, après le déploiement des sites internet, aux vérifications régulières qui lui incombaient quant aux mesures de sécurité mises en place. »

538. La formation restreinte a prononcé une sanction pécuniaire d'un montant de soixante-quinze mille euros. La Commission a, par ailleurs, fait preuve d'une particulière sévérité en rendant publique ses décisions[404] au motif que compte de la nature des données en cause et du *« caractère particulièrement sensible de certaines de ces données, et au regard du contexte actuel dans lequel se multiplient les incidents de sécurité, il était nécessaire de sensibiliser les responsables de traitement mais aussi les personnes concernées, quant aux risques pesant sur la sécurité de leurs données ».*

539. Au regard de la délibération du 24 juillet 2018 nous sommes amené à nous interroger sur la nature de l'obligation de sécurité pesant sur le responsable de traitement et du sous-traitant. S'agit-il d'une obligation de résultat, d'une obligation de moyen renforcé ou d'une simple obligation de moyen ?

540. Dans sa décision de 2014, la formation restreinte avait rappelé qu' »*il est constant que l'obligation de notifier une violation de données, obligation de résultat à laquelle la société a satisfait, est distincte de celle relative à la sécurité et la confidentialité des données, obligation de moyens dont la formation restreinte doit examiner le respect ».* Nous en conviendrons, il serait absurde de considérer que la sécurité et plus particulièrement la sécurité des systèmes d'information doit être soumise à une obligation de résultat. Garantir l'infaillibilité de mesures de sécurité

[404] La CNIL a, depuis 2010, eu particulièrement recours à la possibilité qui lui était faite de rendre publiques les sanctions qu'elle avait prononcées. Elle l'a fait à l'égard de la société ACADOMIA, toujours au motif de la gravité des manquements constatés, voir en ce sens CNIL, délib. 22 avr. 2010 n° 2010-113 ainsi que le communiqué de la Commission concernant l'avertissement adressé à la société ACADOMIA pour des commentaires excessifs dans ses fichiers, 27 mai 2010.

relève de l'utopie et nécessiterait des mesures de protection rendant tout système inexploitable. Aucune technologie, aucune organisation ne permet de garantir un tel niveau de fiabilité contre des attaques externes ou internes ou contre les erreurs humaines résultant des utilisateurs du système.

541. Pour autant, s'il peut paraître déraisonnable de considérer que la sécurité des systèmes d'information soit soumise à une obligation de résultat, cette obligation peut, au fur et à mesure des avancées technologiques et de la maturation des organisations, s'analyser en une obligation de moyen non plus simple mais renforcée.

542. Ce qui nous interpelle dans la décision du 24 juillet 2018, ce sont les similitudes avec l'affaire jugé par la Commission en 2014. En effet, cette décision s'inscrit dans la droite ligne de celle rendue par la CNIL en date du 7 août 2014 [405].

543. Toutefois, contrairement à l'affaire concernant la société Orange, dans l'affaire Dailymotion, la CNIL intervient suite à un fait intentionnel, puisque une attaque a été menée afin d'accéder aux données des clients. Comme pour toute obligation de moyen, la CNIL recherche, dans un premier temps, la faute de la société. La formation restreinte reconnait, par ailleurs, le niveau de complexité avéré de l'attaque menée depuis le territoire des États-Unis d'Amérique. Elle apprécie, si la société Dailymotion a respecté les usages professionnels en réalisant des audits de sécurité de son système.

544. Contrairement à la délibération de 2014, la formation restreinte ne peut, en l'espèce, retenir un manquement du responsable de traitement à ses obligations en raison de l'absence de réalisation d'audits de sécurité

[405] CNIL, délib. 7 août 2014, n° 2014-298 prononçant un avertissement à l'encontre de la société X.

puisque celui-ci procédait, tous les trimestres à des audits afin d'améliorer la sécurité des traitements.

545. Cependant, afin de retenir la responsabilité de la société, elle se fonde sur l'obligation de non divulgation des moyens d'authentification dans le système.

546. Ainsi, la Commission n'infirme pas le moyen soulevé par la partie défenderesse selon lequel, la présence du mot de passe dans le code source n'est pas contraire à l'état de l'art. Afin de retenir la responsabilité de la société, la formation restreinte tempère cette allégation en énonçant qu' *« il est impératif qu'il ne soit pas stocké [constamment] dans un fichier qui ne serait pas protégé ».* Elle retient ainsi qu'il revenait au responsable de traitement *« de chercher une autre solution afin de ne pas le rendre accessible, par exemple, en le stockant au sein de son réseau interne et en s'assurant qu'il était injecté en temps réel dans le code source, uniquement lors des phases de test puis supprimé une fois le test achevé ».*

547. *« S'il était nécessaire, pour le bon déroulement de tests relatifs au compte de service, que le mot de passe associé à ce compte soit inscrit en clair dans le code source, cette circonstance ne saurait toutefois, justifier, selon la formation restreinte, la présence constante du mot de passe dans le code source. Dans la mesure où il était impossible pour la société de conserver le mot de passe dans le code source sous une forme hachée, il lui revenait de chercher une autre solution afin de ne pas le rendre accessible. »*[406]

548. De ce fait, si jusqu'à présent la Commission a pu démontrer des négligences dans les mesures de sécurité mises en œuvre pour retenir la responsabilité de responsables de traitements et/ou de sous-traitant, cette

[406] CNIL, délib., 24 juil. 2018, n° SAN-2018-008 prononçant une sanction pécuniaire à l'encontre de la société DAILYMOTION.

preuve nous semble désormais malaisée. Ainsi, bien que la Commission respecte les dispositions de l'article 34 et recherche une faute ou une négligence, elle ne justifie pas en quoi, les normes professionnelles prises pour référence, constituent l'état de l'art. A cet égard, cette analyse nous semble contestable. Ainsi, compte tenu de la qualité rédactionnelle de l'article 34 de la loi de 1978 modifiée, et de l'absence de prescription concernant les « précautions utiles », les décisions de la formation restreinte tendent progressivement à attribuer à l'obligation de sécurité les traits d'une obligation de moyen renforcée.

549. En effet, l'article été rédigé en des termes imprécis concernant non pas le comportement réprimé mais les mesures susceptibles d'être mises en œuvre. Cette indétermination volontaire a pour principale motivation de permettre l'adaptabilité des mesures aux technologies, méthodologies existantes ainsi qu'aux organisations des responsables. Elle a également pour finalité d'éviter une uniformisation des techniques de sécurisation qui serait, comme cela est reconnu unanimement en matière de sécurité, un non-sens, compte tenu du fait que ces dispositifs sont susceptibles de comporter des failles reproductibles.

550. Comme nous l'avons précisé dans nos précédents développements, on entrevoit, à travers l'approche de la CNIL une analyse orientée vers le « risque zéro », qui constitue un objectif inatteignable pour les responsables de traitements et sous-traitants. Cette analyse est d'autant plus vraie que la formation restreinte se montre beaucoup plus exigeante « au regard de la nature des données et des risques présentés par le traitement »[407].

551. *In fine*, bien que la faute ne soit pas présumée et que le responsable de traitements puisse apporter la preuve contraire, il est

[407] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. art. 21, 4.

raisonnable de considérer que la position de la CNIL rend la tâche laborieuse.

552. *De facto*, l'absence de précision concernant les mesures prescrites peut être source d'insécurité juridique et dénaturer *in fine* cette simple obligation de moyen en une obligation renforcée voir une obligation de résultat ne nécessitant plus la preuve d'une négligence ou d'une faute mais simplement l'existence de l'attaque ou du mésusage et de son dommage.

553. Les recommandations émises par la Commission et, dans le domaine de la santé, les guides et recommandations référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24 du Code de la santé publique ne définissent, hormis quelques exceptions, que de grands principes. Les pratiques professionnelles les plus répandues ne peuvent, par ailleurs, permettre d'atteindre systématiquement le niveau d'exigence attendu par la CNIL.

554. Ainsi, il convient de s'interroger sur la notion d'état de l'art. Celle-ci repose-t-elle sur l'appréciation de la Commission et sur la jurisprudence ou sur les pratiques professionnelles les plus rependues en matière de système d'information et de sécurité ?

555. *De facto, l'absence* de précision, au sein de l'article 34 concernant les mesures prescrites et l'analyse stricte de la formation restreinte peuvent être perçues comme faisant peser sur les responsables de traitements et les sous-traitants une obligation de moyen renforcée et dans une certaine mesure une obligation de résultat concernant la protection des données.

556. En ce sens, les dispositions du RGPD et de son article 32 opèrent un changement de paradigme, en substituant au dispositif de recensement et de contrôle des traitements un système essentiellement responsable et

autonome. Ce système fondé sur l'analyse de risque[408] consiste en son appréciation et en la mise en œuvre de mesures techniques, organisationnelles et juridiques appropriées afin de traiter celui-ci de manière adéquate et pour protéger les données.

557. *« 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.* »[409]

558. Au regard de ces dispositions, peu de doute subsiste quant à la nature de l'obligation pesant sur le responsable de traitements et le sous-traitant. Il convient toutefois de s'interroger sur la prise en compte ultérieure de ces différents critères, par la formation restreinte de la Commission dans son appréciation des diligences accomplies par les acteurs du traitement.

[408] L'art. 35 du Règlement général sur la protection des données (RGPD) impose désormais la conduite d'une analyse d'impact sur la vie privée, ou analyse d'impact relative à la protection des données lorsqu'un traitement de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

[409] Règl. (UE). PE et Cons. UE 2016/679, art. 32.

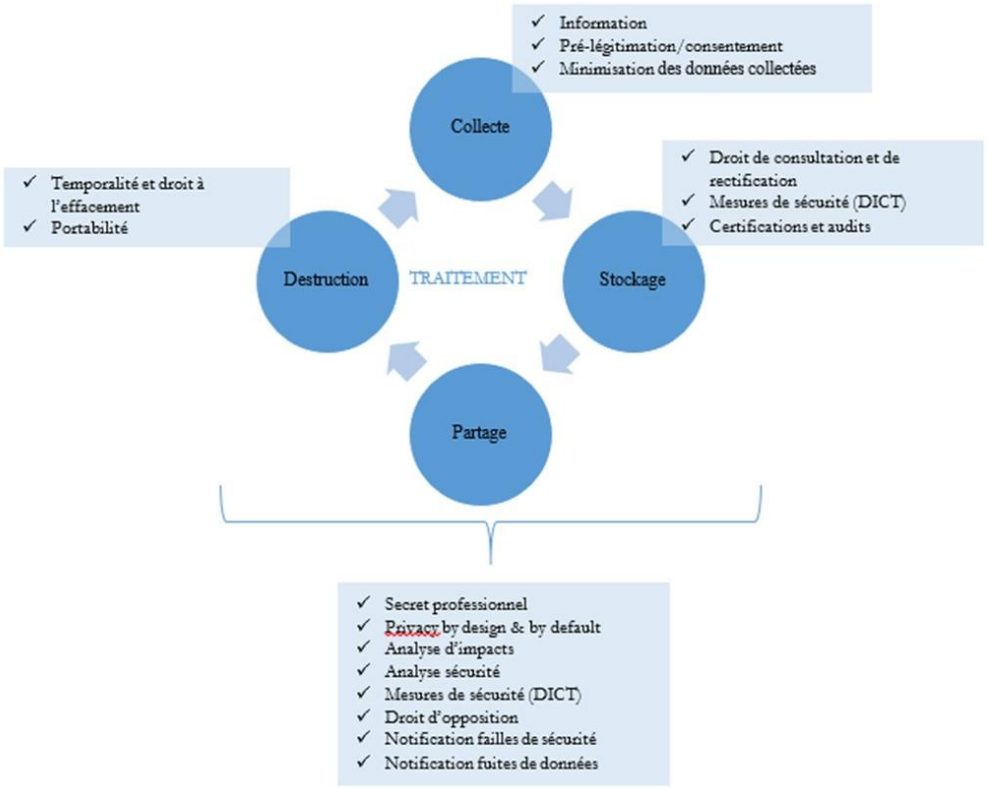


Schéma : Représentation non exhaustive des mesures de sécurité

559. Au regard de ce qui précède, une simple erreur d'appréciation ou une négligence suffirait à déterminer que les conditions de mise en œuvre du traitement ne respectent pas le niveau d'exigence attendue. En conséquence, la simple constatation d'une atteinte à la confidentialité de l'information, à sa disponibilité ou à l'intégrité de la donnée à caractère personnel et à la traçabilité des actions matérialiserait l'inadéquation des mesures mises en œuvre par le responsable de traitements ou le sous-traitant. Face à la généralité de l'obligation imposée, il convient également de s'interroger sur la prise en compte du caractère directe ou indirecte de la négligence dans la réalisation du dommage et de considérer toute cyberattaque extérieure sophistiquée et malveillante comme un fait exonératoire dans l'éventualité d'une causalité indirecte.

CONCLUSION DU CHAPITRE 1

561. **Une protection à organiser.** La notion de coresponsabilité permet de répondre à la réalité des conditions de mises en œuvre des traitements de données de santé. Elle constitue une réponse aux nouvelles formes d'organisations du secteur. Toutefois la sécurité des données repose sur la définition des rôles et responsabilités des différents acteurs intervenant dans le traitement de la donnée de santé. Il est donc indispensable que le rôle et les responsabilités des acteurs intervenant dans la mise en œuvre d'un traitement soient définis en amont et, pour des considérations probatoires, formalisées au sein de contrat en amont. Cette formalisation et nécessaire pour garantir l'effectivité des droits de la personne. A défaut la responsabilité solidaire des acteurs devrait être engagée.

562. **La personnalisation de la sécurité et de la conformité.** La sécurité et la conformité des systèmes d'information de santé nécessitent l'intervention d'un délégué à la protection des données. En raison de la complexité des traitements et des compétences qui doivent être mobilisées par le délégué. Il devrait pouvoir exercer ses fonctions au sein d'une équipe dédiée composée, lorsque ces ressources sont disponibles, d'un responsable sécurité des systèmes d'information, et d'un qualiticien. La mission de délégué à la protection des données suppose la connaissance du cadre juridique dans lequel l'activité du responsable du traitement est exercée. Ainsi le délégué à la protection des données devrait pouvoir s'appuyer sur une ressource juridique. Compte tenu de ses missions, du délégué, il devrait être placé dans une relation fonctionnelle directe avec le représentant du responsable du traitement et bénéficier d'une protection équivalente à celle reconnue aux délégués du personnel.

CHAPITRE 2. UNE UTILISATION CONTROLEE

564. **Un changement de paradigme.** La loi relative à l'informatique, aux fichiers et aux libertés, imposait au responsable de traitement, préalablement à la mise en œuvre d'un traitement de données de santé, d'obtenir des services de la Commission nationale de l'informatique et libertés une autorisation. A cette occasion, la Commission se livrait à un contrôle de conformité. Le Règlement général à la protection des données opère un changement de paradigme en substituant à une logique de contrôle a priori une responsabilisation des acteurs et un contrôle *a posteriori* des modalités de mises en œuvre des traitements. Concernant les traitements les plus sensibles, le Règlement conserve toutefois à la charge des responsables de traitement des obligations déclarative.

565. Ce changement d'approche reposant essentiellement sur la réalisation d'études d'impacts sur la vie privée, la Commission ne dispose plus que d'une connaissance partielle des traitements mis en œuvre. Au regard des nouvelles obligations pesant sur le responsable de traitement, la CNIL dont les pouvoirs de contrôle *a priori* sont minimisés (Section 1) se voit désormais doter de véritables pouvoirs de contrôles, *a posteriori,* (Section 2).

Section 1. Une minimisation du contrôle a priori

567. Sous l'empire de la loi de 1978, les traitements portant sur des données à caractère personnel devaient être préalablement déclaré, aux services de la Commission nationale de l'informatique et des libertés. La catégorie de procédure préalable relevait d'un critère organique. La loi du 6 août 2004 transposant dans l'ordre juridique français les dispositions de la directive de 1995 à modifier ce critère afin de s'attacher à l'objet des traitements et aux risques qu'ils représentent pour la personne concernée. Le RGPD ainsi que la loi du 20 juin 2018 modifiant la loi relative à l'informatique, aux fichiers et aux libertés ont supprimés le système de contrôle préalable. Elle conserve toute fois le système de la déclaration préalable pour ce qui concerne les traitements de données personnelles du secteur de la santé présentant une finalité d'intérêt public ou les demandes d'autorisation de recherche en santé n'impliquant pas la personne humaine. Cette minimisation du contrôle a priori, opéré par la CNIL, est de nature à conduire à un risque d'ineffectivité de la protection (Paragraphe 1) qui doit être compensé par un renforcement du dialogue entre la Commission et les responsables de traitement (Paragraphe 2).

§ 1. Un risque d'ineffectivité de la protection

569. **Un réel besoin de conserver des mesures de contrôle *a priori.*** Quelques soient les contremesures prévues par le règlement, la disparition des formalités préalables, entraine une perte de contrôle du traitement *a priori*.(A) Compte tenu de la nature protéiforme des atteintes aux droits et libertés de la personne et de l'ampleur du préjudice pouvant résulté de la circulation non maitrisée de données à caractère personnel relatives à la santé, une approche fondée exclusivement sur la responsabilisation et le contrôle a posteriori est insuffisante voir inefficace. Le maintien d'opérations de contrôle *a priori* semble indispensable (B).

A. La disparition de déclarations préalables

570. Les données sensibles parce qu'elles font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou parce qu'elles sont relatives à la santé ou à la vie sexuelle de celles-ci, voient leur traitement interdit. Les traitements qui portent sur des données génétiques, biométriques, pénales, ou qui comportent des appréciations sur les difficultés sociales des personnes, sont également soumis au même régime. Cependant, certains fichiers portant sur ces données particulièrement sensibles peuvent faire l'objet d'une pré-légitimation textuelle. Ainsi, si la finalité du traitement l'exige « la règle générale veut ensuite que le recueil des données sensibles ne soit possible qu'à la condition que l'individu donne son "consentement exprès", sauf certains cas où le consentement est insuffisant à permettre le traitement. Cependant, la loi prévoit un certain nombre de situations où le recueil du consentement de la personne n'est pas nécessaire, ce qui aménage

largement les possibilités de traitements de données de santé pour des finalités très diverses »[410.]

571. Au regard de l'étendue des traitements susceptibles d'être mis en œuvre et des risques qu'ils sont susceptibles de constituer pour les droits et libertés de la personne, ces conditions sont nécessaires mais ne sont pas suffisantes pour que le traitement de données de santé soit licite. Il doit également faire l'objet d'un contrôle préalable par la Commission. En effet, la réglementation du traitement de données à caractère personnel relatives à la santé qu'elles soient directement ou indirectement identifiantes a vocation à assurer le respect des droits et libertés individuelles de la personne concernée tels que le droit au respect de la vie privée. Jusqu'à l'entrée en vigueur du RGPD, cet objectif est garanti par la mise en œuvre de mesures de contrôle préalable afin de vérifier que le traitement soit licite et que les modalités de sa mise en œuvre ne portent pas atteinte à ces droits et libertés.

572. Des suites de la transposition de la directive de 1995 par la loi du 6 août 2004, il résulte des dispositions des articles 25, 26 et 27 que la loi relative à l'informatique, aux fichiers et aux libertés, a abandonné l'ancienne distinction opérée entre les fichiers du secteur public qu' étaient soumis à un régime d'autorisation après avis e de la CNIL et les fichiers du secteur privé soumis à un simple régime de déclaration. Ainsi, c'est désormais la finalité du traitement et la nature des données collectées qui déterminent le régime applicable au traitement. Il existe donc principalement deux régimes distincts de formalités préalables. Le régime de la déclaration pour les données les plus courantes et le régime des autorisations concernant les données les plus sensibles comprenant, en raison des dispositions de l'article 8 de la loi de 1978, les données relatives

[410] C. ZORN, *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé*, avant-propos B. Py, préf. I. de Lamberterie, PUN, 2010, p. 226, n° 255.

à la santé[411]. En effet, ces traitements de données à caractère personnel représentant un risque particulier d'atteinte aux droits et libertés de la personne, une autorisation de la Commission est un préalable indispensable.

573. Toutefois, du fait de la transformation de notre environnement technologique et face au caractère évolutif des nouveaux traitements de données, ce système de déclaration préalable ne permet plus aux responsables de traitements de respecter leurs obligations. De ce fait, la réglementation ne peut plus reposer sur un système de déclaration préalable mais sur une adaptabilité en temps réel de la protection afin de garantir aux responsables de traitements le respect de leurs obligations et aux personnes concernées une protection optimale de leurs données.

574. Nous assistons depuis les dix dernières années à une interpénétration entre la technique et le droit. Le RGPD en adaptant notre réglementation à la réalité technologique en constitue l'actuelle synthèse. Au moyen des dispositions de son article 36, le règlement met fin à une forme de contrôle a priori des traitements tout en préservant et en renforçant le contrôle a posteriori. Il substitue aux formalités préalables un système de mise en conformité permanente censé garantir à tout moment une protection maximale des données.

575. Par ailleurs, cette évolution s'inscrit dans une philosophie générale qui imprègne le règlement et qui est fondée sur la responsabilisation des acteurs du traitement de données à caractère personnel. Ainsi à propos de la personne concernée, cette responsabilisation se décline désormais autour du principe d'autodétermination informationnelle. Bien que la Commission ait été initialement peu encline à l'utilisation du consentement comme seule

[411] N. ETIEN-GNOAN, L'encadrement juridique de la gestion électronique des données médicales, Thèse, Lille, 2014, p. 44.

justification du traitement de données sensible[412], le règlement confère désormais au consentement de la personne concernée par le traitement, une place particulière. Il confie à la personne l'appréciation des risques susceptibles de résulter d'un traitement de ses données de santé, le consentement devient donc l'un des principaux instruments de la maîtrise de ses données.

576. Concernant le responsable de traitements, le règlement l'oblige à apprécier les risques sur la protection des données en se plaçant du point de vue des personnes concernées par le traitement dont il projette la mise en œuvre. Il implique pour le responsable de traitements, qu'il détermine les mesures qu'il estime approprier pour réduire les risques identifiés et si des risques résiduels persistent, il l'incite à prendre lui-même l'initiative de consulter l'autorité de contrôle.

577. Le règlement opère par conséquent un transfert de la charge de l'appréciation préalable des risques de la Commission vers les responsables de traitements et les personnes concernées. Il ne supprime, toutefois, pas toute forme de contrôle mais privilégie une approche a posteriori en renforçant les pouvoirs de la CNIL notamment en ce qui concerne les sanctions qu'elle et en mesure de prononcer.

578. Quelques soient les contremesures prévues par le règlement, la disparition des formalités préalables, entraine une perte de contrôle *a priori* et il convient de s'interroger sur ce qu'il va subsister du système déclaratif et les conséquences prévisibles d'un système purement curatif pour les droits des personnes.

B. La persistance de contrôle *a priori*

579. La subsistance de formalités préalables auprès de la CNIL. La protection de la vie privée que ce soit sur le fondement du secret

[412] J.-M. JOB, « La loi « Informatique et libertés » et les données de santé », *Revue Lamy Droit de l'immatériel*, janv. 2008, n° 34, p. 87.

professionnel, de l'obligation de discrétion professionnelle[413], ou de la confidentialité, a pendent longtemps été réalisée de manière curative et non préventive[414].

580. Ainsi, sur le fondement de l'article 226-13 du Code pénal, pour que l'infraction de violation du secret professionnel soit constituée, la protection de l'intimité de la vie privée suppose qu'une révélation de l'information couverte par le secret ait déjà été réalisée par le professionnel. Pour que la personne puisse engager la responsabilité civile de l'indiscret sur le fondement de l'article 1240 du Code civil, il faut qu'il y ait l'existence d'une faute, d'un préjudice mais aussi d'un lien de causalité.

581. Cette protection a posteriori est, dans le cadre de traitements de données à caractère personnel, insatisfaisante. En effet, du fait de la dématérialisation, les conséquences d'une divulgation non consentie sont sans commune mesure pour la personne concernée par le traitement de ses données.

582. Les données sont, par nature, reproductibles et communicables. Par conséquent, elles peuvent aisément être rendues publiques par l'utilisation des technologies de l'information et de la communication et notamment, par le web et ainsi être copiées, stockées, ou encore rendues accessibles, n'importe où dans le monde. Ainsi, le préjudice résultant de la divulgation de l'information est d'autant plus important pour la personne que la donnée devient difficilement effaçable. C'est pourquoi les *« atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques »* sont davantage réprimées. *« Ainsi, à identités de valeurs protégées, la violation de la confidentialité emporte une peine de cinq ans d'emprisonnement et trois cent mille euros d'amende, alors*

[413] Loi n° 83-634 du 13 juillet 1983 portant sur les droits et obligations des fonctionnaires, art. 26.

[414] A. NIETO*, La vie privée à l'épreuve de la relation de soin,* Thèse, Montpellier, 2017, p. 479.

que la violation du secret est punie d'une peine d'un an d'emprisonnement et de quinze mille euros d'amende »[415] .

583. Ces atteintes sont *« beaucoup plus dangereuse, compte tenu des facilités existantes en matière de transfert de données [et de] la faculté d'utiliser des données à des fins radicalement différentes de celles pour lesquelles elles ont été collectées. Pour prendre un exemple extrême, la communication de certaines données de santé à un assureur ou un banquier, peut conduire à des discriminations et à des exclusions inadmissibles. Ainsi, la répercussion encore trop souvent négative de la connaissance de l'état d'infection par le virus HIV sur la vie professionnelle ou sociale des personnes concernées impose-t-elle une particulière vigilance à l'égard de la constitution et du traitement de fichiers comportant ce type de données »*[416].

584. Au regard de de la nature protéiforme des atteintes, susceptibles d'être commises, aux droits et libertés de la personne et de l'ampleur du préjudice pouvant résulté de la circulation non maitrisée de données à caractère personnel relatives à la santé, une approche strictement fondée sur la répression ou l'indemnisation est insuffisante voir inefficace.

585. *« L'accomplissement de formalités préalables auprès de la CNIL permet, ainsi, dans nombre de cas de déceler préventivement les risques d'atteinte aux droits des personnes.* »[417]

---

[415] C. ZORN, *op. cit*.,, p. 70, n° 41. Voir également, A. LEPAGE, « 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 », *Dr. pénal* 2005, chron. 5. Voir également le projet de loi relatif à l'assurance maladie, présenté par P. DOUSTE-BLAZY, Assemblée Nationale, 2004, disponible sur : http://www.assembleenationale.fr/12/projets/pl1675.asp

[416] G. BRAIBANT, *Données personnelles et société de l'information*, Rapport au Premier Ministre sur la transposition en droit français de la directive (dir.) 95/46, 1998.

[417] I. COULIBALY, La protection des données à caractère personnel dans le domaine de la recherche scientifique, Thèse, Grenoble, 2011, p. 89.

586. C'est pourquoi, la réglementation du traitement de données à caractère personnel comporte, depuis la directive de 1995, des dispositions ad hoc, reposant sur la mise en œuvre de procédures administratives préventives[418].

587. En ce qui concerne le domaine du soin, il existe un panel de formalités auprès de la Commission. Celles-ci vont de la déclaration normale[419] en passant, par exemple, par la demande d'autorisation de traitement de données sensibles, la demande d'autorisation de recherche médicale[420], la demande d'autorisation d'évaluation des pratiques de soins, ou encore la demande d'avis. Toutefois, leur préférant un dispositif reposant sur la responsabilisation des acteurs du traitement de données à caractère personnel, l'article 36 du règlement prévoit la suppression de ces formalités déclaratives préalables.

588. *« Un système de protection fondé sur une réparation des préjudices subis du fait d'un mésusage des informations, peut s'avérer superflu. Un système préventif des atteintes s'avère plus protecteur. »*[421]

589. Bien que le RGPD substitue à ce système de déclaration préalable la mise en œuvre d'une étude d'impacts relatifs à la vie privée ; il semble, au regard des dispositions du paragraphe 5 de l'article 36, que la suppression de cette obligation concerne uniquement les traitements ne constituant pas un risque pour la vie privée des personnes.

590. *« Le droit des États-membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et*

---

[418] J. LE CLAINCHE, L'adaptation du droit des données à caractère personnel aux communications électroniques, Thèse, Montpellier, 2008.

[419] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 22.

[420] Loi. préc. art. 44.....

[421] I. COULIBALY, *op. cit.* p. 89.

obtiennent son autorisation préalable en ce qui concerne le traitement effectué par un responsable du responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci, y compris le traitement dans le cadre de la protection sociale et de la santé publique. »[422]

591. Les traitements dont la mise en œuvre exige la réalisation d'une demande préalable d'autorisation ne seraient par conséquent pas concernés par cette évolution.

592. La loi du 6 août 2004[423] transposant dans notre droit national la directive de 1995, a introduit, au sein de la loi relative à l'informatique, aux fichiers et aux libertés, un article 25[424]. Aux termes de ces dispositions, cet article subordonne la mise en œuvre de certains traitements à l'obtention d'une autorisation préalable par le responsable de traitements. Cette autorisation délivrée par la CNIL concerne trois catégories de traitements en raison du fait qu'ils poursuivent des finalités spécifiques, qu'ils nécessitent le transfert de données en dehors de l'Union européenne ou qu'ils portent sur une catégorie particulière de données.

593. Plus particulièrement, en ce qui concerne la nature des données traitées, les données à caractère personnel sensibles[425], autrement dit, les données énumérées au (I) de l'article 8 de la loi du 6 janvier 1978 et qui comportent notamment les données concernant la santé, la religion, la vie sexuelle ou encore des appréciations sur les difficultés sociales des personnes, ainsi que les données biométriques, génétiques, etc. doivent

[422] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 36 § 5.

[423] 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.

[424] Modifié par la Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

[425] N. ETIEN-GNOAN, L'encadrement juridique de la gestion électronique des données médicales, Thèse, Lille, 2014, p. 57.

faire l'objet d'une demande d'autorisation préalable auprès de la Commission.

594. Concernant, les traitements poursuivant une finalité spécifique, ceux-ci doivent également faire l'objet d'une demande d'autorisation, sont notamment concernés les traitements susceptibles d'exclure une personne du bénéfice d'un droit, les traitements de recherche médicale, les traitements ayant pour finalité l'évaluation des pratiques de soins.

595. Au regard des dispositions de l'article 25 (III), la CNIL dispose d'un délai de 2 mois pour se prononcer sur ces demandes. Ce délai commence à courir à compter de la réception du dossier. Il peut toutefois être renouvelé une fois sur décision motivée de son président. Lorsque la commission ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée être rejetée. Toutefois, dans la pratique, ce délai est fréquemment dépassé. D'une manière générale, les services de la CNIL sont dans ce cadre régulièrement sollicités pour la gestion des dossiers de demande. A titre d'exemple, « *pour la période du 1er janvier au 31 décembre 2006, la CNIL a enregistré 72000 nouveaux traitements de données personnelles et 1800 déclarations de modification de traitements déjà déclarés, soit au final 73800 dossiers à gérer sur l'année* »[426].

596. Compte tenu de la complexité des dossiers, la Commission est également régulièrement confrontée à la nécessité de formuler des demandes complémentaires conduisant ainsi à de nombreux échanges avec les déclarants. Aussi, dans les secteurs sanitaire, social et médico-social un retard dans la gestion de ces formalités préalables peut pour certains traitements avoir des implications conséquentes sur la qualité des soins dispensées. Cela peut parfois engendrer une perte de chance pour le

[426] CNIL, 27ème Rapport d'activité, 2006.

patient, notamment en ce qui concerne la mise en œuvre de projets de « Télé AVC »[427].

597. Malgré l'intérêt que peut représenter le maintien d'un système déclaratif, le fait de limiter ce contrôle préalable aux traitements pouvant représenter un risque pour les droits et libertés des personnes ou desquels il peut résulter une atteinte conséquente à leur vie privée, nous paraît être la solution la plus appropriée. Ce compromis permet, à chacun des États-membres de l'Union européenne, de réaliser les arbitrages nécessaires afin de rechercher un équilibre entre la prévention des atteintes à la vie privée et aux droits et libertés des personnes pouvant résulter du traitement de leurs données à caractère personnel et, d'autres intérêts, tel que la qualité des soins ou encore l'efficience du système de santé.

598. Au regard de ces éléments, l'utilisation du NIR, l'exploitation de données de santé, certains transferts de données à caractère personnel à destination de pays situés en dehors de l'Union européenne et qui ne présenteraient pas un niveau de protection adéquat continueraient à être subordonnés à l'autorisation de la Commission.

599. En ce qui concerne le secteur sanitaire, les traitements de données à caractère personnel relatives à la santé étant actuellement essentiellement soumis au régime d'autorisation, les responsables de traitement ne seraient, par conséquent, pas dispenser de déclarer auprès de la CNIL les traitements projetés préalablement à leur mise en œuvre.

600. La demande d'autorisation demeure un moyen pour la Commission de présider au respect des principes issus de la loi Informatique et Libertés. L'analyse des déclarations réalisées sur son site, ou au moyen d'un « Cerfa » lui permettent d'apprécier que le traitement

[427] Le télé-AVC est un dispositif permettant à un praticien de transmettre à un neurologue des examens d'imagerie médicale concernant un patient faisant l'objet d'une suspicion d'Accident Vasculaire Cérébral. Celui-ci accède dans le cadre d'une téléconsultation en urgence à l'expertise d'un médecin neurologue en vue de réaliser un acte de thrombolyse.

repose sur des finalités déterminées, explicites et légitimes et que les données collectées sont adéquates, pertinentes et non excessives par rapport à la finalité poursuivie. La CNIL apprécie également si le responsable du traitement exploite ces données de manière licite, loyale et transparente en vérifiant, d'une manière générale que l'organisation du traitement permette de garantir l'effectivité des droits de la personne. Elle contrôle ainsi, que des supports d'information ont été élaborés, qu'il existe un processus du recueil de consentement ou tout du moins que le traitement repose sur un autre fondement[428].

601. Le dossier de demande d'autorisation comporte également une partie dédiée à la sécurité et à l'architecture informatique qui doit être renseignée par le responsable du traitement, le cas échéant à l'aide de son sous-traitant. Lors de l'examen de la demande, la Commission estime le niveau de maturité du responsable de traitement et du sous-traitant, elle contrôle que des mesures de sécurité, logique, physique mais aussi juridique ont été mises en œuvre afin de s'assurer la confidentialité, l'intégrité, l'authenticité et la disponibilité des données. D'une manière générale, la CNIL apprécie également, par ce moyen, si les mesures de sécurité mises en œuvre pour l'ensemble du processus de traitement des données comprenant leur collecte, leur utilisation, leur sauvegarde, leur archivage mais aussi leur destruction, sont suffisantes au regard des risques et de la catégorie des données traitées.

602. Toutefois, en ce qui concerne les données sensibles et plus particulièrement les données de santé, il convient de s'interroger sur le maintien de ce dispositif, dans son intégralité, postérieurement au 25 mai 2018. Rappelons à cette fin que pour les états monistes comme la France, l'applicabilité immédiate ou effet direct du droit communautaire implique qu'une norme communautaire, à partir du moment où celle-ci est

[428] Règl. (UE). PE et Cons. UE 2016/679, art. 5 (h).). Voir également Dir. n°95/46/CE et Loi n° 78-17 du 6 janvier 1978, article (art. 6.

inconditionnelles et suffisamment précise[429], s'intègre automatiquement dans l'ordre juridique de l'état concerné et qu'elle produit des effets en droit interne sans que les institutions de cet état aient recours à des mesures nationales de transposition[430]. Aussi, le RGPD rappel en son article 99 ce principe figurant également à l'article 288 du Traité sur le fonctionnement de l'Union européenne.

603. Bien que cela ne soit donc pas nécessaire, des modifications de la loi

604. Informatique et Libertés sont actuellement à l'étude. Celles-ci ont pour but de reprendre les dispositions du règlement, essentiellement afin d'utiliser les marges d'appréciation laissées par celui-ci, notamment en ce qui concerne la possibilité de conserver la procédure d'autorisation préalable. Dans ce contexte, Madame Isabelle Falque Pierrotin, Conseillère d'État et présidente de la CNIL depuis le 21 septembre 2011, a précisé, a de nombreuses reprises au cours de l'année 2017, qu'il n'était peut-être pas opportun de changer complètement ce régime d'autorisation préalable en ce qui concerne le traitement de données relatives à la santé.

605. Toutefois, dans la perspective de l'entrée en application du règlement, la CNIL a décidé d'appliquer, par anticipation, les principes qui en résultent. Aussi, dans un souci de simplification et, malgré les dispositions introduites par la loi de 2004 au sein de la loi Informatique et Libertés, elle a résolu de soumettre au régime de la déclaration les

---

[429] CJCE, 5 févr. 1963, NV Algemene Transport – en Expedite Onderneming Van Gend en Loos c/ Administration fiscale néerlandaise, aff. 26/62.

[430] CJCE, 15 juillet 1964, Costa c/ E.N.E.L., aff. 6/64 : *« Une obligation des états membres en vertu du Traité C.E.E., non assortie d ' aucune* condition, *ni subordonnée , dans son exécution ou ses effets , a l ' intervention d ' aucun acte , ni des états , ni de la commission , est juridiquement parfaite et , en conséquence , susceptible de produire des effets directs dans les relations entre les états membres et les justiciables . Une telle obligation est intégrée au système juridique des états membres, constitue la loi même de ceux-ci et concerne directement leurs ressortissants au profit desquels elle a* engendré *des droits individuels que les juridictions internes doivent sauvegarder. »*

Voir également CJCE, 9 mars 1978, Administration des finances de l'État c/ Société anonyme Simmenthal, aff. 106/77.

traitements relevant des exceptions prévues à l'article 8 (II) de la loi « informatique et libertés ». Sont notamment concernés par cette décision de simplification les dispositifs de télémédecine mais aussi les dossiers médicaux partagés. Les motifs invoqués par la Commission dans son communiqué du 19 mai 2017 reposent sur *« la maturité plus grande des responsables de traitement de données de santé quant à leurs obligations au regard de la loi »*[431] mais aussi, sur le renforcement des contrôles a posteriori afin de s'assurer du respect de la réglementation, notamment en ce qui concerne l'information et le consentement des personnes.

606. Conformément aux dispositions de l'article 36 paragraphe 5 du Règlement, le régime de demande d'autorisation continue à s'appliquer pour les traitements de données de santé non visés à l'article 8 II de la loi Informatique et

607. Libertés qui sont justifiés par un intérêt public ainsi que pour les traitements de données à caractère personnel relatives à la santé qui sont réalisés à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé. Ces traitements demeurent régis par les dispositions du Chapitre IX de la loi Informatique et Libertés et, par conséquent soumis à l'autorisation préalable de la CNIL.

608. Cette mesure de simplification des formalités préalables constitue une évolution d'une procédure essentiellement fondée sur un contrôle sur pièces. Elle permet à la Commission de se restructurer afin de se concentrer sur ses missions principales comprenant notamment les contrôles a posteriori. Elle met fin à l'insécurité juridique résultant du dépassement systématique des délais prévus dans le cadre de la procédure de demande d'autorisation. Il est toutefois regrettable que le règlement permette aux États-membres de maintenir exclusivement une demande

[431] CNIL, *« Traitement des données de santé : une logique de simplification et de responsabilisation accrue des acteurs »*, Communiqué du 19 mai 2017, disponible à l'adresse suivante : https://www.cnil.fr/fr/traitement-des-donnees-de-sante-une-logique-de-simplification-et-de-responsabilisation-accrue-des

d'autorisation dans le cadre de traitements relatifs à la santé publique ou encore uniquement dans le cadre d'une mission d'intérêt public et ceci sans définir cette notion.

609. De l'agrément à la certification des hébergeurs de données de santé. Les dispositions du décret étant en cours de finalisation, les observations qui suivent sont fondées sur le projet de décret publié en juillet 2017 et sont purement indicatives. Elles peuvent s'avérer contredites par les termes définitifs du décret.

610. Les récentes évolutions réglementaires en matière de protection des données à caractère personnel sont marquées par la substitution aux formalités préalables d'opérations de contrôle opérées a posteriori. Toutefois, en matière d'hébergement de données de santé, les mutations opérées préservent ce système de contrôle réalisé a priori car *« la nature sensible des données de santé à caractère personnel impose qu'elles soient stockées au moyen de techniques les plus performantes garantissant leur sécurité, leur confidentialité, leur intégrité et leur traçabilité* »[432].

611. Les conditions d'hébergement de données de santé à caractère personnel sont définies par l'article L. 1111-8 du Code de la santé publique. Issue de la loi du 4 mars 2002[433], cet article a été modifié par le décret du 4 janvier 2006[434] qui est venu préciser le déroulement de la procédure ainsi que les exigences devant être satisfaites par le candidat pour l'obtention de l'agrément.

612. S'agissant de l'hébergement sur support électronique, l'agrément est délivré pour une durée de trois ans, par un arrêté du ministère de la

[432] P. BICLET, *Premier rapport d'activité du comité d'agrément des hébergeurs*, 2006-2011, p. 5.

[433] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

[434] 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.

santé pris après avis d'un comité d'agrément des hébergeurs (CAH) et de la CNIL[435].

613. Ce comité a pour fonction d'apprécier les garanties d'ordre éthique, déontologique, technique et économique qu'offre le candidat. La demande d'agrément était simultanément *« examinée par la CNIL qui se prononce sur les garanties que présente le candidat en matière de protection des données à caractère personnel et des droits des personnes, de respect du secret professionnel, ainsi que sur les modèles de contrats à l'origine du dépôt de données et les éventuels sous-traitants de l'hébergeur. »*[447]

614. Cette procédure, en raison de la participation de la CNIL, du ministère de la santé et du CAH[436] est impartiale mais présente pour principal défaut d'être purement déclarative et uniquement réalisée sur pièces. Ainsi, le temps de traitement des dossiers est considérable[437]. Cette modification repose sur un constat de lourdeur administrative clairement posé par l'exposé des motifs, qu'il n'est pas utile de paraphraser :

---

[435] C. santé publ, art. R. 1111-10, al. 1. Modifié par Décret n° 2011-246 du 4 mars 2011, art. 1. 447 C. ZORN, op. cit., p.243.

[436] Conformément aux dispositions de l'art. R. 1111-11 C. santé publ., le comité d'agrément des hébergeurs de données de santé est composé d'un membre de l'inspection générale des affaires sociales, de deux représentants d'associations nationales agréées et qui sont compétentes en matière de santé, de deux représentants des professions de santé et de trois personnalités qualifiées en raison de leurs compétences dans les domaines de l'éthique et du droit, de la sécurité des systèmes d'information (SSI) et des nouvelles technologies, de l'économie et des finances ainsi, qu'à titre consultatif, des directeurs généraux de la santé, de l'offre de soin, des patrimoines mais aussi des entreprises et enfin de la concurrence ,de la consommation et de la répression des fraudes.

[437] Sans tenir compte de la préparation du dossier par le candidat à l'agrément, la durée de la procédure entre la date de réception du dossier par l'Agence des systèmes d'information partagés de santé (ASIP Santé) et la publication de l'arrêté du Ministre de la Santé et de 8 mois en moyenne. Toutefois, *« dans 30% des cas, lorsque des compléments d'information sont demandés aux candidats, le délai d'instruction peut dépasser les huit mois prévus. »* Les données relatives à la procédure d'agrément des hébergeurs de données de santé sont accessibles sur le site de l'Asip Santé http ://esante.gouv.fr/

615. *« Le dispositif d'agrément des hébergeurs repose actuellement sur un double examen des demandes d'agrément par la CNIL (228) et par une instance ad hoc, le "comité d'agrément des hébergeurs de données de santé", dont le secrétariat est assuré par l'ASIP-Santé. La spécificité nationale et la lourdeur de ce dispositif constituent un obstacle à sa transposition au niveau européen ou international. »*[438]

616. Par ailleurs le référentiel d'agrément se limite à identifier les objectifs devant être atteints par les candidats à l'agrément sans pour autant donner d'indications sur les moyens devant être mis en œuvre afin de parvenir au résultat attendu. Aussi, les candidats ne peuvent déterminer si les mesures techniques, organisationnelles et juridiques qu'ils mettent en œuvre sont de nature à assurer un niveau de sécurité suffisant et si elles seront jugées satisfaisantes par le CAH.

617. L'absence de grille d'analyse à disposition de l'hébergeur engendre, au cours de la procédure d'agrément, de nombreuses demandes de compléments d'information, de modifications de l'organisation du candidat mais aussi des réserves. C'est pourquoi, il est reproché à cette procédure d'être coûteuse et, de ne pas être transparente en raison de l'absence de critères définis précisément par les textes et de véritable référentiel d'exigences public, auditable et évolutif.

618. De surcroît, l'agrément obtenu, l'article L. 1111-8 al. 9 du Code de la santé publique confie à l'Inspection générale des affaires sociales (IGAS) le soin de procéder à des contrôles des hébergeurs de données de santé à caractère personnel, le cas échéant, *« les agents chargés du contrôle peuvent être assistés par des experts désignés par le ministre charge de la santé »*. Cette possibilité de contrôle par l'IGAS permise par les textes n'a jamais été mise en œuvre. Ainsi, il n'existe aucun véritable

[438] O. VERAN, B. LACLAIS, J.-L. TOURAINE, H. GEOFFROY, R. FERRAND, Rapport sur le projet de loi relatif à la santé, Rapport n° 2673, 20 mars 2015, p. 832-833.

contrôle des conditions réelles d'hébergement. De ce fait, il n'est pas certain que les hébergeurs agréés mettent en œuvre les mesures décrites, au sein des documents produits lors de la demande d'agrément. Pareillement l'IGAS avait initialement pour mission de contrôler l'ensemble des hébergeurs de données de santé qu'ils soient agréés ou non. Aussi, comme nous l'avons précédemment précisé, en l'absence de véritable contrôle, ces dispositions destinées à protéger les données de santé ainsi que les droits de la personne sont dépourvues d'effet. Aussi, comme l'ASIP Santé le fait remarquer au sein de son référentiel de certification, *« la majorité des données de santé à caractère personnel reste probablement encore hébergée par des tiers hors du cadre juridique de l'agrément »*[439].

619. Enfin, sur le fondement de l'article 44 de la loi Informatique et Libertés, la CNIL a le pouvoir de diligenter des contrôles auprès de tout responsable de traitement ainsi, par le truchement de cet article, la Commission peut contrôler les activités des hébergeurs de données de santé et le cas échéant, sa formation restreinte peut sanctionner les responsables de traitement en respectant par leurs obligations au moyen des dispositions du chapitre VII.

620. Toutefois, l'ASIP Santé précise également au sein du référentiel de certification qu'en ce qui concerne les conditions réelles d'hébergement, l'absence de mise en place « de contrôles et d'obligations d'audits externes par des auditeurs qualifiés empêche les pouvoirs publics d'avoir une vision concrète des réalités du terrain. En outre, les textes relatifs à l'hébergement de données de santé et le référentiel d'agrément ne répondent pas toujours à l'évolution des conditions techniques et de l'offre commerciale des services d'hébergement. Il est donc apparu nécessaire au législateur de proposer une adaptation des conditions

[439] Référentiel de certification version 0.3.0., « Vue. *« vue d'ensemble* »,». p. 6. Publié pour concertation le 16 septembre 2016 et disponible à l'adresse suivante : http ://esante.gouv.fr/actus/services/agrement-des-hebergeurs-de-donnees-de-sante-publication-dureferentiel-de 452 *Ibid.*

d'hébergement de données de santé, avec pour finalité principale la protection des données de santé à caractère personnel »452.

621. Pour ces motifs, un comité de pilotage regroupant des représentants du monde industriel, notamment l'Association Française des Hébergeurs Agréés de Données de Santé à Caractère Personnel (AFHADS), le Syndicat National de l'Industrie des Technologies Médicales (SNITEM), le Syndicat professionnel des entreprises de services du numérique (SYNTEC numérique) et des représentants du secteur public composé du Ministère de la santé, des Fédérations hospitalières, des

622. Ordres professionnels mais aussi de la CNIL et de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été réuni afin de valider le nouveau dispositif défini par la Délégation à la stratégie des systèmes d'information de santé (DSSIS) et l'ASIP Santé, en prenant en considération ces éléments.

623. Ainsi, la loi de modernisation de notre système de santé [440] modifie les dispositions de l'article L. 1111-8 du Code de la santé publique afin de substituer à la démarche visant à l'obtention d'un agrément une procédure de certification[441]. De ce fait, les prestataires proposant des services d'hébergement, sur support numérique, de données à caractère personnel relatives à la santé recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil desdites données ou pour le compte du patient lui-même devront désormais bénéficier d'une certification.

[440] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

[441] C. santé publ, art. L. 1111-8 (II) :). *« L'hébergeur de données mentionnées au premier aliéna du I sur support numérique est titulaire d'un certificat de conformité. »*

624. Cette certification est réalisée suite à une évaluation de conformité à un référentiel de certification élaboré par l'ASIP Santé « en lien avec les organismes d'accréditation concernés et approuvé par arrêté du ministre chargé de la santé »[442]. Elle est, délivrée par un organisme certificateur accrédité par le Cofrac ou un équivalent au niveau européen dans les conditions définies à l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie.

625. Au regard des dispositions de l'Ordonnance n° 2017-27 du 12 janvier 2017 et du projet de décret, cette démarche de certification semble solutionner l'ensemble des carences de la procédure d'agrément. Contrairement à celle-ci, le référentiel de certification élaboré par l'Agence des systèmes d'information partagés de santé (ASIP Santé), s'appuie, outre des exigences spécifiques à l'activité d'hébergement de données de santé, explicitement sur des normes internationales reconnues. Ces normes sont constituées par un comité technique d'experts réunit à l'initiative de l'Organisation internationale de normalisation (ISO)[443]. Il s'agit en l'occurrence des normes ISO 27001 relative au *« système de gestion de la sécurité des systèmes d'information »*[444], ISO 20000 *« système de gestion de la qualité des services »*, ISO 27018 « protection des données à caractère personnel ».

626. Les industriels intervenant dans le secteur sanitaire et/ou proposant ou souhaitant proposer une offre de services d'hébergement de données de santé, se voient, le plus souvent, imposer l'obligation d'être certifié pour une ou plusieurs de ces normes lorsqu'ils soumissionnent à

---

[442] C. santé publ, art. R. 1111-10 dans sa rédaction issue du projet de décret relatif à l'hébergement de données de santé à caractère personnel et modifiant le Code de la santé publique.

[443] Ces normes sont disponibles sur le site de l'Organisation internationale de normalisation, à l'adresse suivante : https ://www.iso.org/fr/standards.html.

[444] La norme ISO 27001 repose sur une approche systémique. Construite selon un processus de management du risque, elle envisage la sécurité de l'information sous l'angle organisationnel afin d'en garantir l'effectivité et l'efficacité. Elle permet également d'instaurer une démarche d'amélioration continue (roue de Deming) de la sécurité des systèmes d'information (SSI).

un contrat portant sur des prestations informatiques, plus particulièrement en ce qui concerne les normes ISO 27001, ISO 27018, voir également ISO 2000. C'est notamment le cas en ce qui concerne l'hébergement du dossier pharmaceutique mis en œuvre, conformément aux dispositions de l'article L. 1111-23 du Code de la santé publique par le Conseil national de l'Ordre des pharmaciens (CNOP) et pour lequel l'hébergeur agréé, la société Docapost BPO protège la chaîne de traitement et de conservation des données *« par des mécanismes de chiffrement et de sécurisation, conformément à la norme internationale ISO 27001 »*[445].

627. Nous l'avons précédemment précisé, contrairement à la procédure d'agrément, le fait que ce référentiel soit constitué d'exigences fondées sur des normes techniques internationales connues et respectées des candidats à la certification, rend cette nouvelle procédure transparente, et permet à un nombre conséquent de prestataires de pouvoir prétendre à la certification. Par ailleurs, cette nouvelle procédure est beaucoup plus souple et contrairement au référentiel d'agrément, elle permet une adaptation des exigences à l'évolution des pratiques, enjeux et risques en raison de la mise en place d'un cycle de vie du référentiel. Par ailleurs, les normes ISO font l'objet d'un processus de révision systématique tous les 5 ans par un comité d'expert et soumises à concertation entre les différentes parties prenantes, universitaires, organisations non gouvernementales (ONG), institutions public, experts du domaine concerné, représentants d'associations de consommateurs, afin de tenir compte de l'évolution des pratiques, des technologies et des organisations. Cette révision repose sur une procédure consensuelle afin de tenir compte des attentes des parties prenantes.

[445] Conseil national de l'Ordre des pharmaciens, Direction des technologies en santé, Rapport d'activité : « Le Dossier Pharmaceutique »,» 2013, p. 8.

628. La procédure de certification est elle-même fondée sur le processus standard de type système de management décrit dans la norme ISO 17021

629. *« Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management » et précisé par la norme ISO 27006 « Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information. »*

630. Ainsi, le candidat à la certification choisit un organisme certificateur accrédité par le Cofrac ou un équivalent au niveau européen, auprès duquel il procède à un dépôt de son dossier.

631. La procédure est désormais décomposée en deux phases. La première phase consiste en un audit documentaire similaire à celui réalisé dans le cadre de l'ancienne procédure d'agrément. L'organisme certificateur réalise une revue de la documentation du système d'information du candidat afin de déterminer la conformité documentaire du système par rapport aux exigences du référentiel de certification. La seconde phase consiste en un audit sur site. Le certificat délivré, un audit de surveillance est mené dans les douze mois suivant la décision puis une fois par an. La seconde phase consiste en un audit sur site, réalisé dans les conditions définies au sein du référentiel. À l'issue de l'audit sur site, l'hébergeur dispose de trois mois pour corriger les éventuelles non-conformités constatées et faire auditer les corrections par l'organisme certificateur. Passé ce délai et sans action de l'hébergeur, l'audit sur site devra être recommencé. Le certificat délivré, un audit de surveillance est mené dans les douze mois suivant la décision puis une fois par an. À l'instar du délai de validé de l'agrément, le certificat est délivré pour une durée de trois ans.

632. Comme le relève C. Zorn, au regard de la conception de la procédure d'agrément, la protection des données à caractère personnel

relative à la santé qui sont hébergées est insatisfaisante[446]. En effet, nous l'avons auparavant énoncé, l'IGAS s'était vue confié, la mission de contrôler l'ensemble des hébergeurs de données de santé qu'ils soient agréés ou non. Toutefois, ces dispositions n'ont jamais été mises en œuvre, ainsi aucun contrôle n'a été formellement réalisé. Aussi, au regard de cette absence de réel contrôle par le CAH et par l'IGAS et, en raison d'une procédure d'appréciation des capacités exclusivement fondée sur une analyse des pièces produites par le candidat, il peut exister un écart significatif entre les diligences réellement mises en œuvre par l'hébergeur et celles décrites au sein du dossier de demande d'agrément soumis au Comité. Cette situation n'est pas de nature à garantir la sécurité des données à caractère personnel relatives à la santé qui sont hébergées et, n'est pas propice au respect des droits de la personne.

633. Aussi, l'ASIP Santé, semble tirer les conclusions de ces faiblesses.

634. C'est pourquoi, dans le cadre de la procédure devant être instituée suite à l'adoption de la loi de modernisation de notre système de santé, il est projeté d'aménager une démarche de suspension mais aussi de retrait du certificat délivré.

635. Ainsi, contrairement aux anciennes dispositions, réitérées à titre transitoire au (VI) de l'article 1 de l'ordonnance n°2017-27[447], à l'issue de la procédure de certification, le contrôle du respect des obligations pesant sur l'hébergeur est confié à l'organisme lui ayant délivré le certificat. Dans ce cadre, l'organisme réalise un audit, dit de surveillance, sur site, 12 mois

[446] *Ibid.,*. p.206.

[447] Ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, art. .)1, VI : *« Les hébergeurs de données de santé à caractère personnel ou qui proposent cette prestation d'hébergement sont soumis, dans les conditions prévues aux articles L. 1421-2 et L. 1421-3, au contrôle de l'inspection générale des affaires sociales et des agents mentionnés aux articles L. 1421-1 et L. 1435-7. »*

après la certification. Cette opération de contrôle doit être réitérée chaque année pendant toute la période de validité du certificat.

636. Si un écart est constaté entre le système de management de l'hébergeur et les exigences découlant du référentiel, ou s'il est établi, *in fine*, que l'hébergeur ne respecte pas ses engagements, cet organisme peut, par une décision motivée, suspendre pour une durée de 3 mois, le certificat. Cette suspension peut être reconduite une fois, pour une durée équivalente, soit une durée totale ne pouvant excéder 6 mois.

637. Si la suspension a été décidée par l'organisme de certification, l'hébergeur dispose d'un délai de 10 jours pour présenter par écrit ses observations ou, le cas échéant, faire appel de la décision. Il semble au regard des dispositions du référentiel que l'appel ne soit pas suspensif de la décision de l'organisme. Ainsi, le certificat demeure invalide pendant la période considérée et l'hébergeur ne peut durant ce délai se prévaloir de sa certification.

638. Il doit également supprimer toute communication sur celle-ci et doit, par ailleurs, informer « tout demandeur » de la suspension de son certificat.

639. Toutefois, sur la base de justifications formulées et documentées ou après qu'un audit ait constaté la mise en œuvre de mesures correctives, l'hébergeur peur voir son certificat réactivé. *A contrario*, le certificat sera invalidé et l'organise sera tenu de cesser toute publicité et d'appliquer le processus de retrait.

640. La procédure de suspension, ainsi que les mesures décrites au sein du référentiel, sont communément admises en ce qui concerne des démarches de certification. Toutefois, il convient de s'interroger sur les conséquences d'une telle décision.

641. En effet, la suspension produit des effets en ce qui concerne les tiers puisque l'hébergeur ne peut se prévaloir de son certificat. Cependant,

dans l'éventualité où l'hébergeur soumissionnerait à un marché passé par un établissement de santé public, cette suspension pourrait être sans incidence. En effet l'article 55 paragraphe I du décret du 25 mars 2016[448] contrairement à l'ancien article 52 du Code des marchés publics permet à « l'acheteur qui constate que des pièces ou informations dont la présentation était réclamée au titre de la candidature sont absentes ou incomplètes peut demander à tous les candidats concernés de compléter leur dossier de candidature dans un délai approprié et identique pour tous ». Ainsi à défaut de la publication de la liste des hébergeurs certifiés ou faisant l'objet d'une suspension, l'hébergeur candidat à un marché pourrait ne pas produire son certificat et attendre une demande de régularisation en fin de procédure de passation de marché pour y procéder. Les marchés portant sur des besoins complexes nécessitent le plus souvent une procédure de dialogue compétitif et il n'est pas rare que celles-ci durent pendant une période pouvant atteindre 6 mois. Par ailleurs, si l'hébergeur dispose d'une certification pour une ou plusieurs des normes entrant dans le périmètre du référentiel, il pourrait également sans méconnaitre ses obligations, se prévaloir de celle-ci sans communiquer sur son certificat dans le cadre de la procédure en cours.

642. Concernant les contrats conclus antérieurement à la suspension prononcée par l'organisme de certification, l'article L. 1111-8 du Code de la santé publique ne fait pas peser explicitement sur les établissements et professionnels de santé ainsi que sur les autres personnes physiques ou morales l'obligation de recourir à un hébergeur certifié mais met à la charge des prestataires de services d'hébergement de données de santé l'obligation d'être certifié. Ainsi, l'hébergeur dont le certificat serait suspendu et qui continuerait à héberger des données de santé à caractère personnel, méconnaitrait ces dispositions et serait susceptible de faire l'objet de sanctions.

[448] Décret n° 2016-360 du 25 mars 2016 relatif aux marchés publics.

643. Par ailleurs, l'article 32 du RGPD impose aux professionnels et structures qui recueillent les données dans les conditions décrites à l'article L. 1111-8 ainsi qu'aux hébergeurs de mettre en œuvre « les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté ». En outre, l'article 42 du règlement qui permet aux États-membres de mettre en place des mécanismes de certification en matière de protection des données formule explicitement que la certification ne diminue pas la responsabilité du responsable du traitement ou du sous-traitant. Ce même article précise que la procédure de certification est sans incidence sur les missions et pouvoirs de la CNIL qui peut ainsi continuer de procéder aux opérations de contrôle et, le cas échéant, prononcer les sanctions prévues au règlement. Au regard de ce qui précède, il n'est prévu aucune dérogation par le règlement. Bien que la suspension soit temporaire, il est surprenant que le référentiel et que les dispositions relatives à l'accréditation de l'organisme de certification ne prévoient aucunement l'obligation d'informer la Commission ou tout du moins les cocontractants lorsque des manquements sont constatés plus particulièrement lorsque la suspension est reconduite pour une période de 3 mois. Cette mesure leur permettrait, en fonction des stipulations du contrat, de procéder à l'application de pénalités prévues au sein de celui-ci, de demander l'application des mesures y étant annexées et qui seraient décrites au sein du Plan d'assurance sécurité (PAS) et/ou du Plan de continuité d'activité (PCA) ou le cas échéant d'anticiper une éventuelle procédure de retrait de certificat et de préparer ainsi la réversibilité des données.

644. Ceux-ci ne sont pas, en effet, relevé de leur obligation résultant du règlement et disposent, le plus souvent, dans le cadre du contrat d'hébergement de clauses de pénalités financières susceptibles d'être appliquées à l'encontre du sous-traitant qui manquerait à ses obligation contractuelles.

645. Toutefois, l'obligation d'information n'intervient qu'à l'issue d'une procédure de retrait du certificat sur décision de l'organisme de

certification. Cette procédure est mise en œuvre sur à la cessation de l'activité de l'hébergeur, ou après que l'organisme est constaté des écarts ou des manquements répétés aux exigences définies dans le référentiel de certification, ou encore dans l'éventualité où l'hébergeur n'aurait pas respecté les délais relatifs à la période de surveillance définie précédemment ou aurait mis en œuvre une pratique frauduleuse de l'activité et ce pendant une période de plus d'un an.

646. À travers plusieurs citations de Georges Ripert, C. Zorn invite à *« la réflexion sur les rapports entre la technique et le droit, ainsi que sur la qualité de la production législative s'agissant du fait technique »*[449]. Elle met en exergue un phénomène de *« translation du juridique vers le technique »* [450] qui a pour principal cause la dématérialisation et la technicisation du soin et pour principal effet de déplacer l'élaboration de la norme du domaine législatif vers le domaine règlementaire « *la loi est devenue réglementaire*[451] *et la multiplication de textes - parfois rédigés de manière très expéditive - nuit à la cohérence de l'ensemble »*[452].

647. Nous constatons au regard des dernières évolutions de la règlementation et de nos précédents développements, que cette translation est désormais bien affirmée[453] et assumée par le législateur qui, du fait de ses difficultés à appréhender ces spécificités se cantonne à définir les

---

[449] C. ZORN, *op. cit.*,, p. 33, n° 10.

[450] C. ZORN, *op. cit*. p. 293, n° 350.

[451] G. RIPERT, Le déclin du droit, LGDJ, 1949, p. 71.

[452] C. ZORN, *op. cit*. p. 33, n° 10.

[453] Nous avons amplement dépassé ce phénomène de translation, la technologie des *blockchains* en constitue un exemple. Cette technologie repose sur le stockage et la transmission d'informations transparentes et sécurisées ne nécessitant pas dans le cadre de son fonctionnement d'organe central de contrôle. Elle contient l'historique de tous les échanges effectués entre ses utilisateurs et est partagée entre ces derniers, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. Les *blockchains* permettent notamment la mise en œuvre de *smart contracts* qui sont des programmes autonomes ne nécessitant aucune intervention humaine et qui consistent en l'exécution automatique de conditions et termes d'un contrat. Dans le cadre de cette technologie, le programmateur se substituant au juriste dans l'élaboration du contrat, celui-ci n'occupe plus qu'un rôle de conseil.

finalités recherchées ainsi que les valeurs protéger et à confier aux « technocrates » et experts le soin de déterminer les moyens et d'en contrôler le respect ainsi que l'atteinte des objectifs fixés.

648. *« Le développement des systèmes d'information de santé confirme les conclusions de RIPERT sur la prolifération législative : "Les juristes s'effacent devant les technocrates qui ont seuls les connaissances nécessaires pour savoir comment il faut orienter l'économie."*[454] *Il s'agit sans doute d'une explication majeure de la piètre qualité juridique des textes destinés à encadrer l'hébergement des données de santé. »* [455]

649. En conséquence, dans le cadre de la procédure de certification des hébergeurs de données de santé, la loi de modernisation de notre système de santé opère une véritable substitution de la norme industrielle à la norme institutionnelle, les pouvoirs et compétences de régulation sont confiés aux techniciens. Ainsi le Cofrac se voit confié la charge d'accréditer les organismes de certification et l'ASIP

650. Santé, le soin d'élaborer le référentiel ainsi que la procédure de certification comprenant les mesures de contrôle, de suspension et de retrait devant être réalisés par ces organismes.

651. S'agissant d'un sujet aussi technique, nous ne concevons pas cette procédure comme un déclin du droit mais comme un gage de qualité et de sécurité. Cette répartition évite une confusion des genres. Chacun demeure sollicité dans le cadre de son domaine de compétence et il est plus sécurisant que la définition et l'appréciation du respect de normes techniques soient confiées à des spécialistes du domaine concerné. Ainsi, comme nous l'avons précédemment expliqué, la définition du cadre général, c'est-à-dire, des droits et valeurs protégées, des rôles et

[454] G. RIPERT, *op. cit.* p., 156.

[455] C. ZORN, *op. cit*. p. 294, n° 350.

responsabilités des acteurs de la certification demeure de la compétence du législateur[456]. Celui-ci, face au constat de sa difficulté à appréhender l'ensemble d'un sujet de plus en plus complexe, confie à des Autorités administratives indépendantes (AAI), le soin de traduire les finalités qu'il a déterminé en normes techniques. Ces autorités sont composées d'experts des différents domaines concernés ainsi que de juristes qui interviennent au cours du processus d'élaboration des référentiels et des actes réglementaires s'y rapportant. C'est notamment le cas au sein de l'ASIP Santé. Dans le cadre de l'attribution, de la suspension et du retrait des certificats, une étude juridique doit être menée. L'hébergement constituant un traitement de données à caractère personnel relatives à la santé, espérons que celle-ci aboutisse à renforcer les obligations d'information et de coopération et adopte une conception transversale du sujet afin de garantir l'effectivité des droits de la personne et la protection de ses données.

652. De l'archivage de données et d'informations. Au regard des dispositions de l'Ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel [457], nous constatons, en ce qui concerne l'hébergement de données de santé à caractère personnel sur support papier, que les dispositions sont toujours

---

[456] O. VERAN, B. LACLAIS, J.-L. TOURAINE, H. GEOFFROY, R. FERRAND, Rapport préc.

[457] Cette ordonnance vise *« à garantir une meilleure articulation entre les dispositions du code du patrimoine et du Code de la santé publique relatives aux modalités d'externalisation des données de santé, sur support papier ou sur support numérique et, le cas échéant, dans le cadre d'un service d'archivage électronique. Elle vise à assurer une protection équivalente des données de santé quel que soit leur statut (données privées ou données publiques), aussi bien dans le cadre de prestations permettant leur traitement par les professionnels, les établissements et les organismes de santé ou sociaux et médico-sociaux, que s'agissant de prestations d'archivage »* (*Projet de loi ratifiant les ordonnances n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel et n° 2017-29 du 12 janvier 2017 relative aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique, présenté par* M. TOURAINE, Sénat, n° 513, 19 avril 2017).

aussi confuses. En effet, bien que les nouvelles dispositions du (I) de l'article L. 1111-8 du Code de la santé publique porte d'une manière générale sur l'externalisation de l'activité d'hébergement, il y est expressément fait mention de données de santé à caractère personnel et non d'informations. Aussi, comme la relève C. Zorn471[458], le maintien de la mention *« quel qu'en soit le support, papier ou informatique » est extrêmement mal venue au milieu de dispositions qui traitent de données. Le législateur fait ici fi de la doctrine, (…) en ne retenant pas qu'une donnée est « la représentation conventionnelle d'une information destinée à faciliter son traitement »*[459] *et qu'elle est donc une information qui possède une valeur ajoutée d'ordre technologique. Dès lors, "l'hébergement de données sur support papier" n'a pas de sens ».*

653. Outre cette mention inchangée depuis 2009[460], il règne, du fait de la rédaction des dispositions de l'alinéa 2 du (I) de l'article L. 1111-8 et celles des premiers alinéas du (II) et du (III) du même article une confusion. Eu égard à la qualité rédactionnelle de l'ensemble de l'article, ces dispositions peuvent faire l'objet de plusieurs interprétations. Ainsi, si l'activité de l'hébergeur consiste en la conservation de données, sous-entendu stockées sur un support numérique, celui-ci est tenu d'obtenir un certificat de conformité *« délivré par des organismes de certification accrédités par l'instance française d'accréditation. »* [461] Toutefois, si son activité consiste en de l'archivage électronique, il doit être agréé par le ministre chargé de la culture.

654. Il convient donc de s'interroger sur le sens de ces dispositions.

---

[458] C. ZORN, op. cit. p. 258, n° 299.

[459] Arrêté du 22 décembre 1981 relatif à l'enrichissement du vocabulaire de l'informatique, JONC, 17 janvier 1982, p. 624.

[460] Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

[461] C. santé publ, art. L. 1111-8. (II), al. 2.

655. L'hébergeur doit-il, dans le cadre d'une activité d'archivage électronique, à la fois être titulaire d'un certificat de conformité en raison de la nature du support et, le cas échéant, s'agissant d'une activité d'archivage, bénéficier d'un agrément ?

656. Le projet de décret relatif à l'hébergement de données de santé qui vise, d'une part, à adapter les dispositions du décret n° 2006-6 du 4 janvier 2006 aux modifications apportées par la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, et à appliquer les modifications apportées par l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, ne donne pas plus d'indications que l'ordonnance du 12 janvier 2017 pour apprécier si les prestataires proposant un service d'archivage électronique et bénéficiant d'un agrément devront nécessairement obtenir le certificat de conformité mentionné à l'article L. 1111-8, (II) du Code de la santé publique.

657. Les prestations de conservation et d'archivage considérées reposent toutes deux sur une activité d'hébergement externalisé mais elles nécessitent du prestataire, la mise en œuvre de moyens distincts. S'agissant de la conservation de données à caractère personnel relatives à la santé, elles concerne des données collectées ou produites de manière relativement récentes compte tenu des obligations de conservation[462] et, doit permettre, à la différence de l'archivage, le traitement quotidien des données par les professionnels des établissements et les organismes de santé ou sociaux et médico-sociaux. Bien qu'il s'agisse d'assurer une protection équivalente des données de santé, nous pourrions donc considérer, au regard de ces éléments, que l'archivage externalisé, qu'il concerne des informations sur support papier [463] ou des données sur support numérique, constitue une activité à part entière disposant de ses

[462] C. santé publ, art. R. 1112-7.

[463] Décret n° 2011-246 du 4 mars 2011 relatif à l'hébergement de données de santé à caractère personnel sur support papier et modifiant le Code de la santé publique.

propres finalités et normes. A fortiori, les prestataires proposant un service d'archivage électronique pourraient être dispensés de l'obtention d'un certificat de conformité.

658. Eu égard au contenu du rapport relatif à l'ordonnance du 12 janvier 2017, il semble toutefois qu'il n'en soit rien. En effet au sein de ce rapport les conjonctions de coordination et/ou sont simultanément employées afin d'exprimer les conditions d'externalisation des archives. Cet emploi ne nous semble pas anodin, ainsi de là à considérer qu'il témoignerait de la volonté du ministère de la santé que les archives sur support papier soient confiées à un hébergeur agréé et que les archives au format numérique soient confiées à un prestataire certifié et agréé il n'y a qu'un pas.

659. *« L'article 2 de l'ordonnance clarifie l'articulation entre le Code de la santé publique et le code du patrimoine en précisant que l'externalisation des données de santé à caractère personnel ayant le statut d'archives publiques doit être confiée à un hébergeur agréé et/ou certifié dans les conditions de l'article L. 1111-8 du Code de la santé publique. »*[464]

660. Nous constatons également qu'il n'est pas fait mention de l'archivage réalisé sur support papier en ce qui concerne la certification contrairement aux dispositions du (III) de l'article qui laisse supposer que l'hébergeur hébergeant des données sur support papier ne soit soumis qu'à une obligation d'agrément en ce qui concerne les prestations d'archivage. Il n'est par ailleurs fait nullement mention de l'externalisation de prestations de conservation de données sur support papier.

661. Inévitablement, au regard de la distinction entre les notions d'archivage et de conservation, il parait difficile de concevoir que des

[464] Rapport au Président de la République relatif à l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, JORF n°0011, 13 janv. janvier2017, texte n° 16.

professionnels, des établissements de santé ou des établissements et services sociaux et médico-sociaux n'externalisent la conservation d'information à caractère personnel relatives à la santé sur support papier dont ils auraient encore l'utilité dans le cadre de leur activité de soins et alors même que ces données seraient conservées depuis une durée inférieure aux dispositions de l'article R. 1112-7 du Code de la santé publique.

662. En conclusion, C. Zorn exprime dans ses travaux, la nécessité, qu'une réflexion sur les modifications de la législation relative à la conservation des archives médicale soit menée. Eu égard aux nouvelles dispositions de l'article L. 1111-8 du Code de la santé publique et aux nombreux renvois réalisés au sein de ses dispositions au Code du patrimoine ainsi qu'aux dispositions spécifiques à la procédure d'agrément dont les modalités seront fixées par décret en Conseil d'État pris après avis de la CNIL et des conseils des ordres des professions de santé, il semble que ce travail de réflexion ait été mené, le résultat est toutefois perfectible.

663. Il aurait été préférable afin d'en faciliter la lecture, que les dispositions relatives à l'archivage aient fait l'objet d'un article spécifique et que le caractère cumulatif ou alternatif de l'obtention d'un certificat et de la délivrance d'un agrément relatif à l'archivage de données ait été explicitement mentionné dans le texte. Il est, par ailleurs, regrettable que la loi de 2016 qui, d'une manière générale, vise à simplifier et alléger les procédures qui lui sont préexistantes, ne serait-ce qu'en ce qui concerne l'accès aux données du Système national des données de santé ou encore l'appréciation de la capacité d'un prestataire à proposer des prestations d'hébergement de données relatives à la santé ne créée une nouvelle procédure fondée sur un agrément. Ainsi l'objectif consistant à « garantir une meilleure articulation entre les dispositions du code du patrimoine et du Code de la santé publique relatives aux modalités d'externalisation des données de santé, sur support papier ou sur support numérique et, le cas

échéant, dans le cadre d'un service d'archivage électronique »[465] ne nous semble que difficilement atteint. Il conviendrait donc de poursuivre la réflexion afin de simplifier la procédure à l'aune des modifications mises en œuvre en ce qui concerne la procédure d'autorisation de recherche nécessitant le traitement de données à caractère personnel relatives à la santé.

[465] *Projet de loi ratifiant les ordonnances n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel et n° 2017-29 du 12 janvier 2017 relative aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique, présenté par* M. *TOURAINE*, Sénat, 19 avril 2017. .

§ 2. Un renforcement du dialogue avec les responsables

665. À l'occasion de l'entrée en vigueur RGPD, la Présidente de la CNIL, I. FALQUE-PIERROTIN a rappelé, au cours de plusieurs entretiens[466], qu'il ne fallait pas considérer le 25 mai 2018 comme un couperet. Elle a précisé que la mise en conformité au Règlement et le principe de responsabilisation des acteurs devaient être élaborée en collaboration avec les autorités de régulation. La CNIL favorise par ce moyen la concertation avec les institutions mais également le dialogue avec les acteurs mettant ou souhaitant mettre en œuvre des traitements données à caractère personnel. Se faisant, elle se positionne en qualité d'accompagnateur plutôt qu'en tant qu'organe de sanction.

666. Les prémices de ce dialogue existaient déjà à la genèse de la loi de 1978, notamment au sein du décret n°78-774 du 17 juillet 1978[467] qui comportait, dans les dispositions de son article 1, la mission pour la Commission de conseiller *« les personnes et organismes qui ont recours au traitement automatisé d'informations nominatives ou procèdent à des essais ou expériences de nature à aboutir à de tels traitements ».*

667. Cette mission concernait également les plus hautes institutions puisque la CNIL avait également pour obligation de répondre « aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions » et de *proposer « au Gouvernement toutes mesures législatives ou réglementaires de nature à adapter la protection des libertés à l'évolution des procédés et techniques informatiques ».*

[466] Ces informations sont disponibles sur le site de la CNIL. Elles sont consultables à partir de l'adresse suivante : https://www.cnil.fr/fr/rgpd-comment-la-cnil-vous-accompagne-dans-cette-periodetransitoire

[467] Décret n° 78-774 du 17 juillet 1978 pris pour l'application des chapitres I à IV et VII de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

668. Ainsi, ce dialogue était en germe au sein des anciennes dispositions de la loi de 1978 mais il a été renforcé lors de l'adoption de la loi de 2004 au sein de son article 11.

669. Au moment de l'adoption de la loi 2004-801 du 6 août 2004 transposant, en droit français, les dispositions de la Directive de 1995, le législateur a souhaité responsabiliser les acteurs du traitement de données à caractère personnel au moyen de l'autorégulation. Il ne souhaitait pas, par ce détours, éloigner la Commission de tout pouvoir de régulation mais escomptait qu'elle soit conduite *« à s'impliquer dans cette démarche, puisque les professionnels [pourraient] lui soumettre des projets de codes de déontologie, ainsi que des logiciels ou d'autres procédures techniques permettant de contribuer à la protection des personnes dont les données sont traitées »*[468].

670. Fidèle à cette mission de « pédagogie, de communication et de dialogue »[469], *« au risque de résumer la loi de 1978 à un procédé plus rhétorique d'orientation et de modération des comportements, plutôt que d'en faire un réel instrument normatif contraignant »*[470], la CNIL a, en sus, de son rôle d'autorité de contrôle et de sanction, développée une mission d'information, de conseil et d'accompagnement. Elle réalise cette fonction de multiples façons notamment par la sensibilisation du législateur aux thématiques en lien avec l'informatique et les libertés mais aussi par l'accompagnement des responsables de traitement ainsi que la mise à disposition d'outils ou la réalisation d'actions de sensibilisation. La Commission a, de ce fait, pendant longtemps *« préféré informer*

[468] Exposé des motifs de la 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

[469] CNIL, 26e rapport d'activité, 2005, p. 7. Voir également R. PERRAY, « PERREY, Quel avenir pour le pouvoir de sanction de la CNIL ? »,?, *Revue Lamy Droit de l'immatériel*, 2008, n°1, p. 82.

[470] V. GAUTRON, « Fichiers de police », *Répertoire de droit pénal et de procédure pénale*, Dalloz, nov. 2017.

directement les contrevenants des règles à suivre et les a invités fermement et solennellement à se mettre en conformité avec la loi »[471].

671. Le RGPD va au-delà des mesures introduites par la directive européenne de 1995 et à la loi relative à l'informatique, aux fichiers et aux libertés modifiée par la loi de 2016[472], en poursuivant dans cette philosophie et en la développant. Il commue, en conséquence, le système administré en un dispositif en grande partie fondé sur l'autorégulation et ainsi prioritairement sur une logique de responsabilisation et de conformité[473]. De ce fait, sous le contrôle et avec l'accompagnement de la Commission, qui va exercer une fonction à la fois de conseil et de régularisation, le contrôle a priori s'en trouve simplifié et prend une dimension subsidiaire vis-à-vis d'une organisation fondée sur un nouveau principe général de dialogue avec l'autorité de régulation.

672. Attention toutefois à ne pas prendre le raccourci de considérer les obligations déclaratives comme étant abrogées puisque celles-ci continuent à exister pour les traitements constituant un risque pour la vie privée des personnes[474]. Ce changement de paradigme, repose sur plusieurs instruments dont la normativité graduée[475] est particulièrement adaptée au nouvel environnement juridique engendré par le règlement.

673. L'un de ces dispositifs consiste en la réalisation d'une étude spécifique, à la fois juridique et technique afin d'évaluer l'impact d'un traitement sur la vie privé des personnes dont les données à caractère personnel sont traitées. Cette procédure permet de recenser et de décrire les opérations de traitement et d'identifier leurs finalités mais aussi,

---

[471] « Comment la CNIL exerce-t-elle son pouvoir de sanction ? », *Lamy D*roit du numérique, étude 2959, juin 2018.

[472] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

[473] *« La CNIL appelle à la mise en œuvre du règlement sur la protection des données »*, Liaisons sociales Quotidien - L'actualité, nº 17297, 30 mars 2017.

[474] *« Les règlements européens »*, Lamy droit du numérique, étude 373, juin 2018.

[475] *Ibid.*

d'évaluer leur nécessité ainsi que les risques pour les droits et libertés des personnes concernées et enfin de déterminer les sources de ces risques et les mesures envisagées pour les prévenir et les corriger.

674. Pour déterminer si une étude d'impact sur la vie privée est requise, *« il est indispensable de déterminer si le traitement est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques. Tel est le cas notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, etc.) »*[476]. Ainsi, dans le domaine de la santé, s'agissant de traitement de données sensibles susceptibles d'être réalisés à l'échelle d'un territoire de santé ou à l'échelle régionale et/ou qui sont susceptibles de concerner un nombre conséquent d'usagers du secteur de santé, ils sont de nature à engendrer un risque élevé pour les droits et libertés des personnes physiques.

675. En conséquence, les établissements ainsi que les structures de soins sont invariablement soumis à l'obligation de réaliser une étude d'impacts sur la vie privée. En effet, le Parlement a, suite à l'entrée en vigueur du Règlement général sur la protection des données, adopté le 14 mai 2018 un projet de loi relatif à la protection des données personnelles[477], venant modifier les dispositions de la loi de 1978. La loi n° 2018-493 du 20 juin 2018 est venue préciser les cinquante-six renvois aux lois nationales de chaque État-membre de l'Union européenne réalisés par le Règlement afin de leur permettre de réaliser des adaptations avec le droit national pour que celui-ci soit pleinement applicable. À cette occasion, le législateur a, comme le Règlement le lui permettait en ses articles 35 et 36, rappelé le caractère obligatoire de l'analyse d'impacts pour les données sensibles mentionnées au II de l'article 8 de la loi de 1978 modifiée. Les responsables de traitements et sous-traitants mettant en

[476] « Règlement général sur la protection des données », Liaisons sociales Quotidien – Le dossier pratique, n° 101, 2 juin 2017.

[477] On remarquera, au passage, la disparition de la formulation plus correcte de « données à caractère personnel »..

œuvre des traitements ne remplissant pas les conditions de l'article 35 sont également incitées à réaliser une telle étude.

676. Si suite à une analyse le responsable de traitements ou le sous-traitant estime que les mesures qu'il a envisagées pour pourvoir à la protection des données à caractère personnel qu'il escompte traiter sont satisfaisantes, il procède à la validation de son étude. *A contrario*, s'il considère que les mesures projetées ne sont pas de nature à garantir un niveau de protection adapté et qu'un risque subsiste, il doit définir des mesures complémentaires et se livrer à une nouvelle étude. Si après plusieurs analyses le responsable de traitements arrive à la conclusion que les risques qu'il a préalablement identifié ne peuvent être réduits à un niveau acceptable, il doit conformément aux dispositions de l'article 36 du Règlement, consulter la CNIL préalablement à la mise en œuvre effective du traitement concerné, cette dernière pouvant s'y opposer[478].

677. *« Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque. »*[479]

678. Ce n'est donc qu'à titre subsidiaire que le responsable de traitement ou le sous-traitant doit informer la CNIL de l'existence du traitement et des risques résiduels que représente celui-ci pour la protection des données. Si l'autorité de contrôle estime le traitement et non conforme au RGPD, elle en informera le responsable du traitement elle sera par ailleurs tenu de ne pas rendre publique les vulnérabilités de la sécurité du traitement.

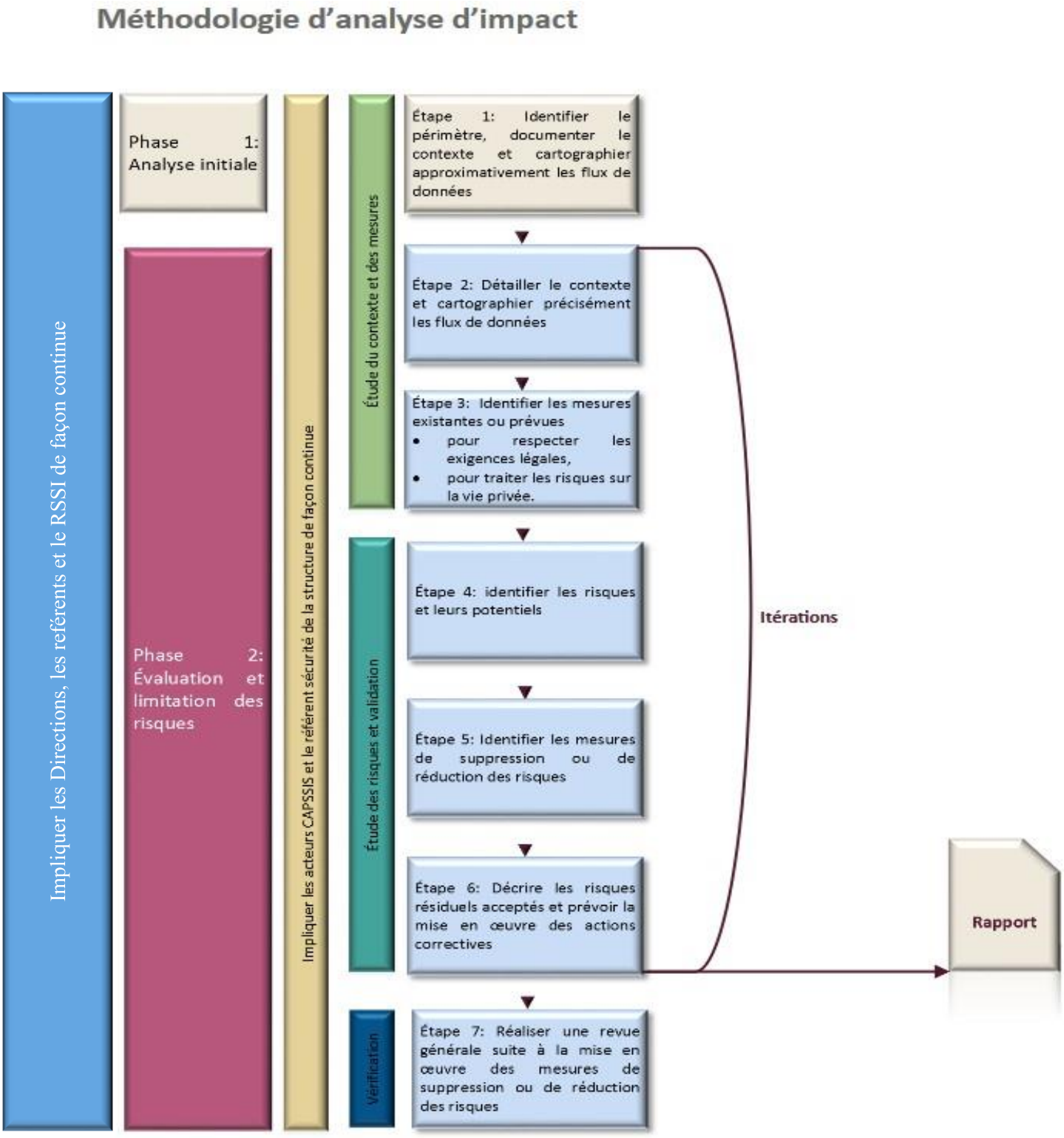
---

[478] *« Règlement général sur la protection des données »*, art. préc.

[479] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 36 (1).

679. Si l'autorité de contrôle estime que le traitement envisagé n'est pas conforme aux dispositions du RGPD, elle l'en informe et l'invite à présenter ses observations et à mettre en œuvre les corrections qu'elle a identifiées. Celles-ci peuvent prendre la forme d'une limitation des données collectées, d'une modification de la durée de conservation, de la mise en œuvre de mesures de sécurité, juridique, logiques, physiques ou organisationnelles.

681.


Méthodologie d'analyse d'impact
Impliquer les Directions, les référents et le RSSI de façon continue
Phase 1: Analyse initiale
Phase 2: Évaluation et limitation des risques
Impliquer les acteurs CAPSSIS et le référent sécurité de la structure de façon continue
Étude du contexte et des mesures
Étape 1: Identifier le périmètre, documenter le contexte et cartographier approximativement les flux de données
Étape 2: Détailler le contexte et cartographier précisément les flux de données
Étape 3: Identifier les mesures existantes ou prévues
pour respecter les exigences légales,
pour traiter les risques sur la vie privée.
Étude des risques et validation
Étape 4: identifier les risques et leurs potentiels
Étape 5: Identifier les mesures de suppression ou de réduction des risques
Étape 6: Décrire les risques résiduels acceptés et prévoir la mise en œuvre des actions correctives
Itérations
Rapport
Vérification
Étape 7: Réaliser une revue générale suite à la mise en œuvre des mesures de suppression ou de réduction des risques

682. Ainsi, à la place d'un système déclaratif imparfait ne comportant pas nécessairement toutes les évolutions liées au traitement ou ne comportant pas les éléments liés au risque, le Règlement favorise une approche effective fondée sur le dialogue dont la déclaration mensongère est sévèrement réprimée. Par ailleurs, dans le cadre des procédures déclaratives, la CNIL avait pris pour habitude de demander de manière quasi systématique des compléments d'informations aux déclarants notamment en ce qui concerne l'analyse de risque et les dispositions prises pour garantir le respect des droits et libertés de la personne, support d'information, architecture technique, procédures et organisation pour l'exercice des droits de la personne. Cette procédure déplace l'analyse auprès du responsable de traitement qui est dans l'obligation d'informer la CNIL de risques résiduels élevés ou susceptibles de se réaliser s'il ne veut pas se voir sanctionner.

683. Loin d'être une simple contrainte, l'étude d'impact sur la vie privée constitue un gage de confiance qui permet au responsable de traitements de revoir les modalités des traitements qu'il met en œuvre et de les améliorer selon les évolutions technologiques, les changements de politique de confidentialité ou encore, à titre d'exemple, l'ajout de finalités susceptibles d'accroitre les risques pesant sur les données et ainsi sur les droits et libertés de la personne.

684. Cette obligation conserve toutefois une dimension coercitive indispensable à son effectivité puisqu'elle s'accompagne d'une sanction suffisamment dissuasive. Ainsi, le non-respect des exigences applicables en matière d'analyse d'impacts sur la vie privée peut donner lieu à des amendes imposées par la

685. Commission. Le fait de ne pas réaliser d'analyse alors que le traitement est soumis à cette obligation [480] ou de menée de manière incorrecte une telle étude ou le fait de ne pas consulter l'autorité de contrôle compétente lorsque la situation l'exige [481] est passible d'une amende administrative pouvant s'élever à dix millions d'euros ou, dans le cas d'une entreprise, jusqu'à deux pourcents du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu[482].

686. **La notification des incidents de sécurité de santé.** l entre le responsable de traitement et les différents acteurs de la protection peut intervenir au cours du traitement suite à un incident de sécurité. Ces événements indésirables mobilisent un nombre considérable d'acteur de la sécurité des systèmes d'information, de la protection des données et de la santé.

687. **Le signalement à la CNIL.** Le Règlement général sur la protection des données impose, au responsable de traitement, à compter de sa date d'entrée en vigueur de procéder au signalement des violations de données à la CNIL. Cette obligation doit intervenir au plus tard dans un délai de 72 heures après avoir pris connaissance de la violation. Lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne concernée, le responsable du traitement en informe ces derniers dans les meilleurs délais. Compte tenu des risques pouvant résulter pour d'une telle violation de données à caractère personnel pour la vie privée de la personne, ces délais nous semble déraisonnables.

688. **Le signalement à l'Agence régional de santé.** la loi de modernisation de notre système de santé a ainsi créé au moyen de son

[480] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 35.

[481] Règl. (UE). PE et Cons. 2016/679, préc. art. 36 (3) (e).

[482] Règl. (UE). PE et Cons. UE 2016/679, préc. art. 83 (4) (a).

article 110 un nouvel article, le L. 1111-8-2 au sein du code de la santé publique. Complété par les dispositions du Décret du 12 septembre 2016[483] cet article impose aux établissements de santé et aux organismes et services exerçant des activités de prévention, de diagnostic, ou de soins de signaler sans délai au moyen d'un portail dédié au signalement des événements sanitaires indésirables[484], à l'Agence régionale de santé, les incidents graves de sécurité des systèmes d'information ainsi que les incidents jugés significatifs. Les incidents significatifs sont transmis par l'ARS aux services de l'Agence des Systèmes d'Information Partagé de Santé. Cette obligation poursuit a pour objectif d'alerter et informer l'ensemble des acteurs de la sphère santé en cas de menaces et d'apporter un appui et un accompagnement aux organismes concernés par la déclaration de ces incidents placée sous la responsabilité du Fonctionnaire en charge de la sécurité des systèmes d'informations (FSSI) A cette fin, le ministère des Solidarités et de la Santé a mis en place une cellule d'accompagnement cyber sécurité des structures de santé (Cellule ACSS).[485]

[483] Décret n° 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information

[484] Ce portail est accessible à l'adresse suivante : http://signalement.social-sante.gouv.fr.

[485] INSTRUCTION N° SG/SHFDS/FSSI/2017/ 281 du 26 septembre 2017 relative au rôle des ARS dans la mise en œuvre du dispositif de déclaration obligatoire et de traitement des signalement des incidents graves de sécurité des systèmes d'information des structures de santé Date

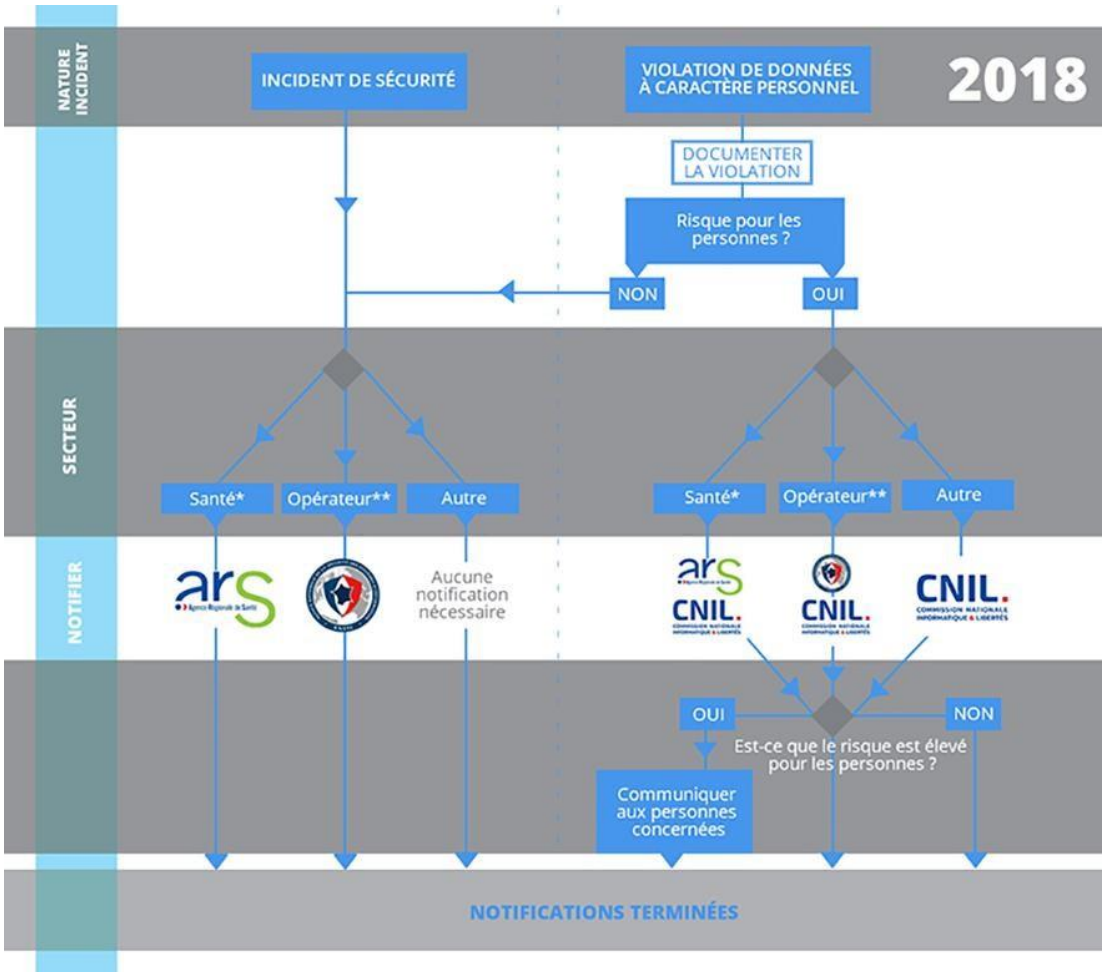


Figure 6Signalement des incidents (Source :CNIL https://www.cnil.fr/fr/notifier-une-violation-de-donneespersonnelles)

Section 2. Un renforcement des pouvoirs de contrôle a posteriori

690. **De véritables pouvoirs de contrôle et de sanction.** Les missions de contrôle de la CNIL ont toujours été essentiellement orientées sur l'appréciation *a priori* de la conformité des traitements projetés. Disposant de moyens inadaptés et d'un cadre réglementaire peu enclin à lui reconnaitre une véritable mission de contrôle *a posteriori.* La Commission ne pouvait se livrer à une véritable appréciation de la conformité des traitements (Paragraphe 1). *« Conscient d'une certaine paralysie de la Commission, le législateur de 2004 est intervenu en renforçant ses pouvoirs d'action, lui permettant d'exercer un contrôle sur la conformité des systèmes de traitements de données. La CNIL s'est ainsi vue attribuer d'importantes prérogatives en matière de contrôle a posteriori. »*[486] Ce renforcement des pouvoirs de contrôle de la Commission s'est accompagné d'une diversification des sanctions (Paragraphe 2) de nature à inciter les responsables de traitement à respecter leurs nouvelles obligations en matière de traitement de données de santé.

§ 1. Une réelle appréciation de la conformité des traitements

691. La CNIL a pour principal objet 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 »*[487].

692. À cet égard, *« elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la (…) loi [relative à l'informatique, aux fichiers et aux libertés] et aux autres dispositions relatives à la protection des données personnelles*

[486] K. RENAUDIN, *Le spamming et le droit – Analyse critique et prospective de la protection juridique des « spammés »*, Thèse, Nancy, 2011, p. 196.

[487] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 1, al. 1.

prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France »[488].

693. La Commission dispose, à cet effet, de nombreux moyens lui permettant de contrôler le respect des dispositions relatives à la protection des données à caractère personnel. Elle peut ainsi examiner tout traitement de données à caractère personnel mis en œuvre, en tout ou partie, sur le territoire français, y compris lorsque le responsable du traitement est établi sur le territoire d'un ou plusieurs autres États membres de l'Union européenne.

694. Initialement, les missions de contrôle de la CNIL étaient essentiellement organisées autour du contrôle préalable. Les effectifs de la Commission dédiées aux opérations de contrôle a posteriori, étaient, par conséquent, réduits à une dizaine de personnes. Elle ne pouvait, de ce fait, apprécier la conformité d'un traitement que pour les déclarants et dans la limite des informations qu'ils avaient préalablement communiqués. L'absence de contrôle a posteriori et la faible appréhension des sanctions par les acteurs économique l'amenaient a fortiori à disposer d'une appréciation tronquée de la conformité des traitements mis en œuvre.

695. Ce n'est qu'avec l'entrée en vigueur de la loi n°2004-801 du 6 août 2004[489] transposant la Directive de 1995 dans notre droit national, que la Commission s'est vue doté de véritables pouvoirs d'enquête. De cette manière, la loi de 2004 à améliorer le niveau de protection des données à caractère personnel et des droits de la personne en rendant plus efficace les opérations de contrôle. Elle a grandement accru les pouvoirs de contrôle de la CNIL, y consacrant un chapitre spécifique, Chapitre VI intitulé « Le contrôle de la mise en œuvre des traitements ». Ainsi, les agents de la

[488] Loi préc. art. 11, I, 2°.

[489] 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.

Commission chargés du contrôle de la conformité des traitements se sont vu confiés de pouvoirs de contrôle sur place et, depuis la loi de 2018, en tout lieu[490], en disposant d'un accès aux matériels et supports sur lesquels sont stockés les informations, mais aussi de pouvoirs de contrôle sur pièces, par ce moyen de contrôle, les membres de la CNIL ainsi que les agents de ses services habilités *« peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie »*[491]. Par ce moyen, ils peuvent recueillir tout renseignement et obtenir par exemple la communication des contrats de sous-traitance informatique, des formulaires de collecte de données et de recueil de consentement, les dossiers papiers et bases de données, les organigrammes, les politiques de sécurité et de confidentialité et les plans de continuité et de reprise d'activité, des procédures de gestion des demandes des personnes concernées, etc. Ils peuvent également accéder aux programmes informatiques et aux données et demander la transcription des documents directement utilisables pour les besoins de l'enquête.

696. Enfin, les membres de la CNIL et les agents de ses services habilités disposent également depuis 2004 de pouvoirs de contrôle d'audition sur convocation sur le fondement de l'alinéa 1 du III de l'article 44 de la loi du 6 janvier 1978, réalisé suite à la convocation des personnes concourent à la mise en œuvre de traitement, qu'il s'agisse du responsable de traitement ou de ses préposés et sous-traitants. Ce contrôle nécessite la réalisation d'une convocation préalable délivrée par la remise en main propre contre récépissé, contre signature ou par acte d'huissier. Ce moyen de contrôle peut paraître moins efficace que les autres procédés mais lorsqu'il est réalisé à titre complémentaire, il permet de corroborer les

[490] La loi de 2018 modifiant la loi de 1978 supprime toute référence aux locaux « à usage professionnel ». Les membres de la Commission et les agents habilités sont désormais en capacité de mener des contrôles en tout lieu, sous réserve de respecter les autres dispositions applicables aux opérations de contrôle et, notamment le droit de s'opposer à un contrôle de la Commission.

[491] Loi n° 78-17 du 6 janvier 1978, art. 44, III, al. 1.

éléments obtenus avec les déclarations des acteurs du traitement et ainsi, d'apprécier la réelle mise en œuvre des mesures décrites dans les documents[492] pris lors du contrôle sur place ou communiquées lors du contrôle sur pièce.

697. Suite à l'adoption de la loi n° 2014-344 du 17 mars 2014 relative à la consommation, dite loi Hamon, modifiant la loi relative à l'informatique, aux fichiers et aux libertés, les agents habilités de la CNIL se sont également vu confier de nouvelles compétences. Ainsi, les agents, dans leurs missions d'enquête, ont pu disposer de la capacité d'effectuer des contrôles en ligne leur permettant *« à partir d'un service de communication au public en ligne, [de] consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations ; ils peuvent retranscrire les données par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle ».*

698. De nombreux traitement de données en ligne ou accessibles en ligne consiste en la réalisation d'opération concernant des données à caractère personnel relatives à la santé ou de données sensibles. Il peut notamment s'agir de services de télémédecine, de géolocalisation de patients à finalité de surveillance médicale, de stockage de données en ligne réalisés par des opérateurs privés, etc.

699. Ce nouveau pouvoir permet aux agents de l'autorité de contrôle d'effectuer des constatations concernant ces traitements, depuis les locaux de la CNIL sans en avoir averti le responsable de traitement. Ils peuvent ainsi vérifier la réelle mise en œuvre des mesures et formalités qui sont déclarées ou documentées et plus spécifiquement la pertinence des

[492] Loi préc. art. 11, 2°, f).

données collectées et le respect du principe de proportionnalité et de spécificité énumérés à l'article 6 de la loi Informatique et Libertés.

700. Ils peuvent notamment contrôler le respect des obligations incombant aux responsables de traitements au titre du chapitre V de la loi de 1978 modifiée et ainsi vérifier l'existence de mentions d'information destinées aux personnes concernées par le traitement de leurs données à caractère personnel [493], la mise en œuvre de mesures de sécurité appropriées ou encore les modalités de recueil de consentement.

701. Par ailleurs, en ce qui concerne les opérations de contrôle en ligne, qui existaient déjà sous l'empire de la loi n° 2014-344 du 17 mars 201,4 les membres de la Commission et les agents de ses services habilités, peuvent désormais réaliser leur mission sous une identité d'emprunt, sans pour autant que la procédure soit déclarée irrégulières.

702. En dehors de ces moyens de contrôle, la CNIL peut également procéder à « toute constatation utile »[494].

703. Malgré l'entrée en vigueur RGPD, les pouvoirs de contrôle de la CNIL demeurent donc relativement inchangés. La Commission disposait déjà de pouvoirs de contrôle, sur place ou à distance, relativement étendus. Ainsi, la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, conformément à la volonté du Gouvernement de simplifier les normes et de lutter contre la sur-transposition des actes européens dans le droit français, simplifie les règles auxquels sont soumis les responsables de traitements et les sous-traitants, tout en maintenant un haut niveau de protection des personnes concernées par la traitement de leurs données à caractère personnel et en apportant, à la marge, des précisions sur les modalités d'exercice des pouvoirs de contrôle par les agents de l'autorité de contrôle. Elle substitue ainsi, dans le respect des

[493] Loi préc. art. 32.

[494] Loi préc. art. 44, III, al. 3.

dispositions du Règlement, un système substantiellement organisé sur la réalisation de contrôles *a posteriori* et fondé sur l'appréciation des risques, par les responsables de traitements et sous-traitants, causés par leurs traitements, aux droits et libertés des personnes concernées, à un système fondé sur un régime administré nécessitant la réalisation de déclarations et d'autorisations préalables.

704. Le RGPD réaffirme et renforce toutefois le pouvoir d'enquête de l'organe de contrôle.

705. Il prévoit également, pour les autorités européennes de protection des données, la possibilité de réaliser des opérations de contrôle conjointes dès lors qu'un traitement concerne les citoyens de plusieurs États membres de l'Union européenne, les autorités de chaque État concerné étant compétentes pour contrôler la conformité des traitements.

706. Afin de se préparer à cette réorganisation de son activité, ce n'est pas moins d'une centaine d'agents de la CNIL qui se sont vu habilités à exercer, en 2018, des missions de contrôle [495] , celles-ci étant essentiellement refondues pour correspondre à un contrôle opéré a posteriori. Ces nouveaux pouvoirs d'enquête permettent aux agents de la Commission nouvellement habilités d'apprécier *in concreto* l'organisation définie par le responsable et les mesures de sécurité ainsi que les moyens matériels et humains mises en œuvre et par lesquels le responsable du traitement et le sous-traitant garantissent l'effectivité des droits de la personne concernée par le traitement de ses données.

§ 2. Une diversification des sanctions

707. **Un vaste panel de sanctions pénales et administratives.** Le Règlement général sur la protection des données présente un vaste panel de sanctions. Il permet aux Etats membres, au moyen de son article 84-1

[495] CNIL, délib. 12 juil. 2018, n° 2018-290, habilitant des agents de la CNIL à procéder à des missions de vérification.

de déterminer le régime des sanctions applicables en cas de violation des obligations en matière de protection des données. Le droit français comporte déjà un véritable arsenal pénal[496] (A). Cependant, les nouvelles sanctions administratives réprimant les manquements aux règles en matière de protection des données à caractère personnel semblent en raison de leur caractère graduel constituer une réponse plus adaptée (B)

A. La permanence de la sanction pénale

708. L'Union européenne n'a pas vocation à supplanter les États membres en matière pénale. Ceux-ci restent souverains. Toutefois, le traité sur le fonctionnement de l'Union européenne (TFUE) qui met fin à l'organisation en piliers accroit considérablement les compétences du Parlement européen et du Conseil de l'Union européenne dans ce domaine. Ainsi, l'article 83 paragraphe 1[497] prévoit que l'Union peut adopter des directives établissant des règles minimales concernant la définition des infractions pénales, à condition que cela concerne des domaines de criminalité particulièrement graves revêtant une dimension transfrontalière, tels que la criminalité informatique. En dehors de tous domaines de criminalité grave présentant un caractère transfrontalier, le paragraphe 2 de ce même article 83 prévoit également que l'Union européenne peut définir, dès lors qu'il s'agit de garantir le respect d'une politique harmonisée au niveau européen, les infractions pénales et leurs sanctions. C'est notamment le cas en matière de protection des données à caractère personnel dont l'efficience est dépendante des conditions de mise en œuvre de la règlementation de la part des États membres.

709. Il est, par conséquent, regrettable que le Parlement européen et le

710. Conseil de l'Union européenne n'est pas profité de cette volonté d'assurer une sécurité juridique uniforme dans l'ensemble de l'Union pour

[496] C. pén. art. 226-16 à 226-24.

[497] Version consolidée du Traité sur le fonctionnement de l'Union européenne (TFUE), *JOUE*JO C 115C115, 9 mai 2008, art. 83, § 1.

définir les infractions et sanctions pénales à la réglementation relative au traitement de données à caractère personnel.

711. Ainsi, la réponse pénale n'entre pas dans le champ du règlement qui se cantonne à inciter les États-membres de l'Union européenne à mettre en œuvre, en cas de violation grave du règlement, des sanctions, pénales *« effectives, proportionnées et dissuasives »*.

712. *« Les États membres devraient pouvoir déterminer le régime des sanctions pénales applicables en cas de violation du présent règlement, y compris de violation des dispositions nationales adoptées en application et dans les limites du présent règlement. Ces sanctions pénales peuvent aussi permettre la saisie des profits réalisés en violation du présent règlement. Toutefois, l'application de sanctions pénales en cas de violation de ces dispositions nationales et l'application de sanctions administratives ne devrait pas entraîner la violation du principe ne bis in idem tel qu'il a été interprété par la Cour de justice. »*[498]

713. Lors de la révision de la loi relative à l'informatique, aux fichiers et aux libertés, le législateur français n'a toutefois pas profité de cette opportunité afin de compléter le champ des infractions pénales et de proportionner les sanctions aux atteintes. D'une manière générale, la CNIL a averti du risque consistant « à n'opérer que des modifications "a minima" (…) et à renvoyer la réécriture d'ensemble de la loi du 6 janvier 1978 à une ordonnance ultérieure »[499].

714. Ainsi, la sévérité de la sanction pénale n'a pas évoluée depuis la création de l'article 226-16-1-A du Code pénal. La volonté du législateur était originellement de garantir, au moyen de la loi de 2004, transposant dans le droit national français la directive de 1995, une meilleure

[498] Règl. (UE). PE et Cons. UE 2016/679, préc. considérant 149.

[499] CNIL, délib. 30 nov. 2017, n° 2017-299, portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la Loi n° 78-17 du janvier 1978.

protection des données à caractère personnel en ayant recours à la dissuasion par l'aggravation des peines. Toutefois, cette mesure modificative de la loi de 1978, a conduit à une uniformisation excessive des peines encourues. Le professeur J. FRAYSSINET l'observait déjà en 2009[500], bien que chacune de ces infractions présente un degré de gravité distinct, elles ne sanctionnent plus les manquements les plus graves aux principes instaurés par la règlementation relative à la protection des données à caractère personnel.

715. De ce fait, quelle que soit la valeur sociale protégée atteinte ou les caractéristiques de l'infraction, qu'elle revête un caractère purement formel ou qu'elle constitue une atteinte grave à un droit de la personne, elle se trouve systématiquement sanctionnée d'une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende. Cette situation est révélatrice du décalage entre le contenu des textes et la nécessité de sanctionner les comportements illicites.

716. Il ressort, selon nous, de cette constance du législateur vis-à-vis de la réponse pénale et *a contrario*, de l'évolution ponctuelle des pouvoirs et sanctions à disposition de la CNIL, une volonté de préserver la sanction pénale mais de lui attribuer le rôle d'une réponse exceptionnelle. Ainsi, la combinaison du règlement, de la réforme de 2018 et du nombre dérisoire de contentieux en la matière démontre que les règles et principes de la protection des données à caractère personnel sont envisagés par le droit pénal mais que le législateur français, les institutions et le justiciable privilégie, au détriment de celui-ci, la procédure et la sanction administrative, le privant, par ce moyen, de tout rôle de régulation.

717. *« Ce n'est pas l'exercice effectif de son pouvoir de sanction qui lui a permis, au fil des années d'asseoir son autorité. »*

[500] J. FRAYSSINET, « La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée en bois », Legicom, avril 2009, n° 42, p. 33

718. Cette revalorisation a également été fortement critiquée par Agathe Lepage[501]. Toutefois, lors de la réforme de 2004, la CNIL ne s'est pas montrée favorable à la pondération des sanctions considérant qu'une telle initiative pourrait altérer l'esprit de la réforme et laisser à penser que la protection des données à caractère personnel et la privée représenteraient désormais une moindre valeur[502].

719. Eu égard à la mise en perspective par laquelle C. Zorn met en avant *« la disproportion entre la sanction des infractions en matière de traitement de données à caractère personnel et d'autres infractions à identité de valeurs protégées »*[503] notamment *« l'homicide involontaire [qui] est puni de trois ans d'emprisonnement et de 45 000 euros d'amende »*[504], cette absence de graduation de la sanction nous parait également regrettable. Elle aboutit à substituer au droit pénal une réponse administrative et à réserver l'application d'une peine privative de libertés à quelques recours exceptionnels.

720. Ainsi, il aurait été souhaitable à l'occasion de la réforme de la loi de 1978 de revenir à la situation antérieure à la réforme de 2004 et ainsi à un système qui laisserait coexister des peines plus ou moins sévères en fonction des infractions considérées.

721. Toutefois, ces propos doivent être nuancés, s'agissant d'atteintes résultant de fichiers ou de traitements informatiques, il paraît raisonnable de recourir à une juridiction d'exception[505] susceptible de faire cesser

---

[501] A. LEPAGE, « 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 », *Dr. pénal* 2005, chron. 5.

[502] CNIL, avis, 26 septembre 2000, relatif au projet de loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, spéc. p. 11..

[503] C. ZORN, *op. cit*. p. 215, n° 237C..

[504] *Ibid.*

[505] CE, 19 fév. 2008, Profil France, n°311974, Inédit : « *Eu égard à sa nature, à sa composition et à ses attributions [la CNIL] peut être qualifié[e] de tribunal au sens de l'article 6-1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentale »*

rapidement le trouble y compris sur ces propres. En ce sens, la CNIL ne disposait initialement pas de véritables moyens coercitifs. Ses pouvoirs étaient limités à la formulation d'avertissements ainsi qu'à la dénonciation, au parquet, des infractions dont elle avait connaissance[506]. Ainsi, les suites données aux dénonciations résultaient de l'appréciation de l'opportunité de poursuivre, réalisée par le procureur de la République et de l'issue d'un hypothétique procès. Le recours à la réponse pénale n'était, par conséquent pas adapté à cette forme de délinquance et aux atteintes susceptibles de résulter de la constitution de fichiers. Celles-ci nécessitent, en effet, une réponse souple et rapide, ainsi que l'application de mesures proportionnées et dissuasives compte tenu de la portée des atteintes susceptible de résulter de la dématérialisation.

722. Ce n'est qu'à partir de 2004 que la Commission s'est vu attribuer, par le législateur de nouvelles compétences et de véritables pouvoirs de contrôle et de sanction étendus. Ainsi, l'article 7 de la 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 est venu modifier l'article 45 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

723. Le RGPD diversifie le panel des sanctions administratives susceptibles d'être prononcées par les autorités de contrôle. Il affermit également leur caractère proportionnel afin de permettre le choix des mesures les plus adaptées en fonction de la gravité des manquements. Les mesures prononcées peuvent aller du simple rappel à l'ordre à une amende de quatre pourcents du chiffre d'affaires annuel mondial total de l'exercice précédent. Elles peuvent par conséquent être adaptées par l'autorité de contrôle à la mesure du (co)responsable du traitement ou du sous-traitant et à la gravité du manquement ou de la violation. Elles présentent, par

[506] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 11, I, 2°, e).

conséquent, un caractère dissuasif y compris pour les GAFA [507] et transnationales.

B. La graduation des sanctions administratives

724. Le RGPD a affermi les obligations des responsables de traitements et des sous-traitants, corrélativement, il a singulièrement étoffé l'arsenal des sanctions susceptibles d'être prononcées par la CNIL. Celle-ci doit désormais, dans le cadre de son rôle de contrôleur, faire preuve de vigilance, de dissuasion et de fermeté et ainsi prononcer des amendes administratives suffisamment dissuasives. Ces sanctions pécuniaires qui peuvent être prononcées à l'issue d'un processus progressif sont graduelles, et varient en fonction de la gravité des violations des obligations du Règlement.

725. L'article47 de la loi de 1978, antérieurement aux modifications apportées par la loi n°2016-1321 du 7 octobre 2016, comportait un plafond rendant les amendes infligées dérisoires lorsque le responsable de traitement condamné disposait des capacités financières conséquentes.

726. Ce plafond d'un montant de cent cinquante mille euros ne pouvait excéder trois cents mille euros en cas de récidive ou, « s'agissant d'une entreprise, cinq pourcents du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 euros »[508]. À titre d'exemple, le 3 janvier 2014[509] et le 27 avril 2017[510] la société Google s'était vue infligée,

[507] GAFA est un acronyme désignant les quatre géants américains de l'Internet fixe et mobile que sont Google, Apple, Facebook et Amazon. Ces firmes possèdent un pouvoir économique et financier considérable, supérieur à celui de beaucoup d'Etats. Etat. Ainsi, les sanctions jusqu'ici applicables n'étaient pas suffisamment dissuasives pour les contraindre au respect de la règlementation relative à la protection des données à caractère personnel.

[508] Loi n°78-17 du 6 janvier 1978, art. 47.

[509] CNIL, délib. 3 janv. 2014, n° 2013-420.

[510] CNIL, délib. 27 avril 2017, SAN-2017-006.

par l'autorité de régulation, deux amendes d'un montant de cent cinquante mille euros chacune. Ces sanctions financières sont insignifiantes lorsque l'on sait que cette société réalise, toutes les deux minutes, un chiffre d'affaire légèrement supérieur à cent cinquante mille euros.

727. Le législateur français, prenant acte du déséquilibre dans le rapport de force et de l'ineffectivité de la loi avait récemment simplifié et augmenté ce plafond, au moyen des dispositions de l'article 64 de la loi pour une République numérique[511] en le portant à un montant de trois millions d'euros. Ce plafond, d'un montant supérieur, avait notamment permis à la CNIL de prononcer à l'encontre de la société Optical Center une amende record de deux cent cinquante mille euros[512]. Cette sanction légèrement plus dissuasive n'était pas encore satisfaisante compte tenu du poids économique des contrevenants.

728. Le Règlement va donc au-delà de cet ordre de grandeur puisqu'il permet, à la Commission, de prononcer des amendes administratives pouvant atteindre un montant de dix millions d'euros ou deux pourcents du chiffre d'affaire annuel mondial ou selon les manquements, vingt millions d'euros ou quatre pourcents du chiffre d'affaire annuel mondial, le montant le plus élevé étant retenu.

729. Les montant prévu étant des plafonds, l'article 83 pose une liste de conditions permettant à la CNIL d'adapter les sanctions à la gravité du manquement. Ces conditions constituent une déclinaison de grands principes issus du droit pénal tels que les principes de personnalisation et de proportionnalité de la peine. La graduation de l'amende administrative repose essentiellement sur ces deux principes, le principe de personnalisation étant fondé sur l'article 8 de la Déclaration des droits de l'homme et du citoyen de 1789 qui dispose que « la loi ne doit établir que des peines strictement et évidemment nécessaires ». Ce principe, en droit

[511] Loi n°2016-1321 du 7 octobre 2016.

[512] CNIL, délib. 7 mai 2018, n° SAN-2018-002.

français, a été étendu par le Conseil constitutionnel a toute sanction présentant le caractère d'une punition, voir en ce sens le considérant 15 de la Décision n° 87-237 DC du 30 décembre 1987.

730. *« Considérant que le principe ainsi énoncé ne concerne pas seulement les peines prononcées par les juridictions répressives mais s'étend à toute sanction ayant le caractère d'une punition même si le législateur a laissé le soin de la prononcer à une autorité de nature non judiciaire. »*[513]

731. Ce principe issu du paragraphe 1 de l'article 83 impose que la sanction soit adaptée à la gravité du manquement reproché. Ainsi, s'agissant du plafond le plus élevé pour lequel la Commission peut imposer une amende de vingt millions d'euros ou de quatre pourcents du chiffre d'affaire annuel mondial, celle-ci peut être prononcée lorsque le responsable de traitement ne respecte pas les principes dits de base relatifs aux traitements de données à caractère personnel et qui sont principalement énumérés aux articles 5, 6, 7 et 9. À titre d'exemple, est concerné par ce manquement, le fait de mettre en œuvre un traitement de données de santé à caractère personnel en dehors des exceptions limitativement énumérées au paragraphe 2 de l'article 9.

732. La CNIL peut également prononcer cette sanction en cas de non-respect des droits des personnes notamment en ce qui concerne, l'information préalable, ainsi que les droits d'accès de rectification et à la portabilité figurant aux articles 44 à 49 du Règlement. Enfin, le fait de ne pas se conformer aux injonctions ordonnées par la CNIL est également susceptible de conduire au prononcé de cette amende, article 58 du Règlement.

733. En ce qui concerne le plafond le moins élevé, l'amende peut être formulée en cas de non-respect des principes de « privacy by design », «

[513] Cons. const.,. 23 juillet 1999, 99-416 DC.

privacy by default » consistant, par exemple, en la minimisation des données traitées et à la limitation de la durée de conservation, article 25 ou encore de *« privacy impact assessment »* conduisant à l'absence de mesures effectives permettant une protection des données dès la conception et par défaut. Peuvent ainsi faire l'objet d'une amende de dix millions d'euros ou de deux pourcents du chiffre d'affaire annuel mondial la mise en œuvre de mesures de sécurité insuffisantes, article 32 du Règlement. La CNIL peut également prononcer cette amende en l'absence de clauses relatives aux obligations découlant du Règlement dans les contrats conclus entre le sous-traitant et le responsable de traitements. Est également concerné par cette sanction, la notification tardive ou l'absence de notification à la CNIL et à la personne concernée, articles 33 et 34, ou encore la non désignation d'un délégué à la protection des données, lorsque sa désignation est obligatoire, article 37 du RGPD.

Amendes	10 m[n] € ou 2% du CA annuel mondial	20 m[n] € ou 4% du CA annuel mondial
735. Dispositions concernées	**Art. 25 -** Non-respect des principes de *« privacy by design » et de « privacy by default »*	**Art. 6 à 9 -**
	Art. 32 – Mise en œuvre de mesures de sécurité insuffisantes **Art. 28 –** Absence de clause dans les contrats de sous-traitance	**Art. 12 à 22 –** Non-respect des droits de la personne concernée par le traitement de ses données à caractère personnel
	Art. 30 – Non tenue d'un registre des activités de traitement **Art 35 –** Absence de réalisation d'étude d'impact sur la vie privée **Art. 37 –** Non désignation d'un Délégué à la protection des données	**Art. 58 –** Non-respect des injonctions ordonnées par la CNIL
	Art. 33 & 34 – Non-respect des obligations notification	

736. Ces amendes peuvent être prononcées à titre principal ou subsidiaire, article 83 paragraphe 2 à l'encontre du responsable de traitements ou d'un sous-traitant qui n'aurait, par exemple, pas désigné un délégué à la protection des données lorsque sa désignation est obligatoire. La CNIL dispose, en effet, d'autres instruments dont elle peut faire un usage adapté à la gravité des manquements constatés, afin de faire respecter les obligations découlant du Règlement.

737. Pour décider du montant de l'amende administrative, la Commission doit dûment tenir compte de la portée conférée au principe de proportionnalité ainsi que de trois principaux éléments, le premier étant la nature du traitement et des conditions de sa mise en œuvre, notamment de sa finalité, de la catégorie de données à caractère personnel concernées par la violation ainsi que du nombre de personnes affectées et du dommage qu'elles ont subi, le deuxième étant le comportement du responsable de traitement et du sous-traitant notamment concernant le caractère intentionnel ou non intentionnel de la violation et leur degré de responsabilité, et enfin des mesures qu'ils ont prises pour atténuer le dommage subi par les personnes dont les données sont traitées. Enfin, la Commission va également tenir compte des circonstances de l'espèce, tels que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

738. À titre d'exemple[514], en 2017, la CNIL avait prononcé plusieurs sanctions relatives à un manquement aux dispositions de l'article 34 de la loi du 6 janvier 1978 modifiée relatives à l'obligation de sécurité et de confidentialité des données à caractère personnel. *In casu*, la CNIL avait été informé qu'un traitement de données à caractère personnel mis en œuvre par la société Hertz était accessible en ligne. Le site de la société Hertz France dont l'activité consiste en la location de véhicules aux particuliers et aux professionnels avait donc fait l'objet d'un contrôle en

[514] CNIL, délib., 18 juil. 2017, n° SAN-2017-010 FRANCE.

ligne. À l'issue de ce contrôle, la Commission avait pris contact avec la société pour l'informer de l'existence d'une violation de données à caractère personnel sur ce site.

739. En l'espèce, la formation restreinte avait pris en considération le comportement du responsable du traitement et, plus particulièrement, la bonne coopération de la société Hertz avec la délégation de la Commission. Elle avait également tenu compte de la rapidité de sa réaction ainsi que la mise en œuvre de mesures de sécurité suffisantes.

740. La formation restreinte note, toutefois, que la société a réagi rapidement dès qu'elle a eu connaissance de la violation de données en alertant son sous-traitant et qu'il a été mis fin à la violation de données dans un délai très bref. Elle a également souligné le caractère non intentionnel de la violation ainsi que de l'étendue du dommage.

741. *« Elle prend également acte de ce que l'incident de sécurité est la conséquence d'une erreur humaine qui ne semble pas avoir donné lieu à une extraction massive de données par des tiers non autorisés. »*

742. Toutefois, la violation de données à caractère personnel des adhérents résultant *« d'une négligence de la société dans la surveillance des actions de son sous-traitant »*, la CNIL a estimé que la violation aurait aisément pu être évitée par la réalisation de vérifications d'usages auprès du sous-traitant.

743. La formation restreinte a ainsi adapté la sanction en prononçant une amende pécuniaire d'un montant modeste. Cependant, eu égard à la négligence dont le responsable de traitement a fait preuve dans le suivi des actions de son sous-traitant et de l'incidence de son inaction sur l'accessibilité des données à caractère personnel, elle a toutefois décidé de prononcer la publicité de sa décision.

744. *In fine* les institutions européennes ont tenu compte des critiques formulées à l'encontre des anciens actes communautaires et des

précédentes lois nationales concernant la proportionnalité des amendes prononcées à l'encontre des responsables de traitements en donnant toute sa valeur au principe de proportionnalité permettant d'adapter la peine aux circonstances de l'espèce et aux moyens économiques des responsables de traitements et, désormais, des sous-traitants. Par ce moyen, l'effectivité et l'efficience de la protection des données et des droits de la personne concernée par un traitement de données à caractère personnel s'en trouve affirmés.

CONCLUSION DU CHAPITRE 2

745. **Un contrôle inadapté mais nécessaire.** Le contrôle a priori ne constituait pas, pour la CNIL, un moyen lui permettant d'apprécier la réalité des mesures mises en œuvre par le responsable de traitement pour assurer la protection des données à caractère personnel relative à la santé. En raison des délais de traitement des demandes, le système déclaratif représentait un frein au développement de projets de santé et un obstacle à la circulation de l'information. Sa suppression semble toutefois préjudiciable puisqu'il prive la Commission d'un pouvoir de contrôle de la licéité des traitements.

746. **Une réorganisation du contrôle répondant aux enjeux.** La mise en œuvre de sanctions administratives graduées ainsi que la responsabilisation des acteurs constituent une véritable avancée favorisant la circulation des données de santé et permettant de renforcer leur sécurité ainsi que les droits des personnes en adaptant la réponse juridique et technique aux risques et aux atteintes.

747. Le renforcement du dialogue avec le responsable de traitement constitue le second apport de la réforme car il concrétise la philosophie du Règlement général à la protection des données en permettant de ne pas incliné entre la disponibilité de l'information et la protection des personnes. Il permet en cas de risque résiduel de faire intervenir l'autorité de contrôle afin de déterminer la réponse la plus adaptée.

748. Ce dialogue permet également à la Commission de connaitre, lors de la réalisation d'incidents de sécurité, les risques qui pèsent sur les données tout en apportant une assistance au responsable de traitement. Il est toutefois regrettable que cette obligation de signalement ne soit pas uniformisée afin que les responsables de traitement bénéficient d'un

interlocuteur unique. Cette situation nous semble de nature à nuire à la qualité des informations remontées mais aussi à l'effectivité de cette obligation et à la gestion des incidents.

CONCLUSION DU TITRE II

749. **Une protection préventive.** Le Règlement général sur la protection des données à caractère personnel, introduit une protection de la donnée qui ne repose pas exclusivement sur le contrôle et la sanction. Celle-ci doit être envisagée par défaut et dès la conception des traitements. Elle se traduit par la mise en œuvre d'une organisation responsable ainsi que la mise en œuvre de mesures techniques et juridiques adaptées aux risques et permettant à la personne de pouvoir exercer ces droits.

750. **Une protection contrôlée et sanctionnée.** La protection des données et des personnes vis-à-vis des traitements est assurée par la CNIL dont les pouvoirs d'enquête et de contrôle ont été renforcé afin de lui permettre de constater par elle-même les manquements et de les sanctionner proportionnellement à la gravité du manquement constaté ainsi qu'au capacités financières du responsable du traitement négligeant.

CONCLUSION DE LA PARTIE I

752. **Une protection originale pour une donnée disponible.** Avec le développement des technologies, la vigilance accordée à la protection de l'information relative à la santé doit être renforcée.

753. Le secret professionnel constitue un moyen de protection éprouvé. Cependant, il doit désormais s'accompagner de mesures spécifiques, adaptée aux risques qui pèsent sur l'information en raison de sa numérisation.

754. Le Règlement général sur la protection des données permet d'apporter cette protection complémentaire sans pour autant restreindre la disponibilité de la donnée de santé. Par une nouvelle approche il inscrit la protection des données à caractère personnel relatives à la santé dans la durée en responsabilisant l'ensemble des acteurs auxquels appartient la personne concernée par le traitement.

DEUXIEME PARTIE LA CIRCULATION : UN NOUVEAU PRINCIPE

755. **La circulation au cœur du système de santé.** La loi du 4 mars 2002 en plaçant le patient au centre du dispositif de soin, a créé les conditions propices au partage d'informations. Ainsi, ces dernières années notre système de santé s'est progressivement réorganisé afin de répondre à cette nouvelle conception du soin. Le partage d'informations entre professionnels qui participent à la prise en charge d'une même personne s'est progressivement imposé comme un principe incontournable du soin et de la coordination des professionnels. Il constitue désormais un nouveau principe de santé publique (Titre 1). Corrélativement, sous l'influence du droit communautaire, la réglementation relative à la protection des données à renforcé les droits de la personne sur ses données à caractère personnel. L'autodétermination informationnelle constitue désormais l'un des fondements de cette protection. Elle permet à la personne, en dehors de toute prise en charge par le système de santé, de consentir au traitement de ses données. Avec la démocratisation des outils numériques liés au bien-être et à la santé et leur appropriation par le grand public, cette disponibilité de la donnée a permis le développement d'une nouvelle forme de santé personnalisée (Titre 2), dans laquelle l'individu devient l'unique acteur mais peut en contrepartie perdre la maitrise de ses données.

TITRE I. UN NOUVEAU PRINCIPE DE SANTE PUBLIQUE

« *Le développement des nouvelles technologies de l'information et de la communication dans les domaines sanitaire et médico-social ainsi que des modes d'exercice pluridisciplinaire accroissent le besoin d'échange dans l'intérêt d'une meilleure prise en charge des personnes. Les données de santé et les données médicosociales sont aujourd'hui des données destinées à être partagées, même si elles relèvent de la vie privée de la personne »* [515]

757. Les données circulent entre les professionnels des champs sanitaires, sociaux et médico-sociaux bouleversant l'organisation coutumière du soin dans l'objectif d'assurer la meilleure prise en charge possible de la personne (Chapitre 1).

758. Cette donnée auparavant difficilement accessible semble être désormais disponible. Elle constitue une richesse informationnelle pour des acteurs parfois bien éloignés de la personne prise en charge et de la relation de soins. Ces personnes parfois motivés par des intérêts privés peuvent contribuer en raison d'une utilisation contrôlée de la donnée à l'intérêt collectif et à la santé publique (Chapitre 2).

[515] *« Le cadre juridique du partage d'informations dans les domaines sanitaire et médico-social: état des lieux et perspectives »*, ASIP Santé, 22 août 2012 (http://esante.gouv.fr/services/reperesjuridiques/le-cadre-juridique-du-partage-d-informations-dans-les-domaines-sanitaire)

CHAPITRE 1. LE PRINCIPE EXPANSIF DU SECRET PARTAGE

759. Pour améliorer la prise en charge de la personne et l'efficience des parcours de soins, la mutualisation des informations relatives à cette personne et à la pathologie est essentielle. Il répond à la nécessité de coordonner les professionnels intervenant auprès de la personne prise en charge qui appartiennent aux champs du sanitaire, du social et du médico-social. Le décloisonnement des soins favorise l'échange et le partage d'informations (Section 1). Celui-ci est motivé par une recherche d'efficience et de qualité (Section 2).

761. Section 1. Un décloisonnement des soins

762. *« Le champ de la santé est indéniablement entré dans l'ère du partage et de la collaboration, qui est aussi celui de l'équipe, de la spécialisation, du glissement des tâches, de la complémentarité, du recours à l'équipement. Ces métamorphoses exigent une volonté de pluridisciplinarité et de transdisciplinarité. Pour autant, les "cultures" propres à chaque secteur originel, les logiques particulières à chaque profession, voire parfois les enjeux et réflexes corporatistes ne peuvent s'effacer par la seule émergence de textes et de cadres nouveaux. On s'aperçoit alors que, sur le champ particulier l'information et du secret, les "traditions identitaires ont "la vie dure". Il apparaît donc nécessaire de promouvoir l'idée de partage, de développer les actions conjointes et coordonnées en faveur de la personne. »*[516]

763. Nous l'avons précisé en introduction de nos travaux, le secret professionnel a été codifié au sein du code pénal dès 1810. Il a connu au fur et à mesure plusieurs dérogations lorsque des intérêts jugés supérieurs l'exigeaient. À l'occasion de la loi du 4 mars 2002 le législateur a inséré au sein du code de la santé publique, un article L. 1110-4 érigeant par ce moyen, le secret professionnel au rang des droits de la personne : *« toute personne prise en charge par un établissement de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et aux informations la concernant.»*

764. Cet article admet également une dérogation circonstanciée au secret professionnel, le secret partagé.[517] *« Lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé, les*

[516] F. VIALLA, « *Perspectives pour une culture commune du secret et de l'information partagée* », Juris associations 2013, n° 474, p. 30.

[517] Loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

informations la concernant sont réputées confiées à l'ensemble de l 'équipe ».

765. Le 2 décembre 2013[518] dans le cadre du projet pilote du parcours de santé PAERPA [519] un décret est venu instauré un dispositif dérogatoire[520] autorisant les professionnels de santé et du champ social et médico-social à échanger des informations de santé, sociales et administratives strictement nécessaires à la détermination de la meilleure prise en charge possible de la personne âgée subissant de graves atteintes cognitives ou de lourdes pertes d'autonomie fonctionnelle. Cet échange était subordonné à l'obtention du consentement exprès et éclairé de la personne, recueilli par tous moyens, y compris sous forme dématérialisée. Cette extension temporaire dont le périmètre était limité au cadre décrit dans le décret a constitué la première pierre du décloisonnement de l'échange d'informations.

766. La loi de modernisation de la Santé du 26 janvier 2016, ainsi que le décret du 22 juillet 2016 semble aller beaucoup plus loin que le pilote PAERPA et définir un nouveau cadre juridique de partage d'informations inter-catégoriel en modifiant les dispositions de l'article L. 1110-4 du Code de la santé publique. Ainsi, le "secret partagé" est désormais ouvert aux professionnels du champ social et médico-social. Ce décloisonnement progressif a permis à l'information de circuler au –delà du cercle initial des partageants (Paragraphe 1) et ainsi de permettre aux professionnels de s'inscrire dans de nouvelles formes d'exercice (Paragraphe 2).

---

[518] Décret n° 2013-1090 du 2 décembre 2013 relatif à la transmission d'informations entre les professionnels participant à la prise en charge sanitaire, médico-sociale et sociale des personnes âgées en risque de perte d'autonomie

[519] Personnes âgées en risque de perte d'autonomie)

[520] Loi n° 2012-1404 du 17 décembre 2012 de financement de la sécurité sociale pour 2013, art. 48, IV, et Décret n° 2013-1090 du 2 décembre 2013 relatif à la transmission d'informations entre les professionnels participant à la prise en charge sanitaire, médico-sociale et sociale des personnes âgées en risque de perte d'autonomie.

767. § 1. La circulation de l'information au-delà du cercle des partageants

768. **Les origines du secret partagé, la reconnaissance légale**. Pendant longtemps la violation du secret professionnel n'a connue 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 pu l'admettre dans le secteur hospitalier, car *« 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. »*[521]

769. La relation de soin est, dans ce cadre précis, conçue comme liant l'établissement et le malade[522]. À l'occasion de la loi du 4 mars 2002 le législateur a consacré la pratique et l'a étendu à la médecine de ville. En effet, 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*

[521] M. Couturier (M. Couturier, *Pour approche fonctionnelle du secret professionnel,op.cit.*,n° 174) à propos de l'arrêt CE 11 février 1972 (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).

[522] 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.

»[523]. Seuls les professionnels de santé pouvaient échanger des informations relatives au patient.

770. **Une extension légale du partage avec les professionnels du secteur social et médico-social.** Lorsque nous avons expliqué la généralisation du secret professionnel à tous les intervenants du système de santé[524], - à l'occasion de la loi du 4 mars 2002[525]- il avait été fait mention de la logique qui consistait à rapprocher la prise en charge sanitaire et la prise en charge sociale ou médico-sociale. Cette stratégie d'amélioration de la prise en charge était menée par le gouvernement depuis la loi « HPST »[526] 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. Il faudra 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, le texte prévoit désormais qu'*« 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. »*[527]

771. Le partage est strictement encadré et le même article distingue entre deux types de prise en charge en équipe de soin où hors équipe de soin. Dans la première situation, les informations peuvent être échangées ou partagées sans que le consentement de la personne concernée ne soit

[523] C. santé publ art. L. 1110-4 al. 3.

[524] V. *supra* n°

[525] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

[526] Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

[527] C. santé publ art. L. 1110-4 II.

sollicité, tandis que dans l'hypothèse où les professionnels prenant en charge la personne ne forme pas une équipe de soin le partage est conditionné au consentement de la personne concernée par les informations. Cette distinction recèle quelques subtilités qu'il convient d'analyser.

772. **Le Cadre général de l'échange et du partage.** Tandis que le professionnel peut « échanger » des informations en vertu du II de l'article L. 11104 du Code de la santé publique, le III du même article précise que les professionnels « partagent » les 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 »*[528]. 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 »*[529]. Partant de ces définitions il faut s'astreindre à articuler les dispositions règlementaires et légales afin de circonscrire le plus clairement possible les champs respectifs du partage et de l'échange d'information.

773. **Les modalités de l'échange et du partage de l'information**. L'article L. 1110-4 du Code de la santé publique prévoit d'abord l'échange et le partage. Les dispositions générales relatives à ces deux hypothèses dans lesquelles l'information circule sont définies par des actes règlementaires[530]. 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. Cette liste, qui a pu faire l'objet de critiques[531],

---

[528] 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.

[529] *Ibid.*

[530] C. santé publ art. R. 1110-1.

[531] Notamment en ce qu'elle n'inclue par les aidants et la famille 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.

distinguent les professionnels susceptibles d'échanger ou de partager des informations relatives au malade. La catégorie des professionnels de santé (dont les professions sont encadrées par le Code de la santé publique) et une sous-catégorie 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. À ce sujet un auteur remarque :

774. *« Une chose très surprenante est à noter car si l'article annonce un listing des professionnels autorisés à échanger ou partager des informations relatives à une même personne prise en charge, le e) vise les "Particuliers accueillant des personnes âgées ou handicapées mentionnées au titre IV du livre IV du code de l'action sociale et des familles". Il s'agit des accueillants familiaux rémunérés pour recevoir les personnes susmentionnées. Cette intégration déroute car l'article 1110-4, que le décret est censé expliciter, ne vise un partage ou échange d'informations qu'entre professionnels ! Si l'on comprend l'intérêt de cet élargissement visant à faciliter la prise en charge de la personne accueillie, le risque d'atteinte au secret médical et à la vie privée est ici évident »*[532].

775. **Un échange d'informations.** Outre les questions relatives à la liste des personnes le cadre général distingue l'échange et partage. L'échange d'informations peut se faire entre toutes les personnes inscrites dans cette liste à condition de respecter l'obligation d'information du patient qui figure à l'article R. 1110-3 du Code de la santé publique. Le patient peut évidemment s'opposer à cet échange en vertu de l'article 1110-4 IV du Code de la santé publique, cette disposition s'applique en

[532] L. Morlet-Haidara, « Le nouveau cadre légal de l'équipe de soins et du partage des données du patient », *RDSS* 2016, p. 1103.

effet dans toutes les hypothèses où le consentement de la personne n'est pas exigé.

776. **Un partage d'informations.** Le partage de l'information relative à un malade dans le cadre de sa prise en charge, tel que précédemment défini [533], correspond à une mise à disposition, c'est-à-dire à une accessibilité de l'information. Une distinction est opérée entre le partage dans le cadre d'une même équipe de soin et le partage hors équipe de soin. L'équipe de soin est définie à l'article L. 1110-12 du Code de la santé publique il s'agit des professionnels qui :

777. *« 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 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. »*[534]

778. Dans le cas où la mise à disposition s'effectue dans le cadre d'une équipe de soin[535] alors le consentement de la personne n'est pas exigé mais les professionnels ont une obligation d'information, il en est de même pour

[533] V. *supra* n° 541.

[534] C. santé publ. art. L. 1110-12.

[535] Pour une analyse complète des variations de l'équipe de soin v. L. MORLET-HAIDARA, « Le nouveau cadre légal de l'équipe de soins et du partage des données du patient », *op. cit.*

l'échange dans le cadre de l'équipe de soin[536]. S'agissant du partage des informations hors équipe de soin, il s'agit de mettre à disposition des informations hors du cadre d'une prise en charge dans une équipe prédéfinie[537]. Aussi, il ne s'agira plus seulement d'informer la personne mais d'obtenir son consentement au partage (mais non à l'échange qui répond au cadre général).

779. **La circulation de l'information hors du cadre de la prise en charge du malade.** Si les informations circulent dans le cadre du secret partagé, d'autres dispositions du Code de la santé publique permettent de fonder une telle circulation mais celles-ci ne constituent ni un partage ni un échange d'information au sens de l'article L. 1110-4 du Code de la santé publique. En effet, le Code de la santé publique comprend d'autres dispositions prévoyant une circulation de l'information non plus pour la prise en charge de la personne mais de manière à permettre l'analyse de l'activité de l'établissement.

780. **Circulation et évaluation de l'activité.** L'article R. 6113-1 du Code de la santé publique prévoit que *« Pour l'analyse de leur activité médicale, les établissements de santé, publics et privés, procèdent, dans les conditions fixées par la présente section, à la synthèse et au traitement informatique de données figurant dans le dossier médical mentionné à l'article 1112-1 qui sont recueillies, pour chaque patient, par le praticien responsable de la structure médicale ou médico-technique ou par le praticien ayant dispensé des soins au patient et qui sont transmises au médecin responsable de l'information médicale pour l'établissement, mentionné à l'article 6113-7 »*. Les informations concernées sont précisées au même article et concernent : « 1° L'identité du patient et son lieu de résidence ; 2° Les modalités selon lesquelles les soins ont été dispensés,

[536] Pour les 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.*

[537] E. BUCKI, G. CASANOVAS, S. LANGARD, « Les règles d'échange et de partage d'informations : aux limites de la démarche empirique », *op. cit.*

telles qu'hospitalisation avec ou sans hébergement, hospitalisation à temps partiel, hospitalisation à domicile, consultation externe. 3° L'environnement familial ou social du patient en tant qu'il influe sur les modalités du traitement de celui-ci ; 4° Les modes et dates d'entrée et de sortie ; 5° Les unités médicales ayant pris en charge le patient ; 6° Les pathologies et autres caractéristiques médicales de la personne soignée ; 7° Les actes de diagnostic et de soins réalisés au profit du patient au cours de son séjour dans l'établissement. ». Ainsi, les informations prévues au présent article ne demeurent pas entre les mains des seuls professionnels de santé. Elles sont transmises aux personnels chargés du

781. PMSI[538], il s'agit des professionnels du service chargés de l'information médicale au sein d'un établissement dont le responsable est un médecin (DIM) et dont les fonctions peuvent être diverses[539].

782. **Circulation des informations hors de l'établissement**. Par ailleurs, les informations relatives au malade peuvent également circuler en vertu de l'article L. 1461-1 du Code de la santé publique. J. Bossi-Malafosse constate en effet que toutes les informations issues des soins sont vouées à intégrer le Système national des données de santé[540.] Ce système est également composé *« des données du Système national d'information inter-régimes de l'assurance maladie (SNIIRAM) produites par les organismes gérant un régime de base d'assurance maladie (CSS, art. L. 161-28-1) ;des données sur les causes de décès mentionnées à l'article 222342 du code général des collectivités territoriales ; - des données médico-sociales du système d'information mentionné à l'article*

[538] Programme de médicalisation des système d'informations prévu à l'article L. 6113-7 du Code de la santé publique.

[539] Les professionnels chargés de l'information médicale peuvent être des techniciens dits « de l'information médicale », mais également des analystes et des statisticiens, data scientist (qui est un nouveau métier s'approchant de celui d'analyste mais nécessitant la maitrise des Big data et donc une maitrise informatique et mathématique accrue).

[540] J. Bossi- Malafosse, « Les nouvelles règles d'accès aux bases médico-administratives », *Dalloz IP/IT* 2016, p. 205.

247-2 du code de l'action sociale et des familles qui rassemble les données produites par les maisons départementales des personnes handicapées sous l'autorité de la Caisse nationale de solidarité pour l'autonomie ; d'un échantillon représentatif des données de remboursement par bénéficiaire transmises par des organismes d'assurance maladie complémentaire et défini en concertation avec leurs représentants »[541]. Or la loi du 26 janvier 2016, si elle prévoit la mise en œuvre de ce système national, elle en prévoit également les accès[542]. En effet, il sera possible pour un tiers et à des fins particulières d'accéder à des données de santé ou des données personnelles contenues dans ce système ou à des données permettant l'identification indirecte des personnes concernées. Cet accès, qui constitue un traitement est soumis à certaines conditions relevant de la loi informatique et liberté et du règlement européen relatif à la protection des données[543]. Ainsi, l'information circule au-delà du cadre de la prise en charge du patient et à d'autres fins.[544]

[541] *Ibid.*

[542] V. *supra* n° 579.

[543] V. *supra* n° 396 et svt.

[544] V. *infra* n° 578.

784. § 2. De nouvelles formes d'exercice

785. **Les coopérations ville-hôpital**. Dans un objectif de restructuration de l'offre de soin ayant pour but de rationaliser les moyens des établissement public et privé et des professionnels libéraux, le gouvernement avait amorcé, dès les années 1990[545] des mécanismes de coopération entre ces différents acteurs. Le premier et le plus pérenne de ces outils juridiques de coopération consiste dans le Groupement de Coopération Sanitaire (GCS). Il s'envisage dans le cadre d'un territoire donné puisque l'un de ses objectifs premiers est de favoriser la proximité des soins, de plus c'est l'ARS qui est chargé de superviser la création des groupements. Les conditions de mise en œuvre de ces groupement a connu plusieurs modifications[546]. Il s'agit pour les acteurs du parcours de santé, qu'ils exercent en ville ou à l'hôpital, de constituer une nouvelle personnalité morale qui peut être de droit public ou de droit privé. Ces cadres d'exercices sont de deux natures : le GCS de moyens[547] et le GCS établissement de santé[548], ils répondent à des conditions et des obligations particulières qui n'intéressent pas notre étude[549]. Ce qu'il convient toutefois de soulever c'est que ces cadres de coopération constituent des terrains particulièrement propices à la circulation de l'information et à la mise en œuvre des dispositions relatives au secret partagé puisqu'il peut être constitué *« par des établissements de santé publics ou privés, des établissements médico-sociaux mentionnés à l'article3 12-1 du code de*

[545] Au travers du « plan Juppé ».

[546] Notamment par l'ordonnance n° 2003-850 du 4 septembre 2003 puis par la loi « HPST » n° 2009879 du 21 juill. 2009 (v. Gallet, *Les enjeux de la réforme du groupement de coopération sanitaire*, Rev. dr. et santé 2009, no 28, p. 114), puis par la loi du 26 janvier 2016 relative à la modernisation du système de santé, *op. cit.*

[547] C. santé publ art. L. 6133-1.

[548] C. santé publ art. L. 6133-7.

[549] Sur ce point v. Dossier « Organisation territoriale ville-hôpital », *Rev. hosp. France*, déc. 2017, no 579, p. 60 ; C. Esper, « Le groupement de coopération sanitaire : actualité et limite », *RDSS* 2007, p. 117.

l'action sociale et des familles, des centres de santé et des maisons de santé, des personnes physiques ou morales exerçant une profession médicale à titre libéral ». Il doit comprendre au moins un établissement de santé, sauf dans le cas prévu au deuxième alinéa de l'article 6133-7[550]. Ainsi, le cadre de la coopération les professionnels sont susceptibles d'échanger ou du partager des informations au regard des dispositions relatives aux dispositions évoquées en amont[551]. Ces échanges et partages sont majoritairement dématérialisés par soucis d'efficacité[552]. Il faut mentionner que certains modes d'exercice se font désormais en réseaux, le fonctionnement de ces réseaux contient des particularités que nous évoquerons en aval[553].

786. **La coopération entre établissements de santé.** Contrairement au groupement de coopération sanitaire, la coopération entre établissement publics de santé est une obligation et non une possibilité, elle prend la forme d'un groupement hospitalier de territoire (GHT) dont l'organisation est centrée sur le parcours du patient. Les établissements de soin privés peuvent toutefois intégrer un tel groupement. Mesure phare de la loi du 26 janvier 2016 relative à la modernisation de notre système de santé, il s'agit d'améliorer la qualité du service public hospitalier en permettant *« […] aux établissements de mettre en œuvre une stratégie de prise en charge commune et graduée du patient, dans le but d'assurer une égalité d'accès à des soins sécurisés et de qualité. Il (le GHT) assure la rationalisation des modes de gestion par une mise en commun de fonctions ou par des transferts d'activités entre établissements. Dans chaque groupement, les établissements parties élaborent un projet médical partagé garantissant une offre de proximité ainsi que l'accès à une offre de référence et de*

[550] C. santé publ art. L. 6133-2.

[551] V. *supra* n° 539 et svt.

[552] Par exemple le GCS télésanté Lorraine a mis en place une multitude d'outils à destination des professionnels par le biais d'une plateforme dénommée SOLSTIS (voir le site en ligne : <https://www.sante-lorraine.fr/portail/>.

[553] V. *infra* n° 567.

recours »[554]. Les GHT constitue un accélérateur de travail commun professionnels, qu'il s'agisse des professionnels de santé ou des professionnels techniques. Il nécessite donc l'échange et le partage d'informations, dans ce cadre de la convergence des systèmes d'informations de chaque établissement partie du GHT. A ce titre le ministère des affaires sociales et de la santé a publié un guide à l'occasion duquel il explique comment doit s'effectuer ce rapprochement en se référant à de nombreuses reprises à la loi informatique et liberté qui structure l'intégralité de cette démarche[555].

787. **L'exercice en équipe :** L'exemple des maisons de santé pluridisciplinaires. Introduite par la loi de financement de la sécurité sociale du 19 décembre 2007, les maisons de santé sont des structures à mi-chemin entre l'exercice libéral et l'établissement de soin. Il s'agit de professionnels libéraux qui choisissent d'exercer dans une structure physique « maison », indépendamment de leurs professions respectives, mais ayant choisies de coordonner leur exercice au travers d'un projet de santé répondant aux besoins identifié par l'ARS. C'est d'ailleurs elle q1ui valide les objectifs à l'occasion de contrats pluriannuels qui conditionnent l'octroi des aides de l'État. Elles sont définies à l'article L. 6323-3 du Code de la santé publique. L'article précise que, même si les professionnels qui exercent en maison de santé sont en principe des professionnels de santé (infirmier libéraux, kinésithérapeute, médecin, dentiste, sage-femme), elles peuvent associer des personnels médico-sociaux. Ce type d'exercice exige l'échange et le partage des informations dès lors que les professionnels travaillant dans ces structures constituent des équipes de soins au regard de l'article L. 1110-12 du Code de la santé publique dès lors que plusieurs professionnels prennent en charge un même patient.

---

[554] C. santé publ art. L. 6132-1.

[555] Ministère des affaires sociales et de la santé, *Guide méthodologique stratégie, optimisation et gestion commune d'un système d'information convergent d'un GHT*, juill. 2016.

788. Section 2. Une recherche d'efficience et de qualité

789. Le système de santé cherche à améliorer l'efficience, la qualité et la sécurité des soins. Cette recherche conduit les décideurs à restructurer et animer des opérateurs publics et privés de santé du territoire (sans préjuger qu'il s'agisse d'une communauté hospitalière de territoire – CHT - ou toute autre forme de coopération) est un objectif prioritaire pour rationaliser et optimiser l'offre de soins sur les différents territoires de la région. Cela conduit çà repenser la prise en charge du patient sur l'ensemble de son parcours de santé, et non plus sur l'acte en lui-même *« Il assure la rationalisation des modes de gestion par une mise en commun de fonctions ou par des transferts d'activités entre établissements. Dans chaque groupement, les établissements partis élaborent un projet médical partagé garantissant une offre de proximité ainsi que l'accès à une offre de référence et de recours. »*[556]

790. Ce nouveau mode de coopération s'établit autour d'un « projet médical partagé » par tous les établissements membres qui formalise la répartition des activités et la gradation des soins sur le territoire. Dès lors, chaque hôpital est partie prenante d'une stratégie territoriale commune de prise en charge des patients et travaille en réseau avec les autres établissements du groupement.

791. Le partage de l'information constitue une réponse aux nouvelles formes d'organisation (Paragraphe 1). L'échange d'informations entre les professionnels est désormais au cœur de la notion de parcours, de continuité des soins et de sécurité des prises en charge. Cette circulation

[556] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, Journal officiel du 27 janvier 2016, art. 107.

de l’information excède la relation de soin afin de répondre aux nouveaux enjeux de santé publique (Paragraphe 2).

793. § 1. Une réponse aux nouvelles formes d'organisation

794. **La continuité des soins une continuité relationnelle et informationnelle.** La continuité des soins peut-être appréciée comme une succession de prestations de soins, cohérents, appropriés aux besoins de la personne prise en charge et compatibles avec sa situation personnelle. Elle comporte, de ce fait, une dimension « relationnelle » et « informationnelle »[557]. La dimension relationnelle s'entend comme le fait d'assurer des soins de manière longitudinale, *« pendant une période substantielle de la vie, non-limités à un épisode de maladie »*[558]. Il s'agit de produire des soins, dans le temps, en assurant la transition entre les événements de vie du patient. Ainsi, elle repose sur une continuité d' « approche », c'est-à-dire sur la capacité des professionnels à assurer, du fait de leur mission, une cohérence entre les soins qu'ils prodiguent au profit d'un même patient. Cette cohérence suppose une continuité informationnelle. Il s'agit, pour les professionnels intervenant dans la prise en charge de la personne, d'avoir connaissance des événements antérieurs la concernant (perte d'autonomie, pathologie, alimentation, soins, etc.) afin de lui prodiguer des soins adaptés à sa nouvelle condition en tenant compte de ses antécédents. L'accessibilité aux informations pertinentes, relatives à l'état de santé de la personne ou à sa situation individuelle évite une rupture du continuum de soins et permet une prise en charge adaptée.

795. **L'apparition du partage à l'issue de la transition épidémiologique.** Cette nécessitée de partager de l'information apparaît également suite à la transition épidémiologique. « *Sous l'influence du*

[557] R. REID, H. AGGERTY, J. HAGGERTY, R. MCKENDRY,, Mc. KENDRY R. DISSIPER la confusion : concepts et mesures de la continuité des soins, Fondation canadienne de la recherche sur les services de santé, Ottawa, mars 2002.

[558] Les définitions européennes de la médecine *générale* de famille WONCA EUROPE, 2002, p. 24.

développement socio-économique [de nos société, nous sommes passé] d'une structure de mortalité à dominante infectieuse à une structure de mortalité à dominante chronique et dégénérative »[559]. En conséquence, un exercice isolé du soin n'est plus adapté. Les personnes souffrant de maladies chroniques, pluri pathologiques, requièrent une prise en charge pluri professionnelle et la création d'équipes pluridisciplinaires au sein desquels l'intervention de chaque professionnel est coordonnée et protocolisée. Cette nouvelle approche du soin a donné naissance à de véritables parcours de soins personnalisés permettant un suivi médical optimal. L'organisation de ses parcours repose sur une coordination des professionnels à deux niveaux et, par conséquent, sur le partage et l'échange d'informations pertinentes concernant l'état de santé, la situation individuelle ou les soins prodigués à la personne. Les professionnels prenant en charge la personne, communiquent ainsi entre eux les éléments pertinents et indispensables pour garantir la qualité de leurs interventions et de natures à garantir le bon suivi du patient et/ou de l'usager.

796. **Une coordination du parcours clinique et de la prise en charge.** Le premier niveau de coordination concerne le parcours clinique du patient. Il a vocation à garantir la cohérence, la continuité, le suivi dans la prise en charge sanitaire de la personne. Le second niveau de coordination, est destiné à garantir une prise en charge globale de la personne par la coordination des professionnels du secteur sanitaire et des professionnels du secteur médico-social. Cette coordination de second niveau, suppose que des échanges soient réalisés entre professionnels de catégories différentes (sanitaire, médico-social). Dans ce cadre, la

[559] A. OMRAN, en 1971, est le premier à théoriser la « transition épidémiologique ». Par ses travaux il essaie d'expliquer les progrès réalisés au 18ème siècle en matière de santé publique et, d'autre part, de l'émergence de nouvelles pathologies dans les pays industrialisés. Ces constatations comportent trois phases dont la troisième marque la transition des pathologies infectieuses vers les pathologies des sociétés développées comprenant les maladies liées aux progrès de la technique et à l'augmentation de l'espérance de vie, autrement dit aux maladies chroniques et dégénératives

personne prise en charge doit recevoir une information préalable relative à la nature des informations et à la qualité du destinataire de l'information[560].

797. **De nouvelles formes d'organisation et de partage répondant à la prévention de la perte d'autonomie.** Nous l'avons précisé précédemment, les professionnels du secteur social faisaient l'objet de dispositions éparses figurant au sein du Code de l'action sociale et des familles et n'étaient pas soumis de manière uniforme au secret professionnel. Ainsi, le partage avait le plus souvent lieu sans autorisation de la loi. La loi du 26 janvier 2016 procède donc à un « décloisonnement » sans commune mesure de la circulation d'information entre les professionnels des secteurs sanitaire, médico-social et social. Elle facilite la prévention mais aussi le suivi afin d'améliorer la prise en charge de la personne concernée et donne un cadre juridique au partage d'informations entre professionnels.

798. En raison de la redéfinition et de l'assouplissement des règles de partage, elle facilite, à titre d'exemple, le suivi des mineurs, atteints d'un handicap, par leur médecin traitant et l'institut médico-éducatif qui les accueils.

799. La prévention fait partie des innovations introduites par la loi relative à l'adaptation de la société au vieillissement[561]. Cependant, son utilisation comme motif de partage de l'information résulte de la loi de modernisation de notre système de santé.

800. Le texte ne définit pas précisément les actions de prévention justifiant une atteinte au secret. Il s'agit d'une notion pouvant regrouper des réalités complexes telles que, la prévention de la délinquance qui oblige les éducateurs de rue à transmettre les informations nominatives concernant les infractions susceptibles d'être commises par les jeunes dont

[560] C. santé publ, art. R. 1110-2 et R. 1110-3, I.

[561] Loi n° 2015-1776 du 28 décembre 2015 relative à l'adaptation de la société au vieillissement.

ils ont la charge[562], ou encore, la prévention des mauvais traitements et la protection des mineurs maltraités etc.

801. Toutefois, si nous nous livrons à une lecture combinée des dispositions des articles L. 1110-4 et L. 1110-12 du Code de la santé publique le terme prévention devrait, a fortiori, faire référence aux actions de prévention et de suivi relatives à la perte d'autonomie des personnes âgées[563.]

802. En la matière, on observe, sur l'ensemble du territoire, en complément des projets nationaux, la multiplication d'initiatives de la part des acteurs impliqués dans le soin et l'aide. Sur l'impulsion du ministère de la santé, l'ensemble de ces actions font l'objet d'une planification au sein des projets régionaux de santé des ARS.

803. Ces dispositifs et expérimentations ont pour principal objectif de prévenir la perte d'autonomie par l'apport d'une réponse simplifiée, harmonisée, complète et adaptée aux besoins des personnes âgées concernées et de leurs aidants.

804. **La définition de nouvelles formes d'organisation et d'espaces de partage**. Une part significative de ces projets repose sur la définition de nouvelles formes d'organisation, la coordination des acteurs préexistants ou la création de moyens ainsi que d'espaces de partage et d'échange d'informations relatives aux personnes prises en charge. Ils permettent, dans le respect du principe de proportionnalité, de collecter, d'échanger, de partager et de conserver suffisamment d'informations pour opérer un suivi personnalisé et efficace des personnes accompagnées, tout en veillant à ne pas porter atteinte au respect de leur vie privé. Ils apportent,

[562] J.-P. ROSENCZVEIG, P. VERDIER, C. DAADOUCH ROSENCZVEIG, Le secret professionnel en travail social et médico-social, Santé Social, Dunod, 6e éd., 2016, p. 192.

[563] Loi n°2015-1776 du 28 décembre 2015 relative à l'adaptation de la société au vieillissement, Chapitre III « Prévention de la perte d'autonomie »..

par ailleurs, des garanties supplémentaires par rapport aux outils traditionnels tels que les cahiers de liaison ou de transmission etc.

805. **Le programme PAERPA et le dispositif MAIA.** C'est notamment le cas du programme PAERPA et du dispositif MAIA (Méthode d'action pour l'intégration des services d'aide et de soin dans le champ de l'autonomie), qui associent et intègrent les services d'aide et de soins.

806. Fondé sur l'art. 48 de la Loi de financement de la sécurité sociale (LFSS) pour 2013[564], ce programme s'inscrit dans le cadre de la stratégie nationale de santé. Il s'adresse aux personnes âgées de plus de 75 ans dont l'état de santé est susceptible d'être altérer pour des raisons d'ordre médical ou social. Il favorise leur maintien à domicile en renforçant la coordination des professionnels de santé de 1er recours, en lien avec les professionnels sociaux, lorsque leur situation médico-sociale le nécessite.

807. Il s'accompagne de la mise en œuvre de coordinations territoriales d'appui (CTA) intégrant les différents dispositifs existant (réseau, CLIC, MAIA, etc.) et, depuis 2016, sur la création de plateformes territoriales d'appui (PTA).

808. Ces dispositifs sont organisé par l'ensemble des acteurs locaux, professionnels du médical et du médico-social reconnus sur le territoire dont, des professionnels libéraux, réseaux, MAIA, établissements sanitaires et acteurs du domicile, établissement sociaux et médico-sociaux, collectivités locales, représentants des usagers etc.

809. Ils permettent de développer la coordination, le suivi et la prévention autour de l'usager et du patient au moyen d'outils notamment tels que le plan personnalisé de santé un de systèmes d'information partagés. Lorsqu'une hospitalisation a été nécessaire, ce acteurs partagent

[564] Loi n° 2012-1404 du 17 décembre 2012 de financement de la sécurité sociale pour 2013.

les informations nécessaires afin de sécuriser la sortie de l'hôpital par l'anticipation et la préparation de la sortie notamment par la transmission des informations nécessaires au médecin traitant, le cas échéant, aux structures d'hébergement temporaire ou qui sont nécessaire à la mobilisation de services d'aide à domicile (SAAD) et services polyvalents d'aide et de soins à domicile (SPASAD).

810. Pour sa part, la MAIA issue du plan Alzheimer 2008-2012, est une méthode de travail collaboratif associant l'ensemble des acteurs engagés dans l'accompagnement des personnes en perte d'autonomie âgées de plus de 60 ans et, qui sont en situation complexe nécessitant un suivi intensif et au long cours. Ce guichet intégré[565] permet, à partir d'une évaluation multidimensionnelle, d'apporter une réponse appropriée au besoin de la personne. Elle repose sur des outils communs de pilotage et de partage de l'information entre les acteurs du sanitaire, du social et du médico-social (EHPAD579, réseaux de santé, SSIAD[566], associations, CCAS[567], etc.) afin d'établir un accompagnement personnalisé est d'en assurer le suivi.

811. Ces deux dispositifs illustrent parfaitement l'importance de la réforme de 2016. Malgré les finalités poursuivies lors de leur création, il était difficile, sans réforme du secret partagé, de parvenir aux objectifs escomptés. En effet, le programme PAERPA et le dispositif MAIA sont fondées sur le partage et l'échange d'informations sur la situation sociale et médicale de la personne prise en charge. Les professionnels intervenant auprès de l'usager et du patient, se comporte *de facto* comme les membres d'une véritable équipe de soins coordonnée et bénéficiant d'outils partagés

[565] Mode d'organisation partagé entre l'ensemble des partenaires chargés de l'information, de l'orientation, et de la coordination sur un territoire donné et qui a pour objectif d'apporter une réponse harmonisée et adaptée aux besoins de l'usager quellequel que soit la porte d'entrée du demandeur. 579 Etablissements d'hébergement pour personnes âgées dépendantes.

[566] Services de soins infirmiers à domicile.

[567] Centre communal d'action sociale.

(agenda, système d'information, outils d'analyse de la situation individuelle de la personne partagé etc.) Cependant, les dispositions de l'article L. 1110-4 du Code de la santé publique ne leur octroyaient pas le statut d'équipe de soins et ne permettait pas de partager des informations entre professionnels nuisant ainsi à une prise en charge optimale de la personne.

812. **PAERPA l'instauration d'un dispositif dérogatoire.** De cette manière, il n'existait pas de dérogation légale permettant aux professionnels de partager de l'information dans le cadre de la prévention et du suivi du patient et de l'usager. Dans ce cadre, l'adoption de PAERPA s'est accompagnée de l'instauration d'un dispositif dérogatoire [568] autorisant les professionnels de santé et du champ social et médico-social à échanger des informations de santé, sociales et administratives dès lors qu'elles sont strictement nécessaires pour déterminer la meilleure prise en charge possible de la personne âgée subissant de graves atteintes cognitives ou de lourdes pertes d'autonomie fonctionnelle.

813. De la même manière, la MAIA ne constitue pas un établissement, un centre, une maison ou un réseau de santé car son activité ne se limite pas à la prise en charge sanitaire de la personne. Elle comprend également la gestion de ses difficultés sociale et des aides financières[569]. Ainsi, elle intervient notamment en ce qui concerne l'allocation personnalisée pour l'autonomie (APA), l'allocation pour le logement (APL) ou encore en matière de prestation compensatrice du handicap (PCH). Par conséquent, le gestionnaire de cas[570] était tenu au secret professionnel mais, de par son

[568] Loi n° 2012-1404 du 17 décembre 2012 de financement de la sécurité sociale pour 2013, art. 48, IV, et Décret n° 2013-1090 du 2 décembre 2013 relatif à la transmission d'informations entre les professionnels participant à la prise en charge sanitaire, médico-sociale et sociale des personnes âgées en risque de perte d'autonomie.

[569] Numéro spécial Secret médical, Bull. CNOM, nov.-déc. 2012.

[570] Le gestionnaire de cas, dans le cadre de ses missions, est chargé de coordonner les différentes interventions tout au long du parcours, d'élaborer le plan de services individualisés en interdisciplinarité et en étroite collaboration avec le

statut de professionnel du secteur social, il ne faisait toutefois pas parti d'une équipe de soins et, ne pouvait bénéficier des dispositions relatives au secret partagé.

814. De la sorte, contrairement aux dispositions existantes au profit des maisons départementales des personnes handicapées, les professionnels intervenant dans le cadre de ce dispositif ne pouvaient être considérés comme constituant une équipe de soins et échanger des informations sociales et de santé.

815. Une réforme était, par conséquent nécessaire afin de remédier aux faiblesses identifiées. La loi de 2016 uniformise, en ce sens, les dérogations au secret partagé et les intègres au sein du Code de la santé publique mettant ainsi fin à la multiplication des régimes dérogatoires. Elle élargie la notion d'équipe de soins afin d'y intégrer ces situations particulières au sein d'un régime général.

816. Au regard des dispositions de l'article L. 1110-12 du Code de la santé publique et L. 113-3 du Code de l'action sociale et des familles, le gestionnaire de cas et l'ensemble des partenaires intervenant dans le dispositif MAIA font désormais partie d'une équipe de soins, puisque participe parmi les professionnels intervenant auprès de la personne en perte d'autonomie un professionnel de santé.

817. Cette équipe de soins est uniquement constituée des professionnels participant directement à la prise en charge de la personne âgée. Ces derniers doivent, toutefois être clairement identifiés, et intégrés de manière formalisée au sein de la méthode. Enfin, il convient de rappeler que l'appartenance à cette équipe de soins ne dispense par les professionnels, ainsi que le porteur de veiller au respect des règles d'échange et de partage. L'équipe de soins n'emporte pas le droit, pour chaque membre de l'équipe, d'échanger et de partager toutes les données

médecin traitant. Il a, par conséquent, besoin d'échanger avec l'ensemble des professionnels, des informations relatives à la personne prise en charge.

relatives aux personnes âgées prises en charge dans le cadre du dispositif conformément aux dispositions des articles R. 1110-1 à R. 1110-3 du Code de la santé publique.

818. Concernant les traitements mis en œuvre dans le champ social et médico-social, cette évolution de la législation est insuffisante. La loi Informatique et Libertés et principalement les formalités préalables devant être réalisées auprès de la Commission, constituent un frein supplémentaire dans le traitement de l'information nécessaire à une prise en charge globale de la personne.

819. **Le recours aux autorisations uniques.** Ainsi, la CNIL, fréquemment sollicitée pour la mise en œuvre de ces traitements a, suite à la modification du cadre réglementaire et « *après concertation avec un échantillon d'acteurs représentatifs du secteur, […] adopté [le 14 avril 2016] trois autorisations uniques pour simplifier les formalités des organismes, œuvrant dans le champ de l'action sociale et médicosociale* ». Cette mesure de souplesse[571] concerne l'accompagnement et le suivi social des personnes en difficultés, la prévention et la protection des mineurs et jeunes majeurs ainsi que l'accompagnement et le suivi social et médico-social des personnes handicapées et des personnes âgées. Ces motifs de partage couvrent la plupart des situations rencontrées dans le champ social et médico-social. Ils constituent une évolution nécessaire et

[571] Faculté reconnue à la CNIL par l'art. 25, II de la 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. Cet aménagement constitue une mesure de souplesse et de simplification des formalités déclaratives auprès de la CNIL afin de faciliter et d'accélérer la gestion des dossiers déposés auprès de ses services. Elle permet une mise en œuvre rapide des traitements soumis à autorisation, les responsables de traitement déclarant, par ce mécanisme, se conformer au cadre défini par la Commission.

G. GOUZES, Rapport *sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, n°3526, Assemblée nationale, 9 janv.janvier 2002.

F. DELATTRE, Rapport *le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, n° 1537, Assemblée nationale, 13 avril 2004.

attendue par les acteurs suite à la réforme de 2016. Cette décision de la Commission permet d'accélérer la mise en œuvre de traitements dans le champ sociale et médico-social, et vient conforter les mesures instaurées afin de parvenir à une prise en charge personnalisée et globale de la personne. Elle supprime un peu plus la frontière artificielle séparant les professionnels. La personne est désormais située au centre du dispositif.

821. § 2. Une réponse aux nouveaux enjeux de santé publique

822. **De l'échange et du partage à l'accès aux données.** La logique qui a initié le secret partagé et son extension tient à des considérations relatives à l'efficience et à la qualité des soins, ainsi que nous avons pu l'exposer[572]. Cette logique est centrée sur le patient et sur son parcours, on peut la qualifier d'individuelle. Toutefois, les enjeux de santé publique, qui s'inscrivent dans une approche collective de la santé impose de rendre accessible certaines données. Il est nécessaire d'en évoquer certaines directement liées à l'ouverture des données de santé : l'Open data.

823. **La loi du 26 janvier 2016 et l'ouverture des données de santé.** Les trois objectifs affichés de la loi sont l'allongement de la durée de vie, le développement des maladies chroniques, et la persistance des inégalités de santé[573].

824. Pour répondre à ces problématiques le législateur propose notamment d'utiliser les données de santé à meilleures escient. En effet, le système national des données de santé doit permettre une amélioration substantielle de la sécurité sanitaire, par le biais par exemple de la pharmacovigilance.

825. **L'objectif de sécurité du médicament**. La pharmacovigilance[574] est définie par le Code de la santé publique de la manière suivante :

---

[572] V. *supra* n° 551 et svt.

[573] M. BORGETTO, « La loi santé », *RDSS* 2016, p. 595.

[574] A l'origine la pharmacovilance est une obligation des états instauré par le droit européen : « La législation pharmaceutique révisée (art. 101 à 108 du code révisé ; Règl. n° 726/2004, art. 21 et s.) impose aux États membres et au titulaire de l'autorisation, des obligations de pharmacovigilance renforcées depuis 2004 et assorties de sanctions si elles ne sont pas respectées, afin que le médicament fasse l'objet d'un suivi tout au long de sa mise sur le marché. À cet effet, les États membres prennent les mesures appropriées pour encourager les médecins et les autres professionnels de la santé à notifier les effets indésirables des médicaments. Ils mettent par ailleurs en œuvre un système de pharmacovigilance

826. *« La pharmacovigilance a pour objet la surveillance, l'évaluation, la prévention et la gestion du risque d'effet indésirable résultant de l'utilisation des médicaments et produits mentionnés à l'article 5121-1. »*

827. La mise en œuvre de cette surveillance devrait être largement améliorée grâce à l'ouverture des données de santé puisque l'article L. 1461-1 du Code de la santé publique prévoit dans son III 5° que contribue *« À la surveillance, à la veille et à la sécurité sanitaires ».* Une telle mise à disposition devrait pouvoir réduire les risques de scandale sanitaire[575] tel que ceux du Médiator®, des prothèses PIP ou encore plus récemment du Lévothirox®.

828. **Les autres objectifs affichés.** L'article L. 1461-1 du Code de la santé publique dévoile les objectifs. Au titre des finalités avec une visée collective il faut citer la mise en œuvre et l'évaluation des politiques de santé et de protection sociale qui permettent la pérennité du système de santé basé sur la sécurité sociale au même titre que la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales.

829. **La mise à disposition des données à des fins de recherche.** Les données et leur ouverture servira également à des fins de recherche,

---

chargé d'une part, de recueillir des informations utiles pour la surveillance des médicaments, notamment quant à leurs effets indésirables sur l'homme, et, d'autre part, d'évaluer scientifiquement ces informations. Celles-ci sont transmises aux autres États membres et à l'Agence, et enregistrées dans une banque de données (prévue par Règl. n° 726/2004, art. 57-1, al. 2, point l) accessible aux États et au public (art. 102 du code). La mise en place, par l'Agence d'un réseau informatique, facilite l'échange d'informations relatives à la pharmacovigilance concernant les médicaments mis sur le marché (art. 105 du code) » (N. De Grove-Valdeyron, « Médicament », *Rep. de droit européen*, janv. 2007 (act. 2018), n° 41.

[575] Les scandales précédents la loi de 2016 avait déjà donné lieu à une certaine ouverture des données personnelles. Sur ce point v. J. Peigné, *« Du Médiator aux prothèses PIP en passant par la loi du 29 décembre 2011 relative à la sécurité sanitaire des produits de santé », RDSS* 2012, p. 315.

permettant ainsi de réduire les coûts de la recherche[576]. Comme le remarque un auteur, cela concerne aussi les données médico-sociales dont l'utilité n'est pas moindre.

830. « *Si les données médico-sociales mises à disposition sont des données dont la richesse n'est pas celle des informations purement médicales, elles présentent néanmoins l'intérêt d'être des données objectives et exhaustives qui portent sur une très large population et permettent un suivi de longue durée. Enfin, les recherches peuvent être désormais engagées par des acteurs privés alors qu'auparavant seules les entités publiques pouvaient avoir accès aux données.* »[577]

[576] Sur ce point v. notamment : P.-J. Lancy, *« Les financements et les coûts de l'innovation », adsp* n° 39, juin 2002, spéc. p. 42.

[577] L. MORLET-HAÏDARA, « Le système national des données de santé et le nouveau régime d'accès aux données », *RDSS* 2018, p. 91.

CONCLUSION DU CHAPITRE 1

« Le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi. »[578]

832. Bien que le secret professionnel soit toujours nécessaire pour protéger la personne prise en charge de toute divulgation indiscrète, la formulation de l'article R. 4127-4 nous paraît désormais incorrecte.

833. A moins de considérer, le secret professionnel comme un secret partagé, cet article parait désuet. Il résulte désormais des dispositions de l'article L. 1110-4 du Code de la santé publique que la circulation de l'information relative à la santé est réalisée dans l'intérêt de la personne prise en charge. Celle-ci doit toutefois être réalisée entre des professionnels autorisés dans un contexte maitrisé et être motivée par l'efficience du système de santé et la qualité des soins prodigués.

[578] C. santé publ. art. R. 4127-4

CHAPITRE 2. LA SYSTEMISATION DE L'ACCESSIBILITE

« Les procédures d'autorisation via l'arrêté SNIIRAM, faisant intervenir un grand nombre d'acteurs et d'instances (membres du COPIIR, CNIL, ministre chargé de la sécurité sociale), prennent un temps très long même en cas d'urgence sanitaire : il a fallu ainsi plus de deux ans pour que l'ANSM obtienne le droit d'accéder aux données du SNIIRAM, accès qui lui est pourtant indispensable pour évaluer les risques associés à l'usage en vie réelle de certains médicaments ou produits de santé ; dans l'intervalle, les services de la CNAMTS ont mené eux-mêmes les plus urgentes des études exigées mais cette lenteur démontre à elle seule que la procédure est inadéquate. »[579]

835. **Des données constituant une ressource considérable.** Notre système de santé produit de nombreuses données composées de données médicales et de données médico-administratives (catégories majeures de diagnostics, durée d'hospitalisation, facturation, remboursement des soins, etc.) L'exploitation de ces données constitue une ressource considérable pour la recherche scientifique et permettrait également de veiller à la sécurité sanitaire et de réaliser des actions de promotion de la santé, d'amélioration de la qualité des soins et de l'efficience de notre système de santé. Des Une utilisation insuffisante des données .Cependant, ces données sont insuffisamment utilisées en raison de difficultés concernant leur mise à disposition. Il s'agit principalement de difficultés techniques

[579] P.-L. BRAS, A. LOTH, Rapport sur la gouvernance et l'utilisation des données de santé, sept. 2013, p. 34.

résultant du format des données, de la diversité des supports ou de la complexité de la base de données.

836. En effet, le SNIIRAM c'est quinze bases de données thématiques, un échantillon général des bénéficiaires (EGB) et une base de données individuelle des bénéficiaires (DCIR). Les données constituant la base de données sont initialement recueillies auprès des divers acteurs du système de santé pour diverses finalités, telles que le versement de prestations aux assurées. Ainsi, les bases de données constituant le SNIIRAM obéissent à des contraintes architecturales et leur contenu intègrent des contraintes de production et évoluent avec la réglementation.

837. Ces difficultés résultent également de l'existence de procédures d'autorisation d'accès longues et complexes. *« Malgré l'élargissement des finalités assignées au SNIIRAM, la diversification de ses utilisations en dehors de l'assurance maladie est freinée par la complexité et la lenteur des procédures d'accès aux données qu'il s'agisse d'accès permanents ou ponctuels. Les premiers se caractérisent encore par leur très inégale répartition. »*[580]

838. Les conditions d'accès aux données conservées dans le SNIIRAM étant complexes elles ont engendré une sous-exploitation des potentialités d'utilisation de la base. Compte tenu des enjeux de santé publique, une libération des données s'emble nécessaire (Section 1). Il convient d'apprécier si les conditions d'accès au Système National des Données de Santé (SNDS) ont été suffisamment simplifiées pour créer un environnement propice à la libération des données de santé. (Section2).

[580] Cour des comptes, Rapport 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 – Les données personnelles de santé gérées par l'assurance maladie – Une utilisation à développer, une sécurité à renforcer, mars 2016, p. 34.

839. Section 1. Une libération nécessaire des données

840. **Un scandale sanitaire menant à une prise de conscience.** L'affaire du Médiator® [581][582] a permis de révéler le mésusage et les difficultés d'accès aux bases de données médico-administratives tel que le SNIIRAM et, est à l'origine du mouvement d'ouverture des données publiques dit - open data - en France. Ainsi, en 2013, la Commission d'accès aux documents administratifs (Cada) avait été ainsi saisie par le collectif *« Initiative Transparence Santé », « à la suite du refus opposé par le directeur de la caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) à leur demande de communication des informations relatives à la consommation du Mediator® entre 1999, année de création par la CNAMTS de la base SNIIRAM, et 2009, année d'arrêt de commercialisation du médicament* »[583]. Ce refus reposait sur la décision du directeur de la CNAMTS qui estimait que la demande de communication présentée par le collectif *« Initiative Transparence Santé » « ne portait pas sur des documents administratifs existants mais concernait des informations, non immédiatement disponibles sous la forme souhaitée, dont la communication supposerait de sa part un traitement, par requêtes multiples, des données sources de la base ».*

841. Après avoir préalablement rappelé que *« sont regardés comme des documents administratifs existants, les informations qui sont contenues dans des fichiers informatiques et peuvent en être extraites par un traitement automatisé d'usage courant »,* la Cada s'était livrée à une appréciation des conditions d'extraction des informations sollicités. Elle

---

[581] S. Hocquet-Berg. *Réparation intégrale du préjudice dans l'affaire du Mediator sans réduction possible à raison des prédispositions de la victime.20.fév..2018.*

Source : https://www.revuegeneraledudroit.eu/blog/2018/02/20/reparation-integrale-du-prejudicedans-laffaire-du-mediator-sans-reduction-possible-a-raison-des-predispositions-de-la-victime/ (Consultée le 10 mai 2018)

[582] /02/2018 by Sophie Hocquet-Berg

[583] CADA, 21 nov. 20132017, avis n° 20134348.

avait ainsi considéré que la demande du collectif ne nécessitait qu'un simple extrait de données à caractère médical anonyme *« ne permettant pas, compte tenu de leur niveau d'agrégation, l'identification, même indirecte, des patients ou des médecins concernés »* et ne nécessitant pas un traitement des données source de la base qui excédait un usage courant.

842. Elle avait également précisé que la demande du collectif ne pouvait être regardée comme portant sur la constitution d'un nouveau document.

843. *« Ces informations correspondent, non à des données spécifiques n'existant pas en tant que telles dans la base, mais à l'agrégation de données que le SNIIRAM a pour vocation de répertorier conformément à ce que prévoit l'arrêté du 19 juillet 2013, relatif à sa mise en œuvre. »*[584]

844. Enfin, la Cada avait, à cette occasion, observé que le collectif *« Initiative Transparence Santé »*, ne faisait pas partie des personnes spécialement habilitées à consulter le SNIIRAM. L'article 37 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, n'y faisant pas expressément obstacle, elle avait cependant considéré que les dispositions de l'arrêté du 19 juillet 2013 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie ne faisaient pas obstacle à ce que ce collectif puisse demander, sur le fondement du droit d'accès reconnu par l'article de la loi du 17 juillet 1978[585], la communication des documents administratifs[586].

[584] Voir également en ce sens, CADACada, 10 oct. 2013, avis n° 20133264.

[585] 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 (abrogée).

[586] Notons que la Commisison utilise en l'espèce le terme de « documents administratifs » et non celui d'« informationd'information publique »..

845. Suite de l'affaire du *Médiator®* et aux problématiques d'accès précédemment exposées, les études menées, tardivement[587], à partir de l'exploitation des données de la base SNIIRAM, du PMSI mais aussi de l'INSEE ont permis de révéler responsabilité de l'État dans la mauvaise gestion de l'affaire et les conséquences sanitaires de ces carences[588]. Ces résultats ont également permis de démontrer l'intérêt d'une bonne exploitation de la base et de l'importance de faciliter l'accès aux données. De ce fait et compte tenu du contexte précédemment exposé, la communauté scientifique ainsi que les institutions, ont reconnu, pour la plupart, les enjeux de la collecte, de la conservation ainsi que de la concaténation de ces données[589].

846. L'arrêté du 19 juillet 2013 précité constitue une première réponse destinée à étendre l'accès au SNIIRAM aux organismes à but non lucratif *« université, école ou autre structure d'enseignement liés à la recherche »*[603] pour effectuer une étude en santé publique, après approbation du bureau de l'Institut des données de santé (IDS) et

---

[587] La première étude menée et qui a démontré que *« le risque d'hospitalisations pour valvulopathies associé à la prise de benfluorex était multiplié par trois et que le risque de chirurgie valvulaire était multiplié par quatre dans la période 2006-2008 »* n'a été publiée qu'à partir de l'année 2010 alors que le benfluorex a été commercialisé sous le nom de Mediator par les Laboratoires Servier de 1976 à 2009. Voir en ce sens, Médiator® (chlorhydrate de benfluorex). Etude sur les données de remboursement de l'Assurance Maladie (SNIIRAM*)*, AFSSAPS,). 16 nov. 2010.

[588] Franck Von Lennep expert ès protection sociale à la Direction de la recherche, des études, de l'évaluation et des statistiques (DREES),) lors de son audition par la Mission commune d'information (MCI) sur l'accès aux documents administratifs et aux données publiques, avait précisé que *« dès lors qu'on dispose des données nécessaires à la mise en évidence de tels dangers, il devient criminel de ne pas les utiliser* ». V, notamment, en ce sens, C. BOUCHOUX, *Rapport d'information fait au nom de la mission commune d'information sur l'accès aux documents administratif et aux données publiques*, n° 589, Sénat, Session ordinaire 2013-2014.

[589] Cour des comptes, Rapport 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 – Les données personnelles de santé gérées par l'assurance maladie – Une utilisation à développer, une sécurité à renforcer, mars 2016.

autorisation de la CNIL conformément aux dispositions du chapitre IX de la loi du 6 janvier 1978 modifiée.

847. **Une réforme créant les conditions d'un accès ouvert à des fins de recherche.** C'est dans ce contexte que la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé a été votée afin de mettre fin à cette situation. Elle a intégré, au moyen de son article 193, un titre VI relatif à la *« mise à disposition des données de santé »* au sein du livre IV de la première partie du Code de la santé publique. Ces dispositions modifient la gouvernance de l'accès aux données de santé en transformant l'IDS en Système National des Données de Santé

848. (SNDS). Le bénéfice attendu est de permettre l'exploitation des données de santé avec pour attente des bénéfices en terme de démocratie et de veille sanitaire, en matière de santé publique et de qualité et d'efficience du système de santé

849. (Paragraphe 1). L'objectif clairement affiché est de « *créer les conditions d'un accès ouvert [et maitrisé] aux données de santé »*[590] à des fins strictes de recherche, d'étude ou d'évaluation présentant un caractère d'intérêt public (Paragraphe 2).

§ 1. Un besoin de qualité et d'efficience

« Les enjeux de l'accès aux données de santé sont nombreux. Ils touchent à la démocratie sanitaire, à l'autonomisation des patients, à l'efficience de l'action publique, aux progrès de la recherche et à la capacité de notre pays à favoriser l'innovation et à rester compétitif (…) »

[590] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, Chapitre V.

850. Depuis 1977, *« deux systèmes d'information relatifs aux dépenses de santé coexistaient au sein du système national inter-régimes (SNIR) »*[591]. Cet outil à disposition de la Caisse Nationale de l'Assurance Maladie des Travailleurs Salariés (CNAMTS) permettait de comptabiliser les dépenses d'assurance maladie.

851. **Le « SNIR établissements »**. Il rassemblant le champ des établissements publics, privés, sanitaires et médico-sociaux regroupait l'ensemble des flux financiers liés aux dépenses hospitalières prises en charge par l'assurance maladie. Cette base de données était composée des données fondées sur la nomenclature générale des actes professionnels ainsi que d'informations sur les patients.

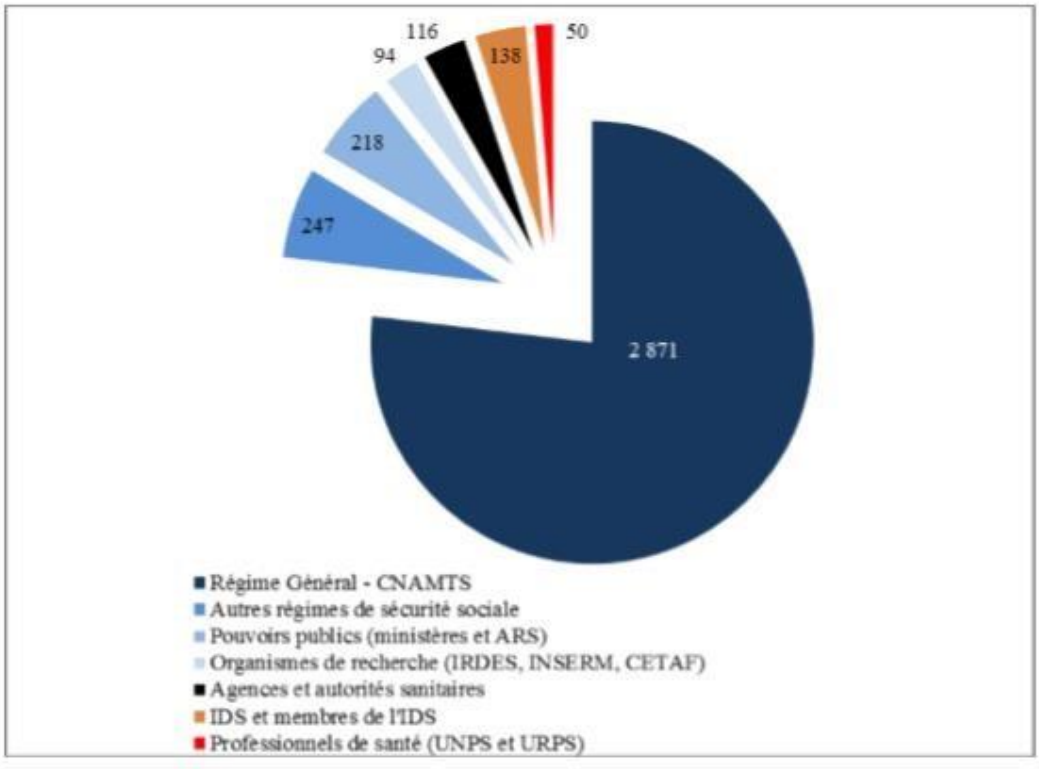
852. **Le « SNIR professionnel de santé ».** Il permettait quant à lui de recueillir et d'agréger, au niveau national, l'ensemble des données relatives à l'activité des professionnels de santé exerçant sous forme libérale et qui avaient donné lieu à remboursement par les organismes de l'assurance maladie, maternité et accident du travail. Cet outil statistique avait notamment pour finalité de permettre à l'assurance maladie de connaître le volume et le montant des prestations réalisées.

853. **Le SNIR une base de données incomplète**. Ne disposant d'aucun fondement légal imposant la transmission des données ou en réglementant l'accès de manière spécifique, l'alimentation du SNIR reposait sur de simples accords conventionnels inter-régimes. Ainsi, la Caisse ne disposait pas de moyens juridique et techniques suffisant pour contrôler la qualité des données fournies. C'est pourquoi cette base de données était incomplète et ne comportait pas de données provenant de certains régimes de l'assurance maladie notamment les régimes particuliers des militaires.

[591] Cour des comptes, Rapport préc.

854. **Le SNIIRAM une base de données dont l'alimentation est obligatoire.** Afin de remédier aux carences de ce système et de répondre aux besoins croissants de maîtrise des dépenses de santé, l'État créé, au moyen de la loi de financement de la sécurité sociale pour 1999[592], le « Système national d'information inter-régimes de l'Assurance maladie » (SNIIRAM) et en réglemente l'accès. L'article 21 de cette loi, codifié aux articles L. 161-28-1 à L. 11-28-4 a permis d'imposer aux organismes de base la transmissions, au SNIIRAM, des données relatives aux dépenses d'assurance maladie, tout en préservant l'anonymat des personnes ayant bénéficié des prestations de soins.

Graphique n° 7 : répartition des habilitations par organisme au 1er septembre 2015

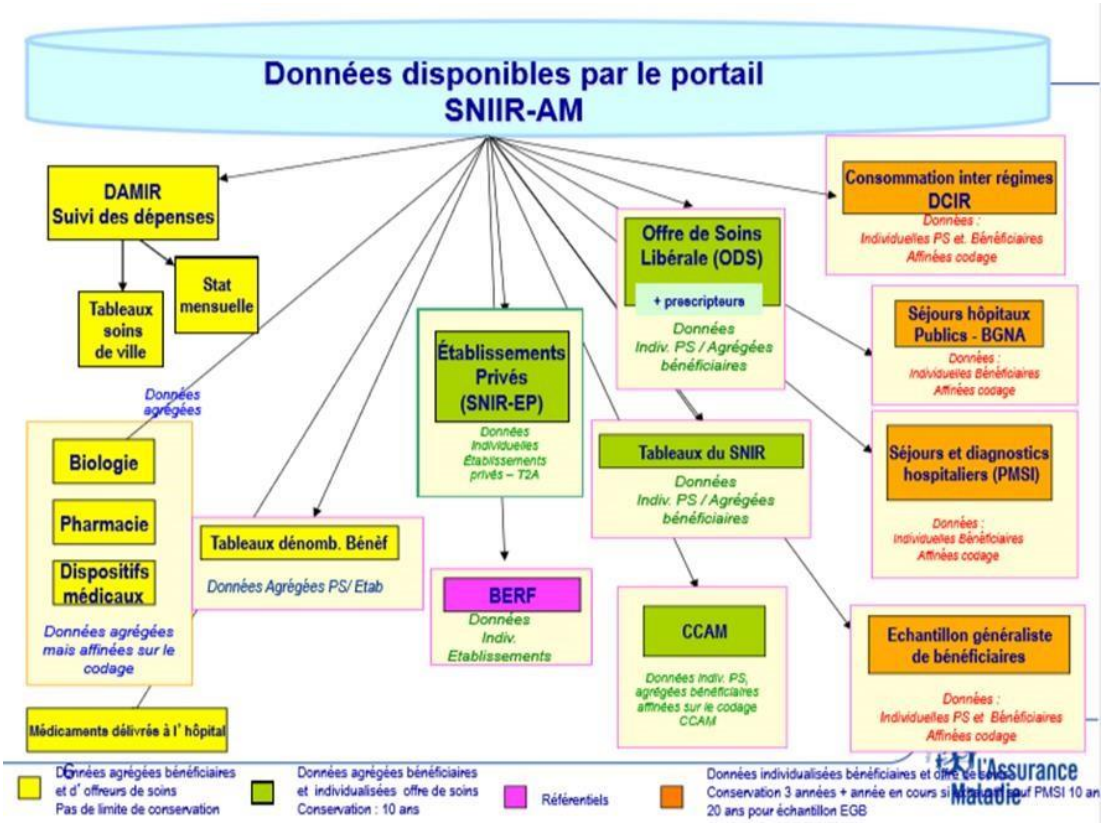


Source : Cour des comptes d'après les données de la CNAMTS.

[592] Loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale pour 1999.

855. Cette nouvelle base médico-administrative, l'une *« des plus grandes, voire [la] plus grande base médico-administrative au monde »*[593] procède ainsi de la fusion des deux bases constituant le SNIR. Ce système devait permettre de contribuer à la connaissance des dépenses d'assurance maladie et assurer la transmission aux prestataires de soins d'informations pertinentes relatives à leur activité, leurs recettes et, le cas échéant, leurs prescriptions[594].

856.



857. *Tableau 1 Données disponibles par le portail SNIIRAM*

[593] P.-L. BRAS, A. LOTH, Rapport sur la gouvernance et l'utilisation des données de santé, septembre 2013, p. 21. Voir également en ce sens, APMPM International, « Les dessous du Sniiram, la plus grande base de données de santé du monde »,, 25 mars 2013.

[594] Loi préc. art. 21 2°.°)

858. Antérieurement à la loi de modernisation de notre système de santé, l'accès au SNIIRAM était restreint par rapport aux enjeux sanitaires et financiers que peut représenter l'exploitation des données constituant cette base. Les contraintes d'accès et la faible utilisation des données à des fins d'intérêt général découlaient de l'application d'une forme de principe de précaution visant à protéger les droits et libertés des personnes et à titre principal, le droit au respect de la vie privé. Cette approche restrictive, résultait de l'absence d'appréciation *in concreto* de la probabilité de pouvoir procéder à la ré-identification des assurés en raison de deux facteurs. Le premier était lié à la masse de données dont la concaténation est susceptible de permettre la ré-identification[595] de la personne et le second résultant des progrès de la technique et des moyens technologiques disponibles pour procéder notamment à l'appariement de données.

859. Rappelons qu'initialement, l'article L. 161-28-1 du Code de la sécurité sociale précisait que « les organismes gérant un régime de base d'assurance maladie

860. (…) [devaient transmettre] au système national d'information interrégimes de l'assurance maladie les données nécessaires ». Ces catégories d'informations concernaient *« l'identification des organismes de prise en charge, les caractéristiques des décomptes de remboursement, les numéros d'anonymat des assurés et des bénéficiaires, le sexe, l'année et le mois de naissance, le département et la commune de résidence, les informations relatives aux prestations servies, comportant notamment le code détaillé des actes, biens et services présentés au remboursement ainsi que le code des pathologies, le numéro d'identification des professionnels de santé, le sexe, la date de naissance, la spécialité médicale, la nature d'exercice, le statut conventionnel, la caisse de rattachement, le*

[595] La réidentification se définitdéfinie comme la *« capacité à découvrir l'identité réelle d'une ou plusieurs personnes dont on ne connaît pas directement l'identité (par exemple par déduction ou inférence sur un ou plusieurs jeux de données »* (Arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé)..

département et la commune d'établissement, les informations relatives à l'activité des établissements de santé et des données comptables »[596597].

861. La CNIL, qui avait été saisie sur le fondement de l'article 15 de la loi relative à l'informatique aux fichiers et aux libertés dans sa version antérieure à la réforme de 2004, considérait que ces informations étaient « pertinentes au regard des finalités poursuivies » et jugeait exclusivement au regard des mesures techniques mises en œuvre que celles-ci étaient de nature à « assurer de façon convenable la confidentialité des informations ».

862. Cependant, bien que « les données reçues et traitées par le SNIIRAM préservent l'anonymat des personnes ayant bénéficié des prestations de soins »[598] en ce sens que, prises individuellement, elles ne permettent pas d'identifier un bénéficiaire déterminé, les caractéristiques[599] de ces données sont susceptibles de leur conférer la qualité de données indirectement identifiantes. En conséquence, si une démarche de ré-identification systématique semble peu probable et difficilement réalisable, lorsque ces données sont prises dans leur ensemble, une ré-identification indirecte relève tout de même du champ du possible.

---

[596] Délibération n° 01-054 du 18 octobre 2001 portant avis sur le projet d'arrêté présenté par le Ministère de l'emploi et de la solidarité relatif à la mise en œuvre du Système National d'Information Inter-Régimes de l'Assurance Maladie (SNIIRAMNIIRAM). Voir également Arrêté du 11 avril 2002 relatif à la mise en œuvre du système national d'information inter-régimes de l'assurance maladie, a. rt.

[598] CSS, art. L. 161-28-1.

[599] L'exhaustivité de la base, la précision des données et plus particulièrement, le fait qu'elles soient chainées font la richesse du SNIIRAM et peuvent permettre la mise en œuvre d'un système de veille sanitaire, la réalisation d'études épidémiologiques ou encore d'études en économie de la santé. V*oir notamment* P.-L. *BRAS*, A. LOTH,*André Rapport sur la gouvernance et l'utilisation des données de santé*, septembre 2013.

863. Plusieurs solutions ont été envisagées pour limiter le risque de ré-identification telle que la mise à disposition d'un échantillon généraliste de bénéficiaires (EGB), l'agrégation de données, l'occultation de certaines variables, ou encore la sélection et la limitation des catégories de personnes susceptibles d'accéder à la base.

864. Une simple appréciation des mesures d'anonymisation[600] fondée sur les procédés techniques utilisés et l'occurrence d'une réversibilité de cette méthode appelée encore ré-identification n'est pas adaptée. La protection de la vie privée des bénéficiaires nécessite la mise en œuvre de mesures et procédures destinées à contrôler l'accès à la base. Ainsi, en ce qui concerne la restriction des droits d'accès à la base, l'article L. 161-28-1-22 du Code de la sécurité sociale renvoyait initialement à l'arrêté du 11 avril 2002 relatif à la mise en œuvre du SNIIRAM de l'assurance maladie qui organisait notamment les procédures d'accès aux données contenues dans cette base ainsi que les modalités de leur transmission et de leur gestion[601].

865. Cette base de données a été complétée par un outil de veille épidémiologique introduit, dans notre système français, par Jean de Kervasdoué. Ce « Programme de médicalisation des systèmes

[600] L'anonymisation désigne un « processus *empêchant la ré-identification des individus* » (Arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé).. Il rend ainsi impossible le lien entre une donnée et une personne, de manière directe ou indirecte. « *Ce processus permet de rendre une donnée anonyme. Il peut parfois utiliser un mécanisme de pseudonymisation, mais ce n'est pas une obligation.* » (INDS, SNDS, Référentiel sécurité : Guide d'accompagnement, p. 32)..

[601] Cet arrêté imposait également la génération d'un numéro d'anonymat en prévoyant un double chiffrement du NIR. A noter que les données relatives aux différents soins réalisés au profit d'un même bénéficiaire peuvent être « chaînées ». Ainsi, bien que la personne demeure désignée par un même numéro d'anonymat résultant d'un double chiffrement du NIR, il n'est pour autant pas, théoriquement, possible de procéder à sa réidentification. Toutefois, bien que le SNIIRAM soit habituellement présenté comme une base de données individuelles anonymes, il convient de privilégier la notion de pseudonymisation. Voir Trouessin Dossiers solidarité et santé, Données de santé *: anonymat et risque de ré-identification*, n° 64, juillet 2015.

d'information » (PMSI) résulte de l'adaptation de la méthode de « *Diagnosis Related Groups* » mise au point aux États-

866. Unis, dans les années 1980, pour endiguer les dérives des dépenses de santé. Il s'agit d'un outil d'allocation budgétaire reposant sur la mesure médicalisée de la production hospitalière française et, l'adaptation de la rémunération des hôpitaux et des cliniques à ce produit.

867. Obligatoire depuis la loi du 31 juillet 1991, le PMSI a été généralisé en 1994 dans le secteur hospitalier public en 1994 et dans le secteur hospitalier privé en 1996 et permet désormais aux établissements de santé de procéder à l'évaluation et à l'analyse de leur activité.

868. Notons que *« les conditions d'accès aux données du PMSI sont plus simples et moins strictes que celles du SNIIRAM. En effet, les dispositions combinées du chapitre X de la loi du 6 janvier 1978 et du Code de la santé publique définissent deux régimes d'accès. En vertu de l'article 63 de la loi du 6 janvier 1978, l'accès à des fins statistiques d'évaluation ou d'analyse des pratiques et des activités de soins et de prévention est libre, dès lors que les données transmises sont agrégées ou ne permettent pas d'identifier les patients concernés. L'accès aux données identifiantes (qui ne peuvent en aucun cas comprendre le nom, le prénom et le NIR), quant à lui, est subordonné en vertu des articles 63 et 64 à une autorisation de la CNIL. »*[602] *Tableau 2 : Accessibilité au SNIIRAM ; Arrêté d'avril 2002*[603]

[602] Commission open data en santé, Rapport à Madame Marisol TOURAINE, Ministre des Affaires sociales et de la Santé, 9 juillet 2014, p. 18.

[603] Source : Institut des Données de Santé (IDS), disponible à partir de l'adresse suivante : http://www.institut-des-donnees-de-sante.fr/

Evolution depuis 2002 de l'arrêté donnant accès aux données du SNIIRAM et comparaison avec le PMSI

Arrêté d'avril 2002

[1] *En 2002, il n'y avait pas de données exhaustives individuelles anonymisées accessibles. Les accès et les extractions de ces données n'étaient pas possibles.*
Par ailleurs en 2002, les dispositions de la loi relative à l'informatique, aux fichiers et aux libertés alors en vigueur, n'encadraient pas le traitement des données relatives à la santé.
[2] *L'Echantillon Généraliste de Bénéficiaires n'a été crée qu'en 2005.*

		Données exhaustives individuelles anonymisées [1]	Extractions [1] (échantillons spécifiques)	Echantillon Généraliste de Bénéficiaires [2]	Données agrégées
CNAMTS[6], CCMSA[6], RSI[6], URCAM[3]		Accès possible	Autorisation CNIL	Sans objet[2]	Accès possible
Organisme poursuivant un but non lucratif	CNSA	Autorisation CNIL	Autorisation CNIL	Sans objet[2]	Autorisation CNIL
	Ministères, ARH[3]			Sans objet[2]	Accès possible
	Autres organismes (exemple : CHU, ORS, Université, etc...)			Sans objet[2]	Autorisation CNIL
Les membres de l'IDS		Autorisation CNIL	Autorisation CNIL	Sans objet[2]	Autorisation CNIL
Structures adhérant aux membres de l'IDS ou les constituant				Sans objet[2]	
26 Unions Régionales de Médecins Libéraux (URML)		Autorisation CNIL		Sans objet[2]	Accès possible[3]
17 organismes complémentaires d'assurance maladie participant au projet MONACO		Autorisation CNIL		Sans objet[2]	Autorisation CNIL
Organisme poursuivant un but lucratif (exemple : industrie du médicament et des produits de santé)		Autorisation CNIL		Sans objet[2]	Autorisation CNIL

[3] *Accès sur le champ de leur compétence régionale.*
[6] *Possibilité en plus de croisement des variables sensibles des personnes (code commune, date des soins, mois et année de naissance) uniquement pour les médecins conseils.*

869. Au regard des dispositions de l'arrêté de 2002 relatif au SNIIRAM, pouvaient être destinataires de l'ensemble des informations relatives aux bénéficiaires de soins, exclusivement « les médecins-conseils [des échelons locaux et régionaux des services médicaux des caisses] et les personnels placés sous leur responsabilité ainsi que les agents administratifs des caisses des différents régimes de base d'assurance maladie et des unions régionales des caisses d'assurance maladie [URCAM] nommément désignés, suivant leur rattachement administratif, par les directeurs ou les agents comptables des caisses et des unions ».

870. Cette autorisation d'accès permanent aux données « anonymisées » était justifiée par le fait que ceux-ci disposaient déjà de ces informations dans leurs autres bases, en particulier au niveau régional. Ainsi, *« l'accès par le SNIIRAM leur permet[tait] de disposer d'une vision plus complète et plus fiable puisqu'interrégimes »*[604]. Cet accès avait pour contrepartie la soumission des personnels des organismes d'assurance maladie au secret professionnel. En effet, bien que les dispositions concernées figurent à l'article L. 161-29 du Code de la sécurité sociale, l'obligation de secret à laquelle sont tenus les personnels (médecins et

[604] Cour des Comptes, Le partage des données entre les systèmes d'information de santé – La sécurité sociale, septembre. Septembre 2007, p. 138.

agents administratifs) des organismes d'assurance maladie n'est pas limitée aux informations dont ils auraient pris connaissance lors de la mise en œuvre de traitements de données à caractère personnel relatifs à la détermination des pathologies diagnostiquées, des actes effectués et des prestations réalisées au bénéfice d'une personne déterminée. Celle-ci présente un caractère général de par sa formulation et concerne également les données contenues dans le SNIIRAM. Ainsi, les médecins et agents administratifs des organismes d'assurance maladie peuvent avoir accès, dans le cadre de leurs missions de contrôle aux données de la base sans pour autant pouvoir en révéler le contenu. Le secret est présenté comme une garantie supplémentaire permettant de préserver la vie privée des bénéficiaires et autorisant ainsi la mise en œuvre d'un accès élargi aux données de la base. Il constitue une mesure de dissuasion permettant une hypothétique condamnation pénale *a posteriori* en cas de violation de cette obligation[605].

871. Cette garantie était accompagnée d'une mesure de protection *a priori,* fondée sur une double restriction visant à minimiser le risque d'atteinte à la vie privé. Ainsi, en ce qui concerne la formulation de requêtes au niveau de la base, *« seuls les médecins-conseils et les personnels placés sous leur responsabilité, nommément désignés par les médecins responsables selon l'organisation des régimes, [étaient] autorisés à effectuer des recherches mettant en œuvre simultanément plus d'une des trois variables sensibles (code commune, date des soins, mois et année de naissance) avec d'autres données »*[606].

872. En ce qui concerne les services de l'État, les Agences Régionales d'Hospitalisation (ARH) et les Unions Régionales de Médecins Libéraux (URML), les catégories de professionnels identifiés au sein de l'arrêté

[605] P.-L. BRAS, A. LOTH, *Rapport sur la gouvernance et l'utilisation des données de santé,* septembre 2013, p. 28.

[606] Arrêté du 11 avril 2002 relatif à la mise en œuvre du système national d'information inter-régimes de l'assurance maladie, art, artart. 4. .

pouvaient accéder aux données mais exclusivement sous une forme agrégée. Enfin, les autres organismes pouvaient également accédés à ses données mais à la condition d'obtenir l'autorisation préalable de la CNIL. Comme l'IDS le fait, à juste titre, remarquer au sein du tableau synthétique reproduit ci-dessus (cf. tableau 2 : Arrêté d'avril 2002), la loi relative à l'informatique, aux fichiers et aux libertés ne comportait initialement pas de dispositions spécifiques réglementant le traitement de données à caractère personnel relative à la santé. Ces dispositions ont été introduites tardivement, en 2004, lors de la transposition de la directive de 1995. Ainsi, à l'exception des droits d'accès précédemment développés, les autres organismes habilités à consulter les données conservées dans le système devaient obtenir au préalable l'autorisation de la CNIL. La base était, par conséquent, accessible à concurrence des données disponibles, selon des modalités distinctes et en fonction de la qualité des organismes auxquels appartenaient les professionnels souhaitant en consulter le contenu.

873. Au grès des réformes successives, les motivations et conditions d'accès au SNIIRAM se sont développées et complexifiées au point d'en rendre la compréhension confuse et les modalités contestées. Ainsi, entre la parution du premier arrêté de mise en œuvre du SNIIRAM en 2002 et la réforme résultant de la loi de 2016, on peut dénombrer pas moins de huit arrêtés successifs qui ont élargi le périmètre initial des données disponibles, étendu la liste des organismes habilités à en connaître et multiplié les modalités d'accès.

<table>
<tr><th colspan="6">Arrêté de juin 2005
[4] L'IDS n'a été installé qu'en mai 2007. Entre 2005 et 2007, il n'était donc pas possible d'accéder aux données du SNIIRAM pour les organismes relevant du champ de compétence de l'institut.</th></tr>
<tr><th colspan="2"></th><th>Données exhaustives individuelles anonymisées</th><th>Extractions (échantillons spécifiques)</th><th>Echantillon Généraliste de Bénéficiaires</th><th>Données agrégées</th></tr>
<tr><td colspan="2">CNAMTS[6], CCMSA[6], RSI[6], URCAM[3]</td><td>Accès possible</td><td>Autorisation CNIL</td><td>Accès possible</td><td>Accès possible</td></tr>
<tr><td rowspan="3">Organisme poursuivant un but non lucratif</td><td>CNSA</td><td>Accès possible</td><td rowspan="3">Approbation IDS[4] et autorisation CNIL</td><td>Accès possible</td><td>Accès possible</td></tr>
<tr><td>Ministères, agences (AFSSAPS, HCAAM, INVS), grands organismes de recherche (CNRS, INSERM, IRDES…)…</td><td>Pas d'accès</td><td>Accès possible</td><td>Accès possible</td></tr>
<tr><td>Autres organismes (exemple : CHU, ORS, Université, etc…)</td><td>Pas d'accès</td><td>Approbation IDS[4] et autorisation CNIL</td><td>Approbation IDS[4] et autorisation CNIL</td></tr>
<tr><td colspan="2">Les membres de l'IDS</td><td>Pas d'accès</td><td rowspan="5">Pas possible ? / Approbation IDS[4] et autorisation CNIL ?</td><td>Pas d'accès[4]</td><td>Pas d'accès[4]</td></tr>
<tr><td colspan="2">Structures adhérant aux membres de l'IDS ou les constituant</td><td>Pas d'accès</td><td>Pas d'accès</td><td>Pas d'accès</td></tr>
<tr><td colspan="2">26 Unions Régionales de Médecins Libéraux (URML)</td><td>Pas d'accès</td><td>Pas d'accès</td><td>Accès possible[3]</td></tr>
<tr><td colspan="2">17 organismes complémentaires d'assurance maladie participant au projet MONACO</td><td>Pas d'accès</td><td>Pas d'accès</td><td>Pas d'accès</td></tr>
<tr><td colspan="2">Organisme poursuivant un but lucratif (exemple : industrie du médicament et des produits de santé)</td><td>Pas d'accès</td><td>Pas d'accès</td><td>Pas d'accès</td></tr>
<tr><td colspan="6">[5] Accès sur le champ de leur compétence régionale.
[6] Possibilité en plus de croisement des variables sensibles des personnes (code commune, date des soins, mois et année de naissance) uniquement pour les médecins conseils.</td></tr>
</table>

Tableau 3 Accessibilité au SNIIRAM : Arrêté de juin 2005

874. En 2005, suite à la création de la Caisse nationale de solidarité pour l'autonomie (CNSA) par la loi du 30 juin 2004[607] et à l'adoption de la loi n°2004806 du 9 août 2004 relative à la politique de santé publique, un premier élargissement des droits d'accès a été réalisé par arrêté[608]. De la sorte, les médecins-conseils, des personnels placés sous leur responsabilité ainsi que des agents administratifs de la CNSA disposaient, dans les mêmes termes, de droits équivalents à ceux reconnus aux personnels des organismes d'assurance maladie par l'arrêté de 2002. Ces droits avaient pour objet de permettre aux personnels de la Caisse de réaliser son objet social, et ainsi de financer l'aide à la perte d'autonomie des personnes âgées et des personnes handicapées.

875. Concomitamment, afin de répondre aux besoins des organismes de réaliser des études longitudinales et des recherches et de reconstituer le parcours de soins des patients l'arrêté, en son article 3, autorise la création

[607] Loi n° 2004-626 du 30 juin 2004 relative à la solidarité pour l'autonomie des personnes âgées et des personnes handicapées.

[608] Arrêté du 20 juin 2005 relatif à la mise en œuvre du système national d'information inter-régimes de l'assurance maladie.

un « échantillon généraliste […] représentatif des personnes protégées des régimes est constitué, afin d'assurer le suivi de la consommation de soins et des taux de recours aux soins. Sa durée de conservation est de vingt ans au-delà de l'année en cours ». Cet échantillon a été constitué à partir d'un sondage au 1/97^{e} sur le NIR des bénéficiaires de l'Assurance maladie.

876. L'accès à l'échantillon par les médecins-conseil ainsi que les agents administratifs habilités des caisses des différents régimes de base d'Assurance maladie ont accès à l'ensemble des données constituant l'EGB.

877. L'évolution substantielle de ces accès, résulte, de manière générale, de l'évolution des finalités de ce système. En effet, l'arrêté de 2005 adjoint aux finalités principales que sont l'amélioration de la qualité des soins et de la gestion de l'assurance maladie une nouvelle finalité relative à l'amélioration de la gestion des politiques de santé avec, pour sous-finalités, l'appréciation de la qualité des soins dispensés, l'adéquation entre l'offre de soins et la demande et l'économie de la santé notamment dans l'objectif de maitriser les dépenses de santé. Ces finalités révèlent l'objectif principal de la réglementation ainsi, bien que le caractère privé des mesures de protection de l'information, guidé par la préservation la vie privée soit important, la conception publiciste semble désormais prédominante. La réglementation parait dorénavant tendre à la préservation de la confiance dans le système de santé et, dans l'utilisation qu'il fait des outils numériques afin de parvenir à son efficience ainsi qu'à sa pérennité. Elle opère, en conséquence, un changement de paradigme en s'efforçant, d'une part, de faire de l'accès aux données de santé un principe au moyen de la diversification des finalités des traitements de données de santé, par l'accroissement des droits et des motifs d'accès et par la standardisation des modalités d'accès aux données de santé des bénéficiaires. D'autre part, elle a recours aux concepts de sécurité et de secret professionnel. Elles démontrent également que la donnée de santé constitue une information à valeur ajoutée qui dépasse le cadre du soin ou de la recherche et, est susceptible de constituer un moyen d'apprécier la

qualité du système de santé, d'adapter la politique de santé publique et de maitriser les dépenses de santé.

Tableau 4 : Accessibilité au SNIIRAM : Arrêté de septembre 2012

Arrêté de septembre 2012					
		Données exhaustives individuelles anonymisées	Extractions (échantillons spécifiques)	Echantillon Généraliste de Bénéficiaires	Données agrégées
CNAMTS[6], CCMSA[6], RSI[6]		Accès possible	Autorisation CNIL	Accès possible	Accès possible
Organisme poursuivant un but non lucratif	CNSA, agents et/ ou médecins salariés des ARS (ex URCAM et ARH)[3 et 5], INVS	Accès possible	Approbation IDS et autorisation CNIL	Accès possible	Accès possible
	Ministères, agences (ANSM - ex-AFSSAPS ; HCAAM…), grands organismes de recherche (CNRS, INSERM, IRDES…)…	Pas d'accès		Accès possible	Accès possible
	Autres organismes (exemple : CHU, ORS, Université, etc…)	Pas d'accès		Approbation IDS	Approbation IDS
Les membres de l'IDS		Pas d'accès	Pas possible ? / Approbation IDS et autorisation CNIL ?	Accès possible	Accès possible
Structures adhérant aux membres de l'IDS ou les constituant		Pas d'accès		Pas d'accès[5]	Accès possible
26 Unions Régionales de Professionnels de Santé (médecins) : ex URML		Pas d'accès		Pas d'accès	Accès possible[3]
17 organismes complémentaires d'assurance maladie participant au projet MONACO		Pas d'accès		Pas d'accès	Accès possible
Organisme poursuivant un but lucratif (exemple : industrie du médicament et des produits de santé)		Pas d'accès		Pas d'accès	Pas d'accès

[3] *Accès sur le champ de leur compétence régionale.*
[5] *Hormis pour la FNMF.*
[6] *Possibilité en plus de croisement des variables sensibles des personnes (code commune, date des soins, mois et année de naissance, date de décès) uniquement pour les médecins conseils.*
[8] *Les agents des ARS ont accès aux données agrégées et à l'EGB du SNIIRAM. Seuls les médecins salariés des ARS ont accès aux données du DCIR.*

878. À la suite de l'adoption de la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, les médecins, membres du personnel des ARS désignés par les directeurs généraux des ARS se sont vus également reconnaitre le droit d'accéder au système national d'information.

879. *« L'agence régionale de santé a accès aux données nécessaires à l'exercice de ses missions contenues dans les systèmes d'information des établissements de santé (…) ainsi que des organismes d'assurance maladie et de la Caisse nationale de solidarité pour l'autonomie, notamment à ceux mentionnés aux articles L. 161-28-1 du code de la sécurité sociale (…). Cet accès est assuré dans des conditions garantissant l'anonymat des personnes (…) dans le respect des dispositions de la loi n°*

78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (…) »[609]

880. L'arrêté du 11 juillet 2012 est venu préciser les modalités de ce droit d'accéder aux données des bénéficiaires et de procéder, sur autorisation préalable de la CNIL et de l'IDS, à des extractions d'échantillons spécifiques (cf. tableau 4 figurant ci-dessus). Ils se sont vu autorisé, uniquement sur le champ de leur compétence régionale, à effectuer des recherches mettant en œuvre, simultanément plus d'une des quatre variables sensibles (code commune, date des soins, mois et année de naissance, date de décès) dans le cadre d'une charte d'engagements pour la mise à dispositions et les principes d'utilisation des données issues du SNIIRAM.

881. Ce droit d'accès, de recherche et d'extraction obéissait à un régime spécial puisque ces opérations devaient être strictement nécessaires à l'accomplissement de leurs missions.

882. *« Les agents de l'agence régionale de santé ayant la qualité de médecin n'ont accès aux données de santé à caractère personnel que si elles sont strictement nécessaires à l'accomplissement de leurs missions, dans le respect de l'article 226-13 du code pénal. »*[610]

883. Suite à l'arrêté du 19 juillet 2013, l'ensemble des membres du personnel des ARS ont bénéficié d'un accès aux données agrégées et à l'EGB les médecins pouvant seuls accéder à l'ensemble des données[611]. Toutefois, ce dispositif global d'accès accordé aux personnels des ARS s'est montré peu efficace et peu cohérent en raison d'une interprétation restrictive réalisée par la CNIL en ce qui concerne les dispositions

[609] C. santé publ, art.article L. 1435-6.

[610] Ibid.

[611] Voir en ce sens, J. LE MENN, A. MILON, Rapport d'information fait au nom de la misión d'évaluation et de contrôle de la sécurité sociale et de la commission des affaires sociales sur les agences regionales de santé, n° 400, Sénat, Session ordinaire de 2013-2014. Voir en ce sens,

précitées relatives aux recherches impliquant le croisement de variables dites sensibles. Ainsi, elle a considéré que les médecins concernés n'avaient pas, dans le cadre de leurs missions, à connaître et réaliser des croisements de variables dites sensibles. « Les statisticiens des ARS venus des anciennes Unions régionales des caisses d'assurance maladie notamment, qui sont tenus au secret professionnel au même titre que les médecins et qui avaient naguère un accès au SNIIRAM (et aux bases régionales de l'assurance maladie), l'ont ainsi perdu »[612].

884. En témoigne la rédaction de l'article 48 de la loi de financement de la sécurité sociale pour 2013[613]. Ses dispositions spécifiques ont été intégrées concernant l'expérimentation menée dans le cadre du programme PAERPA afin de permettre aux médecins des ARS d'accéder aux données relatives au parcours.

Arrêté de juillet 2013					
		Données exhaustives individuelles anonymisées	Extractions (échantillons spécifiques)	Echantillon Généraliste de Bénéficiaires	Données agrégées
CNAMTS[6], CCMSA[6], RSI[6]		Accès possible	Autorisation CNIL	Accès possible	Accès possible
Organisme poursuivant un but non lucratif	CNSA, agents et/ ou médecins salariés des ARS (ex URCAM et ARH)[3 et 8], INVS, ANSM et HAS	Accès possible	Approbation IDS et autorisation CNIL	Accès possible	Accès possible
	Ministères, agences (ATIH, HCAAM…), grands organismes de recherche (CNRS, INSERM, IRDES…)…	Pas d'accès		Accès possible	Accès possible
	Autres organismes (exemple : CHU, ORS, Université, etc…)	Pas d'accès		Approbation IDS	Approbation IDS
Les membres de l'IDS		Pas d'accès	Pas possible ? / Approbation IDS et autorisation CNIL ?	Accès possible	Accès possible
Structures adhérant aux membres de l'IDS ou les constituant		Pas d'accès		Pas d'accès[5]	Accès possible
Unions Régionales de Professionnels de Santé (toute profession de santé)		Pas d'accès		Pas d'accès	Accès possible[3]
17 organismes complémentaires d'assurance maladie participant au projet MONACO		Pas d'accès		Pas d'accès	Accès possible
Organisme poursuivant un but lucratif (exemple : industrie du médicament et des produits de santé)		Pas d'accès		Pas d'accès	Pas d'accès

[1] *Accès sur le champ de leur compétence régionale.*
[3] *Hormis pour la FNMF.*
[4] *Possibilité en plus de croisement des variables sensibles des personnes (code commune, date des soins, mois et année de naissance, date de décès) uniquement pour les médecins conseils. Pour l'INVS, possibilité en plus de croisement des variables sensibles des personnes à titre expérimental, pour une durée de 3 ans, uniquement pour les médecins.*
[5] *Les agents des ARS ont accès aux données agrégées et à l'EGB du SNIIRAM. Seuls les médecins salariés des ARS ont accès aux données du DCIR.*

Tableau 5 : Accessibilité au SNIIRAM : Arrêté de juillet 2013[614]

612 P.-L. BRAS, A. LOTH, Rapport sur la gouvernance et l'utilisation des données de santé, septembre 2013, p. 36.

613 Loi n° 2012-1404 du 17 décembre 2012 de financement de la sécurité sociale pour 2013.

614 Source : D. POLTON, *« Le SNIIRAM et les bases de données l'assurance maladie : fonctionnement, potentiel et limites »*, Septième école d'été

Arrêté de février 2014					
		Données exhaustives individuelles anonymisées	Extractions (échantillons spécifiques)	Echantillon Généraliste de Bénéficiaires	Données agrégées
CNAMTS[6], CCMSA[6], RSI[6]		Accès possible	Autorisation CNIL	Accès possible	Accès possible
Organisme poursuivant un but non lucratif	CNSA, agent et/ou médecins salariés des ARS (ex URCAM et ARH)[3,6 et 8], INVS[6] ANSM, HAS	Accès possible	Approbation IDS et autorisation CNIL	Accès possible	Accès possible
	Ministères, agences (ATIH, HCAAM…), grands organismes de recherche (CNRS, INSERM, IRDES…)…	Pas d'accès		Accès possible	Accès possible
	Autres organismes (exemple : CHU, ORS, Université, etc…)	Pas d'accès		Approbation IDS	Approbation IDS
Les membres de l'IDS		Pas d'accès	Pas possible ? / Approbation IDS et autorisation CNIL ?	Accès possible	Accès possible
Structures adhérant aux membres de l'IDS ou les constituant		Pas d'accès		Pas d'accès[5]	Accès possible
Unions Régionales de Professionnels de Santé (toute profession de santé)		Pas d'accès		Pas d'accès	Accès possible[3]
17 organismes complémentaires d'assurance maladie participant au projet MONACO		Pas d'accès		Pas d'accès	Accès possible
Organisme poursuivant un but lucratif (exemple : industrie du médicament et des produits de santé)		Pas d'accès		Pas d'accès	Pas d'accès

[3] *Accès sur le champ de leur compétence régionale.*
[3] *Hormis pour la FNMF.*
[6] *Possibilité en plus de croisement des variables sensibles des personnes (code commune, date des soins, mois et année de naissance, date de décès) uniquement pour les médecins conseils.*
Pour les ARS, dans le cadre des expérimentations PAERPA, possibilité en plus de croisement des variables sensibles des personnes pour les médecins salariés des ARS et le personnel placé sous leur responsabilité.
Pour l'INVS, possibilité en plus de croisement des variables sensibles des personnes à titre expérimental, pour une durée de 3 ans, uniquement pour les médecins.
[5] *Les agents des ARS ont accès aux données agrégées et à l'EGB du SNIIRAM. Seuls les médecins salariés des ARS ont accès aux données du DCIR.*

885. *Tableau 6 Accessibilité au SNIIRAM : Arrêté de février 2014*

886. L’arrêté du 19 juillet 2013[615] relatif à la mise en œuvre du Système national d'information interrégimes de l'assurance maladie, démontre les limites d’un accès organisé autour d’un système analogue au fonctionnement de l’article 378 du Code pénal fondé sur un principe général d’interdiction d’accéder et de traiter des données issues du SNIIRAM faisant l’objet de dérogations obéissant à des règles complexes et multiples.

Adéquation du SNIIRAM aux besoins des acteurs[7]	Données exhaustives individuelles anonymisées	Extractions (échantillons spécifiques)	Echantillon Généraliste de Bénéficiaires	Données agrégées
A des fins d'études et recherches en santé publique, et de veille sanitaire	****	****	**	*
A des fins de pilotage financier	****	****	***	**

[7] *Les * constituent une hiérarchie d'utilité et non un jugement en valeur absolue.*

Comparaison avec le PMSI - Situation en août 2013	Données détaillées exhaustives anonymisées	Données agrégées
CNAMTS, Ministères…	Accès possible	Accès possible
Autres organismes poursuivant un but lucratif ou non	Autorisation CNIL	Accès possible

méditerranéenne d’information en santé, *Système d’information : de la clinique à la santé publique*, 15 juillet 2013.

615 Arrêté du 19 juillet 2013 relatif à la mise en œuvre du Système national d'information interrégimes interrégimesde l'assurance maladie.

887. *Tableau 7 : Liste des organismes ayant accès aux bases de données du SNIIRAM (arrêté du 19 juillet 2013)*[616]

	Suivi des dépenses	Suivi de l'activité par offreur de soins (1)	Echantillon généraliste des bénéficiaires	Données individuelles exhaustives (DCIR +PMSI)
Régimes de base d'assurance maladie	X	X	X	X
Ministères (santé, sécurité sociale, agriculture, finances)	X	X	X	
dont Direction de la Recherche des Etudes, de l'Evaluation et des Statistques (DREES)	X	X	X	Attente accord CNIL et arrêté
Agences Régionales de Santé (ARS)	X	X	X	X (pour médecins et sur périmètre régional)
Haute autorité de santé (HAS)	X	X	X	X
Agence nationale de sécurité du médicament (ANSM)	X	X	X	X
Institut de veille sanitaire (InVS)	X	X	X	X
Agence technique de l'information sur l'hospitalisation (ATIH)	X	X	X	Attente accord CNIL et arrêté
Agence de la biomédecine	X	X	X	
Haut conseil pour l'avenir de l'assurance maladie (HCAAM)	X	X	X	
Institut national du cancer (INCa)	X	X	X	
Fonds CMU	X	X	X	
Institut des données de santé (IDS)	X	X	X	
Union nationale des professions de santé (UNPS)	X	X	X	
Syndicats de professionnels libéraux membres de l'UNPS	X	X		
Unions régionales des professions de santé (toutes professions)	X	X		
Fédérations hospitalières (FHF,FHP, FEHAP)	X	X	X	
Etablissements membres des fédérations hospitalières	X	X		
Union Nationale des Organismes Complémentaires d'Assurance Maladie (UNOCAM)	X	X	X	
Fédérations constitutives de l'UNOCAM (FNMF, CTIP, FFSA) signataires de la charte d'engagement entre l'assurance maladie obligatoire et les assureurs maladie complémentaires	X	X	X	
Organismes complémentaires contributeurs de données membres des fédérations constitutives de l'UNOCAM signataires de la charte d'engagement entre l'assurance maladie obligatoire et les assureurs maladie complémentaires	X	X	X	
Collectif interassociatif sur la santé CISS	X	X	X	
Associations adhérentes du CISS	X	X		
Institut national de la santé et de la recherche médicale (INSERM)	X	X	X	
Centre national ed la recherche scientifique (CNRS)	X	X	X	
Institut de Recherche et Documentation en Economie de la Santé (IRDES)	X	X	X	
Centre technique d'appui et de formation des centres d'examens de santé (CETAF)	X	X	X	
Observatoire des drogues et toxicomanies	X	X	X	

(1) identification nominative des professionnels réservée aux régimes d'assurance maladie, géolocalisation à l'IRIS pour l'INVS et médecins des ARS (URPS en attente accord CNIL et arrêté), au département pour les autres organismes.

[616] Source : P.-L. BRAS, A. LOTH, Rapport sur la gouvernance et l'utilisation des données de santé, septembre 2013, p. 34.

888. Ainsi, à partir de 2013, incité par les dispositions de la directive du 26 juin 2013[617], un consensus s'est dégagé. Celui-ci résidait dans les constatations, selon lesquelles, les dispositions concernant l'accès aux données pouvaient paraître peu protectrices au regard des risques de ré-identification et des conséquences susceptibles d'en découler pour la vie privée des personnes. Toutefois, les différents acteurs ont également aboutit à la conclusion que ces mêmes dispositions pouvaient constituer des obstacles excessifs à la réalisation d'activités de recherche et de veille sanitaire. Nous considérons, pour notre part que ces obstacles, techniques, réglementaires et procéduraux résidaient essentiellement dans la simple méfiance à l'égard de potentiels mésusages pouvant résulter de l'exploitation des données du système national.

889. En conséquence, l'approche qui préside l'accès au Système National des Données de Santé (SNDS) procède d'un principe de mise à disposition des données de santé.

§ 2. Un accès facilité pour la recherche

890. **L'accès aux données dans l'intérêt général.** L'exploitation des bases nationales de données de santé et médico-administratives ne peuvent constituer un moyen de réponse à toutes les études et recherches. L'ouverture de ces bases est toutefois nécessaire aux chercheurs qui ont besoin de disposer de quantités d'informations de la vie réelle afin de mener à bien leurs études et recherches. L'accès aux données qui sont conservées au sein de ces bases, dans le respect des droits et libertés des personnes peut également s'avérer indispensable pour élever le niveau de connaissance des pouvoirs publics et ainsi éclairer leurs décisions dans la conception des politiques de santé et dans l'évaluation de leurs effets. La bonne utilisation de ces données peut apporter une aide précieuse dans la

[617] Dir. (UE). PE et Cons. UE 2013/37, 26 juin 2013 modifiant la directive (dir.) 2003/98/CE concernant la réutilisation des informations du secteur public.

recherche de l'efficience du système de santé, dans la connaissance et l'évaluation de l'offre et de la qualité de soins, ainsi que dans l'efficacité de la veille sanitaire et de la santé publique en général.

891. *« Si l'on veut progresser dans le domaine de la santé, il faut que les chercheurs aient accès, dans des conditions simples et rapides, aux données qui leur sont indispensables, notamment pour évaluer les effets exacts de tel traitement, tel médicament ou tel parcours de santé. L'enjeu est bien de leur permettre d'avoir accès à des données détaillées, afin qu'ils puissent connaitre les parcours de soins suivis par les patients atteints, par exemple, de certains cancers, de pathologies vasculaires ou encore de troubles psychiatriques, et comparer l'efficacité de différents traitements et parcours de soins. »*[618]

892. **Le SNIIRAM contraintes techniques nuisant à la disponibilité des données.** Nous l'avons démontré précédemment, l'accessibilité au SNIIRAM a progressivement été étendue au cours des vingt dernières années. Antérieurement à la loi de modernisation de notre système de santé, la recherche française se heurtait à de nombreuses difficultés, à la fois juridico-organisationnelles, techniques et financières[619]. D'un point de vue technique, l'exploitation des données soulevait bon nombre d'obstacles. Ainsi, identifier les personnes, extraire les données pertinentes et les mettre en forme afin de réaliser des analyses de qualité n'est pas chose aisée[620].

---

[618] Compte rendu intégral de la séance du jeudi 1er octobre 2015, Sénat, *JORF*, n° 103 S, déclaration de M.M. Yves Daudigny, p. 9049.

[619] Voir également M. GOLDBERGGoldberg, M. COEURET-PELLICERCoeuret-Pellicer, C. RIBETRibet, M. ZINS, « Zins. Cohortes épidémiologiques et bases de données d'origine administrative : Un rapprochement potentiellement fructueux », médecine/sciences, avril 2012, vol. 28, n° 4, p. 430.

[620] Pour avoir une appréciation des difficultés techniques rencontrées par les organismes de recherche afin d'obtenir une mise à disposition effective des données conservées au sein des bases nationales, il convient de consulter : Pour

893. *« L'extraction proprement dite des données des bases nécessite également une participation active des organismes gestionnaires des bases de données, car cette activité implique diverses étapes techniques qui peuvent être lourdes et qui nécessitent des moyens humains, et une organisation rigoureuse : formulation des requêtes en fonction des besoins des utilisateurs, tests, production, vérifications, transferts sécurisés. »*

894. **Une gouvernance de du SNIRAM imprécise.** Concernant les difficultés juridiques, l'article L. 161-28-1 du Code de la sécurité sociale créant le

895. SNIIRAM prévoit que ce système est *« mis en place par les organismes d'assurance maladie »* et que ses *« modalités de gestion et de renseignement »* sont définies *« conjointement par protocole passé entre au moins la Caisse nationale de l'assurance maladie des travailleurs salariés, la Caisse centrale de mutualité sociale agricole et la Caisse nationale du régime social des indépendants, [elles] sont approuvées par un arrêté du ministre chargé de la sécurité sociale »*[621].

896. L'insertion de ces dispositions relatives au SNIIRAM au sein d'une section du Code de la sécurité sociale relative au *« Système d'information de l'assurance maladie et cartes de santé »* ainsi que les dispositions de l'article 5 de l'arrêté du 19 juillet 2013 par lesquelles la CNAMTS s'est vue confier la gestion technique de la base, sont à l'origine d'une confusion entre l'administration et la propriété de la base de données. Cette confusion est à l'origine du retard considérable pris dans

une meilleure utilisation des bases de données administratives et *médico*medico-administratives nationales pour la sante publique et la recherche, Haut conseil de la santé publique, mars 2012, p. 9.

[621] CSS, art. L. 161-28-1.

l'exploitation du SNIIRAM au bénéfice de la santé publique et de la recherche.

897. *« La CNAMTS gère en pratique le SI qui est placé sous sa responsabilité. Même si le protocole rappelle qu'il s'agit d'une "base nationale" (…), il est clair qu'une confusion s'est installée entre la gestion et la propriété de la base. On peut voir un exemple de cette logique propriétaire dans l'institution du COPIIR SNIIRAM qui régule les accès au SI sur la base d'un partage des voix par tiers entre État/assurance maladie/professionnels de santé. [...] Il est donc nécessaire de rappeler que le SI est un "bien public" constitué en vue des bénéfices collectifs que la collectivité peut attendre de son exploitation. »*[622]

898. Sous l'angle juridico-organisationnel, ces difficultés concernent pour l'essentiel les modalités d'obtention d'une autorisation d'accès aux données à caractère personnel relatives à la santé conservées au sein des bases de données nationales. Les organismes sollicités, leur nombre et les modalités procédurales dépendent de multiples facteurs et varient en fonction du gestionnaire de la base, des finalités de l'étude ou de la recherche ce qui rend l'accès complexe.

899. **Une multiplicité d'organismes pour gérer les demande d'avis.** De la sorte, plusieurs organismes étaient compétents pour donner un avis sur les demandes d'accès aux données du SNIIRAM. L'IDS institué par la loi de 2011[623] était sollicité pour les études qualifiées comme relevant de l' « offre standard », c'est à dire des tableaux de bord, des *datamarts* et de l'EGB. Pour les autres études, les organismes consultés dépendaient du type d'étude menée. Ainsi, de manière analytico-synthétique, les projets

[622] P.-L. BRAS, A. LOTH, Rapport sur la gouvernance et l'utilisation des données de santé, septembre 2013, p. 48.

[623] Loi n° 2011-525 du 17 mai 2011 de simplification et d'amélioration de la qualité du droit.

de recherche nécessitant le traitement de données à caractère personnel directement ou indirectement personnelles relevant de l'ancien chapitre IX de la loi relative à l'informatique, aux fichiers et aux libertés étaient soumis à l'avis préalable du Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé (CCTIRS). Son rôle était d'éclairer, au moyen d'un avis sur la méthodologie de recherche, la CNIL sur la finalité et les justifications du traitement projeté, la nature des données de santé utilisées ainsi que leur intérêt pour l'étude ou la recherche envisagée. La CNIL se prononçait ensuite sur l'autorisation du traitement projeté et la nécessité de déroger au secret professionnel, la demande était transmise à l'IDS qui procédait à la priorisation des demandes. Dans l'éventualité ou au cours de la recherche ou de l'étude, un complément de projets, non prévue dans le projet initial, nécessitait une extraction particulière de données issues du SNIIRAM, en vue d'alimenter une cohorte, un nouveau circuit de demande devait alors être formulé auprès des différents organismes, sans que le CCTIRS ne soit, cette fois-ci, consulté.

900. Les projets de recherche portant sur des données anonymisées relevant de l'ancien chapitre X de la loi du 6 janvier 1978 étaient quant à eux soumis à l'avis préalable de l'IDS dont l'une des missions consiste à faciliter l'accès aux données de santé aux organismes de recherche. Le dossier de demande était ensuite communiqué à la CNIL pour avis puis à l'IDS pour priorisation de l'accès.

901. Enfin, concernant les demandes des services statistiques ministériels tels que la Direction de l'animation de la recherche, des études et des statistiques (Dares), l'obtention de l'avis préalable du Conseil national de l'information statistique était nécessaire, la demande devait ensuite être adressée à la CNIL puis à l'IDS.

902. *« L'architecture actuelle de cette gouvernance est largement considérée comme complexe. Ainsi le rapport Bras qualifie les règles actuelles de "touffues et contestées". Au regard des données personnelles de santé, certaines dispositions peuvent paraître peu protectrices, d'autres au contraire paraissent élever des obstacles excessifs aux besoins de la recherche. »*[624]

903. **Une procédure d'accès couteuse.** Au sujet des difficultés financières, les contraintes d'accès aux bases de données médico-administratives obligeaient les laboratoires de recherche et chercheurs à prospecter d'autres moyens d'acquérir des données, généralement en réalisant des entretiens de collecte de données auprès d'un nombre conséquent de personnes afin d'obtenir des informations pertinentes relatives à l'état de santé des personnes. Cela n'était pas sans conséquence sur la recherche puisque cela engendrait, un coût nettement supérieur aux subventions qu'ils pouvaient solliciter auprès des organismes nationaux de financement de la recherche pour des études de grande dimension.

904. Au regard de ce qui précède, la Cour des comptes a dénoncé *« un retard considérable (…) pris dans l'exploitation du SNIIRAM au bénéfice de la santé publique, de la recherche »*[625]. Les données de santé et les données médico-administratives constituent, en effet, une ressource primordiale pour la recherche en santé. Cette ouverture de la base de données est nécessaire aux chercheurs qui ont besoin de disposer de quantités d'informations variées de la vie réelle, données sociales et économiques, environnementales et biologiques, relatives à la consommation de soins, etc. afin de mener à bien leurs études, évaluations

[624] P.-L. BRAS, A. LOTH, Rapport préc., p. 31.

[625] Cour des comptes, Rapport 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 : Les données personnelles de santé gérées par l'assurance maladie : Une utilisation à développer, une sécurité à renforcer, mars 2016, p. 117.

et recherches. Les bases nationales permettent également d'éprouver la sincérité des études menées par « *la reproductibilité de la preuve et (…) la constitution de cohortes significatives* ».

905. À titre d'exemple, l'accès à ces viviers de données rendent possible la réalisation d'études et de recherches *« de grande dimension et de longue durée, comme les études de cohorte qui vont continuer de se développer dans beaucoup de domaines, notamment en épidémiologie, où l'effectif envisagé de certaines cohortes ne se compte plus en dizaines, mais en centaines de milliers de sujets, une envergure comparable à ce qui existe dans plusieurs pays »*[626].

906. Elles permettent ainsi l'obtention de populations exhaustives et de données jugées fiables ainsi que l'appariement avec des enquêtes et *« la reproductibilité de la preuve et [...] la constitution de cohortes significatives »*[627].

907. À titre d'illustration, on constate que les cohortes prospectives françaises se caractérisent par une taille relativement faible, aucune ne dépassant quelques dizaines de milliers de sujets, alors que certaines cohortes prospectives dans d'autres pays peuvent atteindre plusieurs centaines de milliers de sujets, voire plus. On peut citer en Grande-Bretagne la Million Women Study, le projet UK Biobank qui a mis en place le suivi prospectif de 500 000 personnes, et la Norvegian Mother and Child Cohort Study qui a inclus 100 000 femmes à la 18e semaine de grossesse puis leurs 100 000 nouveau-nés, ainsi que 70 000 pères, soit au

[626] En ce sens, se référer à l'exemple des cohortes Gazel et Constance : M. GOLDBERG, M. ZINS, « Les cohortes généralistes en population – L'exemple des cohortes Gazel et Constance », Bull. Acad. Natle Méd., 2013, 197, n° 2, p. 299.

[627] P. MORANGE, Rapport *d'information* fait au nom de la commission des affaires sociales en conclusion des travaux de la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale, sur les données médicales personnelles inter-régimes détenues par l'assurance maladie, versées au SNIIRAM puis au Système national des données de santé (SNDS), n° 4533, Assemblée nationale, 21 févr.février 2017, p. 17.

total 270 000 personnes. La Nurses' Health Study a été mise en place aux États-Unis dès 1976 et assure le suivi prospectif de près de 250 000 infirmières. Actuellement se mettent en place en Europe de nouvelles très grandes cohortes, comme LifeGene en Suède (www.lifegene.ki.se), LifeLines aux Pays-Bas (www.lifelines.net), ou la cohorte nationale allemande, qui doivent inclure et suivre plusieurs centaines de milliers de sujets recrutés en population générale. On peut citer aussi l'exemple des pays scandinaves qui disposent de multiples registres dans le domaine de la santé, de la protection sociale ou de l'activité économique couvrant la totalité de la population de ces pays. Ces registres sont largement ouverts aux chercheurs et permettent, par appariement de ces bases de données, de constituer des cohortes dont l'effectif se compte en millions de sujets et qui sont à l'origine d'une immense bibliographie scientifique.[628]

908. **Des modalités d'accès distinctes en fonction de la finalité.** D'un point de vue procédurale, nous l'avons évoqué, ci-dessus, la loi du 6 janvier 1978 prévoyait, antérieurement à sa modification par la loi de 2016, deux modalités distinctes selon la finalité du traitement de données. Ainsi, les traitements automatisés de données nominatives ayant pour fin la recherche dans le domaine de la santé relevaient, comme nous l'avons précédemment rappelé, du Chapitre IX de la loi informatique et liberté. Les traitements de données de santé à caractère personnel à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention réalisés à partir de données conservées au sein du SNIIRAM ou du PMSI étaient régis, quant à eux, par les dispositions du Chapitre X de la même loi.

909. **Désormais un seul est même régime d'autorisation.** Il résulte des nouvelles dispositions de la loi de 1978 que les deux chapitres sont fusionnés au sein d'un unique chapitre IX qui concerne dorénavant

[628] Commission open data en santé, Rapport à Madame Marisol TOURAINE, Ministre des Affaires sociales et de la Santé, 9 juillet 2014, p. 41.

l'ensemble des « traitements de données à caractère personnel dans le domaine de la santé ».

910. Un seul et même régime d'autorisation a donc vocation à s'appliquer pour tous les types de recherche dans le domaine de la santé. Ainsi, à l'exception des recherches biomédicales interventionnelles et non interventionnelles, toutes les demandes ne relevant pas du droit d'accès permanent au Système national de données de santé, doivent, dans le cadre de la procédure standard[629], être désormais déposées auprès de l'INDS. Il s'agit des demandes d'accès aux données à caractère personnel indirectement identifiantes pour la réalisation de recherches, études ou évaluations répondant à un motif d'intérêt public et dont l'objectif contribue à l'une des finalités mentionnées au III de l'article L. 1461-1 du Code de la santé publique, à savoir, des finalités en relation avec *« 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 l'évaluation des politiques de santé et de protection sociale », « la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médicosociales », « l'information des professionnels, des structures et des établissements de santé ou médico-sociaux sur leur activité », « la 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 ».*

911. Cet institut va vérifier la complétude du dossier puis, à moins qu'une appréciation de l'intérêt public ne soit nécessaire, le transmettre sous sept jours ouvrés au Comité d'expertise pour les recherches, les

[629] Terme employé ici par opposition à la procédure simplifiée qui concerne « *les catégories les plus usuelles de traitement automatisés de données de santé à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé* » pour lesquelles *« 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° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 54-I)

études et les évaluations dans le domaine de la santé (CEREES). Notons que pour les demandes d'accès au SNDS qui sont relatives aux traitements soumis à la loi Jardé [630] et qui nécessitent la collecte de données spécifiques, celles-ci sont transmises, non pas à l'INDS mais pour avis, au Comité de protection des personnes compétent préalablement au recueil de l'avis de la CNIL.

912. Le CEREES contrairement au CCTIRS n'a plus pour unique mission d'apprécier les protocoles de recherche qui lui sont soumis du point du vue de la protection de la vie privée. Ainsi, il est également chargé d'apprécier la méthodologie de la recherche et la qualité scientifique du projet [631] . Il peut, de cette manière, être amené à formuler des recommandations destinées à faire évoluer le projet de recherche apprécié. Il dispose d'un mois à compter de sa saisine pour rendre un avis.

913. Conformément aux dispositions de l'article 54 de la loi relative à l'informatique, aux fichiers et aux libertés, après avoir rendu son avis, le CEREES ou le CPP selon le projet de recherche considéré, saisie la CNIL. La Commission peut, le cas échéant, avant d'approuver la demande d'accès, si celle-ci est fondée sur un motif d'intérêt public, saisir l'INDS pour qu'il se livre à une appréciation de l'intérêt public du projet de recherche. En effet, la loi de modernisation de notre système de santé confie à l'INDS la mission d'évaluer l'intérêt public des projets de recherche qui lui sont soumis[632]. L'INDS peut être également saisie pour cette évaluation par le Ministère de la santé, il peut également s'autosaisir. Il apprécie, dans le délai d'un mois à compter de sa saisie l'intérêt public de la demande au moyen d'un Comité d'expertise sur l'intérêt public (CEIP) qui lui est directement rattaché. Composé de dix-sept experts issus

[630] La Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine a été modifiée par l'ordonnance n° 2016-800 du 16 juin 2016.

[631] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 54-I, 2°, °al. 2 modifié par la Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

[632] C. santé publ, art. L. 1462-1.

d'organismes de droit public et de droit privé, à but lucratif et non lucratif afin d'en assurer l'indépendance[633], ce Comité a également pour mission d'établir et de maintenir *« une doctrine sur l'appréciation du caractère d'intérêt public d'une recherche, une étude ou une évaluation »*[634], et de conseiller l'Institut sur toute question d'ordre éthique à laquelle il pourrait être confronté.

914. En conclusion, pour comprendre ce nouveau dispositif d'accès aux données médico-administratives, il convient de procéder à une lecture combinée des dispositions des articles 53 à 61 de la loi du 6 janvier 1978 et 193 de loi du 26 janvier 2016. Il en résulte que la loi de modernisation de notre système de santé simplifie le dispositif antérieur de demande d'autorisation et le rend plus souple. Bien que plus agile, celui-ci n'en demeure pas moins complexe car il requiert toujours que plusieurs organismes soient mobilisés de manière successive. Par ailleurs, les modalités procédurales d'accès variant en fonction de la nature juridique du demandeur ainsi qu'en fonction de la nature des données et plus précisément de leur caractère anonymes, pseudonymes ou indirectement identifiant, la compréhension de ce dispositif n'en est que plus laborieuse. Cependant, remarquons que l'Institut national des données de santé, créé à partir de l'IDS suite à un arrêté du 20 avril 2017[649] est désormais au centre du nouveau dispositif procédural puisqu'il constitue désormais le secrétariat unique pour le dépôt et la gestion des demandes d'accès.

915. Il est également l'autorité qui autorise l'accès au SNDS[635], tandis que le CEREES a un rôle d'expertise sur la qualité scientifique des protocoles déposés par les demandeurs.

---

[633] Arrêté du 20 avril 2017 portant approbation d'un avenant à la convention constitutive du groupement d'intérêt public « Institut des données de santé » portant création du groupement d'intérêt public « Institut national des données de santé », art. 11.

[634] *Ibid.* 649

[635] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 54 modifié par la Loi n° 2016-41 du 26 janvier 2016 de

916. La composition de l'INDS diffère de celle de l'Institut des données de santé. En effet, il conserve la forme d'un groupement d'intérêt public (GIP) mais sa composition se veut beaucoup plus représentative des utilisateurs du système. Il demeure composé de l'État et des régulateurs publics, des caisses nationales d'assurance maladie (CNAM), de l'Union nationale des organismes d'assurance maladie complémentaire (UNOCAM) et de l'Union nationale des professionnels de santé (UNPS) ainsi que de représentants de la recherche. Toutefois, l'article L. 1462-1 du Code de la santé publique intègre désormais un collège des usagers composé d'un représentant de l'union nationale des associations agréées d'usagers du système de santé ainsi qu'un collège composé de représentants des industriels et des bureaux d'études. Cette extension permet une meilleure adéquation avec les besoins des différents collèges d'utilisateurs et prend en considération les attentes des utilisateurs privés. Elle témoigne également de l'ouverture du système et des bases de données médico-administratives le composant aux organismes poursuivant un but lucratif.

917. En ce qui concerne les délais d'autorisation d'accès aux données médico-administratives, sous l'égide de l'IDS, le délai entre le dépôt de dossier et la délivrance de l'autorisation d'accès pouvait varier de trois mois pour un accès à l' « offre standard » contre neuf voir douze mois en ce qui concerne l'accès effectif aux données dans le cadre d'une demande portant sur l' « offre non standard ». Au regard des dispositions des articles 53 et suivants de la loi relative à l'informatique, aux fichiers et aux libertés et compte tenu des délais laissés aux différents organismes pour se prononcer sur la demande d'accès à des fins d'étude, d'évaluation et de recherche, il faut désormais compter environ deux à deux mois et demie entre la saisine de l'INDS et la décision de la CNIL.

---

modernisation de notre système de santé;54 et Arrêté du 20 avril 2017 préc.», art. 2.

918. L'accès aux données du SNDS peut faire l'objet, dans certaines circonstances, de procédures dérogatoires ayant pour fin de simplifier et de raccourcir les délais de gestion des dossiers de demandes. C'est notamment le cas en situation d'urgence lorsque le traitement de données a pour finalité de répondre à une alerte sanitaire[636] et d'en gérer les suites[637].

919. La CNIL peut également contribuer à la création de procédures dérogatoires. A cette fin, elle voit également son pouvoir de simplification renforcé par les dispositions du IV et du V de l'article 54 de la loi de modernisation de notre système de santé et de l'article 62 de la loi Informatique et Libertés modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. Le législateur a ainsi entendu simplifier l'accès aux données médico-administratives en proposant de facilité la mise à disposition de jeux de données agrégées ou d'échantillons. En ce sens, la Commission a, conformément aux dispositions du V de l'article 54 de la loi de 1978 modifiée[638], par une délibération n° 2018-134 du 12 avril 2018, homologué une procédure d'accès simplifié a ces données agrégées et tableaux de bord ainsi qu'à l'EGB[639] du SNDS. Dans cette recherche de simplification et de souplesse,

---

[636] Pour la définition de l'alerte sanitaire, l'article 55 de la Loi n° 78-17 du 6 janvier 1978 modifiée par la loi de 2018 renvoie aux dispositions de la section 1 du chapitre III du titre Ier du livre IV de la première partie du Code de la santé publique. L'alerte sanitaire s'entendrait ainsi de *« tout événement sanitaire anormal représentant un risque potentiel pour la santé publique, quelle qu'en soit la nature »* InVS, *L'alerte sanitaire en France – Principes : Principe et organisation,»*. mai 2005, p. 12.

[637] Loi n° 78-17 du 6 janvier 1978 modifiée par la Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles, art. 55.

[638] Loi n° 78-17 du 6 janvier 1978 art. 54, V. Les dispositions de cet article ont été modifiées par la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

[639] Il est constitué de données anonymisées sur les caractéristiques sociodémographiques et médicales ainsi que la consommation de soins. Ces données sont issues de différentes bases de données composant le Système national de données de santé (SNDS). L'échantillon généraliste des bénéficiaires (EGB) recense approximativement six cent mille bénéficiaires de l'assurance maladie et, est représentatif au 1/97ème de la population française. Il comprend l'ensemble du parcours individuel de soins de ville ou en établissement de santé dans le champ de la médecine, la chirurgie et l'obstétrique (MCO) et permet ainsi

la CNIL reconnait, au moyen de cette délibération, la compétence exclusive de l'INDS. Ainsi, dans le cadre de cette procédure de gestion des demandes, l'Institut, pareillement à la procédure de droit commun, apprécie la satisfaction de plusieurs conditions telles que l'intérêt public de la recherche, de l'étude ou de l'évaluation envisagée. Il contrôle également que les données ne vont pas être utilisées pour des finalités interdites prévues au V de l'article L. 1461-1 du Code de la santé publique. Enfin, il vérifie également que le traitement de données envisagé respecte bien les dispositions relatives à l'accès aux données du référentiel de sécurité applicable au SNDS. L'Institut se voit ainsi confier les missions du CEREES, à ce titre, il va analyser la déclaration d'intérêts et apprécier la pertinence scientifique du projet. Les modalités préalables d'accès à l'EGB présentent ainsi des garanties satisfaisantes puisqu'elles ne dispensent pas le responsable de traitement de respecter les exigences attendues dans le cadre de la procédure de droit commun.

920. Cette dérogation repose donc essentiellement sur la compétence exclusive de l'INDS ce qui a pour effet de porter le délai pour bénéficier d'une autorisation de mise à disposition à quinze jours ouvrés, à compter de la réception du dossier. Ce dossier étant constitué des mêmes pièces que la demande d'accès ordinaire, si à la suite de l'examen de la demande, le dossier n'est pas approuvé au motif qu'une des conditions nécessaires pour bénéficier de la procédure simplifié fait défaut, l'INDS se retrouve incompétent. Il se trouve alors dans l'obligation d'analyser le dossier selon les conditions de la procédure d'accès de droit commun qui nécessite un avis du CEREES et par une autorisation de la CNIL. Pour des raisons de transparence l'INDS est toutefois tenue de transmettre, au moins une fois

---

de réaliser des études longitudinales et de reconstituer le parcours de soins des patients sur une période de vingt ans. Voir L. DE ROQUEFEUIL, A. STUDER, E. NEUMANN, Y. MERLIERE, *« Merlière. L'échantillon généraliste de bénéficiaires : représentativité, portée et limites », Pratiques et organisation des soins* 2009/3, p. 96.

par an, au CEREES ainsi qu'à la CNIL les approbations de mise à disposition des données de l'EGB délivrées.

921. Il en résulte que, dans le cadre de cette procédure particulière, un équilibre demeure entre la protection des droits et libertés de la personne et l'accessibilité des données. L'accès est réalisé dans un environnement maitrisé puisque les modalités d'accès à l'EGB ne permettent également pas la constitution d'un système fils du SNDS. Le responsable de traitement se voit imposer en contrepartie de la rapidité d'analyse de sa demande que l'étude, la recherche ou l'évaluation soit réalisée à partir du portail sécurisé de la CNAM. Ce cadre obligatoire constitue une garantie supplémentaire vis-à-vis de la sécurité des données et des conditions de l'autorisation d'accès. Cela permet, en effet, de limiter l'accès au portail à une durée n'excédant pas vingt-quatre mois, ce qui correspond au temps nécessaire pour mener une étude ou une évaluation, ou une recherche à partir de l'EGB. Enfin, la mise à disposition des données à travers ce portail permet également de contrôler qu'aucun croisement de plusieurs identifiants potentiels, ne soit réalisé[640].

922. La CNIL dispose également d'autres moyens de simplifier l'accès aux données. À ce titre, elle peut, au moyen d'une décision unique autoriser un même demandeur à mettre en œuvre plusieurs traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques sans qu'il soit nécessaire, pour le demandeur de solliciter l'examen préalable de l'INDS ou du CEREES. La CNIL dispose alors d'un délai de deux mois pour se prononcer. Le délai s'en trouve donc fortement réduit par rapport à la procédure standard d'accès.

923. Le traitement de ces données devra se conformer à des référentiels, règlements types et méthodologies de référence établis par la

[640] Se référer au Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé » ainsi qu'aux dispositions de l'art. R. 1461-14 C. santé publ.

CNIL en concertation avec l'INDS et des organismes publics et privés représentatifs des acteurs concernés.

924. La mise en œuvre devra être précédée (i) d'une déclaration de conformité au référentiel, règlement type ou méthodologie de référence ou (ii) d'une autorisation préalable de la CNIL. La commission peut, par décision unique, délivrer à un même demandeur une autorisation pour des traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques. Elle peut également au moyen de méthodologies de référence, constituer de véritables cahiers des charges que l'organisme, souhaitant réaliser une recherche s'engage à respecter s'il souhaite bénéficier d'un accès simplifié aux données.

925. Notons que, contrairement aux méthodologies de référence MR-005 [641] et MR-006 [642], sont exclus du champ d'application des méthodologies de référence MR-001 à MR-004 les traitements nécessitant un accès direct au SNDS ou aux de données médico-administratives le composant. Toutefois, il est possible pour les responsables de traitement de bénéficier de ces méthodologies de référence lorsque la réutilisation de données est réalisée au moyen de systèmes fils du SNDS, c'est-à-dire de Systèmes du SNDS, élargis hébergeant ou mettant à disposition des données relatives au SNDS cédées par le SNDS central[643]. Ces systèmes se caractérisent par la réutilisation de bases préconstituées qui mettent en

[641] CNIL, délib., 7 juin 2018, n° 2018-256 portant homologation d'une méthodologie de référence relative aux traitements de données nécessitant l'accès par des établissements de santé et des fédérations aux données du PMSI et des résumés de passage aux urgences (RPU) centralisées et mises à disposition sur la plateforme sécurisée de l'ATIH (MR 005).)

[642] CNIL, délib., 7 juin 2018, n° 2018-257 portant homologation d'une méthodologie de référence relative aux traitements de données nécessitant l'accès pour le compte des personnes produisant ou commercialisant des produits mentionnés au II de l'article L. 5311-1 du Code de la santé publique aux données du PMSI centralisées et mises à disposition par l'ATIH par l'intermédiaire d'une solution sécurisée (MR 006)

[643] Guide relatif au référentiel de sécurité applicable au Système national des données de santé, p. 5.

œuvre les mêmes conditions d'accès que le SNDS central[644]. À ce titre, les différentes méthodologies de référence exigences applicables au SNDS doivent être respectées, qu'il s'agisse des interdictions de traitement de données de santé su SNDS à des fins de promotion des produits mentionnés au II de l'article L. 5311-1 en direction des professionnels de santé ou d'établissements de santé ou à l'exclusion de garanties des contrats d'assurance et à la modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque. À ce titre, ces méthodologies de référence, ne dispense pas les responsables de traitement du système fils et le responsable de traitement de la nouvelle recherche utilisant les données du système fils de respecter les exigences résultant des dispositions applicables au SNDS notamment en ce qui concerne l'interdiction d'utiliser les données pour les finalités décrites au V de l'article L. 1461-1 du Code de la santé publique.

926. Afin de disposer de quelques chiffres témoignant de l'intérêt des organismes souhaitant disposés de données du SNDS, pour cette procédure simplifiée, selon les chiffres mentionnés dans son rapport d'activité[645], la CNIL a enregistré, au cours de l'année 2016, 1161 demandes comprenant 287 demandes « évaluation » et 874 demandes « recherche ». En 2017, elle a enregistré, toujours selon les chiffres figurant dans son rapport d'activité une baisse de 424 demandes par rapport à l'année 2016 soit 737 demandes d'autorisation au total, dont 156 réalisées dans le cadre des nouvelles dispositions du chapitre X de la loi relative à l'informatique, aux fichiers et aux libertés. Cette baisse s'expliquerait par la publication de nouvelles méthodologies de référence au cours de l'année 2016. Ainsi, depuis l'adoption de ces méthodologies de référence, 5 532 engagements de

[644] Le SNDS central est défini comme le *« système réunissant, organisant et mettant à disposition le SNDS. Le gestionnaire du SNDS central est la CNAMTS »* (Guide relatif au référentiel de sécurité applicable au Système national des données de santé, p. 4)..

[645] CNIL, Rapport d'activité – Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles, La Documentation française,. 2017, p. 39.

conformité ont été adressés à la CNIL (toutes MR confondues), dont 1 447 pour la seule année 2017.

927. Ainsi, par ce processus de simplification des formalités préalables dans le domaine de la recherche en santé, la CNIL offre un cadre sécurisé permettant de disposer de données issues du SNDS sans être contraint de soumettre une demande auprès de l'INDS à la seule condition de s'engager à satisfaire à l'ensemble des conditions énoncées au sein de la méthodologie de référence concernée.

929. Section 2. Une accessibilité simplifiée

930. **Un contrôle des accès réduit à deux critères.** S'agissant de données de santé, dès lors qu'elles présentent un risque de ré-identification des assurés, l'accès à ces données doit, en principe, être restreint[646]. En effet, la capacité de rapprocher un fichier ou un ensemble de données qu'on cherche à protéger d'une ré-identification au moyen, par exemple d'un rapprochement voir d'une interconnexion opérée avec d'autres fichiers dépend du niveau de sécurité qui entoure l'accès au fichier ou à la base de données. De ce fait, le législateur a recherché à créer un équilibre entre la protection de la vie privée et l'utilisation de la donnée, sans pour autant concéder à un compromis inutile au détriment des droits et libertés des personnes concernées par le traitement. Par ce moyen, il se dissocie ainsi d'un raisonnement exclusivement binaire et fait du risque de ré identification un curseur de l'accessibilité (Paragraphe 1). Cependant, compte tenu du risque que peut représenter un accès permanent au SNDS consentie aux organismes à but lucratifs, l'article 193 de la loi de 2016 fait de la nature des utilisateurs un critère discriminant (Paragraphe 2)

931. § 1. Le risque de ré-identification comme curseur

932. Le concept d' « *open data* » apparait aux États-Unis, au cours de la guerre du Vietnam. Confrontée au refus des institutions de délivrer des informations en se protégeant derrière des motivations de sécurité nationale, l'opinion publique exige que l'accès aux documents de l'administration américaine soit plus aisé. Ces revendications aboutissent à l'adoption de la loi d'accès à l'information appelée encore loi pour la liberté d'information ou « *Freedom of Information Act* » (FOIA).

---

[646] C. CASTETS-RENARD. *« Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data »,».* Revue Lamy Droit de l'immatériel, nº 108, 1er oct. 2004.

933. Adoptée le 4 juillet 1967 cette loi oblige les agences fédérales Américaines à transmettre, sous certaines conditions, leurs documents à toute personne en faisant la demande. Ce droit connait toutefois quelques exceptions, afin de préserver, entre autre chose, le secret médical ou encore de protéger la vie privée des citoyens américains.

934. Nous avions évoqué ce sujet lors de nos développements antérieurs, ce n'est qu'à la fin des années 70 au début des années 1980, que la société française a vu émerger, en matière de traitement de données nominatives, une défiance des citoyens à l'égard des pouvoirs publics, principalement suite à la révélation de l'affaire SAFARI. En réponse et aux revendications de transparence à l'égard des actions et décisions des institutions trois lois ont été successivement votées. Afin de rétablir la confiance et de réglementer l'utilisation des données publiques, ces lois sont venue encadrer les conditions de mise en œuvre de traitements de données dans le but les protéger les citoyens contre toute utilisation de l'outil informatique à des fins liberticides et contre les immixtions dans leur vie privée. Elles ont également reconnu, aux administrés, le droit d'accéder aux documents administratifs. Il s'agit, par ordre chronologique, de la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978[647], de la loi du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et notamment ses dispositions concernant l'accès aux documents administratifs[648] ainsi que la loi du 3 janvier 1979 sur les archives[649].

---

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

[648] 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.

[649] *« Les archives sont l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale, et par tout service ou organisme public ou privé, dans l'exercice de leur activité. La conservation de ces documents est organisée dans l'intérêt public tant pour les besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques ou privées, que pour la documentation*

935. Ces normes ont été ultérieurement complétées par une directive du 17 novembre 2003[650] transposée en droit français par l'ordonnance du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques[651] et par un décret du 30 décembre 2005 portant la même dénomination[652].

936. En ce qui concerne la loi relative à l'informatique aux fichiers et aux libertés, celle-ci a institué un système fondé sur le principe de finalité. En raison de ce principe, les données à caractère personnel collectées ne peuvent être recueillies et traitées que pour un usage déterminé et légitime sous peine de sanctions pénales pouvant s'élever à une peine de cinq ans d'emprisonnement et trois cent mille euros d'amende[653]. Sous son égide, la collecte le traitement de données à caractère personnel requiert également l'information préalable et de consentement de la personne concernée par le traitement de ses données à caractère personnel.

937. Au sujet de la liberté d'accéder aux données publiques[654]. Celui-ci fait l'objet de plusieurs normes de portées générales telles que les lois du 17 juillet 1978 et du 3 janvier 1979 mais aussi spéciales au domaine ou secteur d'activité considéré. Il a pour objet, de permettre la réutilisation des données collectées et traitées[670] à d'autres fins que celles initialement mise en œuvre et selon des modalités différentes, qu'il s'agisse de la nature

---

historique de la recherche. » Loi n° 79-18 du 3 janvier 1979 sur les archives, art. 1.

[650] Directive 2003/98/CE concernant la réutilisation des informations du secteur public modifiée par la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013.

[651] Ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques.

[652] Décret n° 2005-1755 du 30 décembre 2005 relatif à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, pris pour l'application de la Loi n° 78-753 du 17 juillet 1978.

[653] C. pén., art. 226-16 et suivants.

[654] Code des relations entre le public et l'administration (CRPA),) art. L. 300-2. 670 CRPA, art. L. 321-1 à R. 321-8.

des opérations de traitement projetées ou réalisées ou encore de la durée de conservation des données.

938. Utilisé les données à d'autres fins que celles explosées et envisagées au moment de leur collecte n'est pas sans poser de difficultés compte tenu du fait que le principe de finalité constitue la pierre angulaire de la loi relative à l'informatique, aux fichiers et aux libertés. Cette liberté d'accès, aux données publiques repose, par conséquent, sur cinq principes que sont la disponibilité et la gratuité de l'information afin de permettre sa réutilisation, selon un format accessible [655]. Il s'agit également de permettre son adaptabilité afin que celle-ci soit exploitable, sans discrimination [656]. De la sorte, l'autorisation d'accès à l'information publique ne peut, en principe, être subordonnée à la nature du demandeur d'accès, il peut ainsi s'agir de personnes morales ou physiques poursuivant ou non un but lucratif.

939. Le cadre réglementaire originel du traitement de l'information pose donc les fondements de la problématique de l'ouverture des données publiques en France. Il met en lumière les causes à l'origine des difficultés rencontrées ces cinquante dernières années en matière d'accès aux données médico-administratives.

940. Celle-ci résulte de la confrontation de deux logiques qui paraissent inconciliables. D'une part, le système institué par la loi du 6 janvier 1978 qui accorde une valeur supérieure à la protection des droits et libertés des personnes dont les données à caractère personnel font l'objet

---

[655] 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, ancien art. 10 (abrogé). L'accessibilité doit être à la fois technique et juridique. Elle suppose ainsi que les systèmes d'information soient interopérables, c'est-à-dire en capacité de communiquer, et communique qu'il existe un cadre juridique favorable à la communication de ces informations.

[656] *« Il importe d'établir un cadre général fixant les conditions de réutilisation des documents du secteur public afin de garantir que ces conditions seront équitables, proportionnées et non discriminatoires.»* (discriminatoire » Dir. (UE). PE et Cons. UE 2003/98/CE, 17 nov. 2003 modifiée par Dir. (UE). PE et Cons. UE 2013/37, 26 juin 2013) 673 Loi n°78-17 du 6 janvier 1978, art. 8, ,,al. 1.

d'un traitement et par confusion aux informations à caractère personnel numérisées et, d'un autre tenant, les la loi du 17 juillet 1978, qui permet l'accessibilité des archives et *lato sensu* des informations publiques.

941. Rappelons que les informations conservées au sein du SNDS comportent des données à caractère personnel relatives à la santé des assurés sociaux qui sont, par nature, des données sensibles[673]. Celles-ci sont donc régies par les dispositions de la loi du 6 janvier 1978. En conséquence, excepté quelques dérogations, principalement motivées par des considérations thérapeutiques et strictement encadrées par le règlement, ces données font, par principe, l'objet d'une interdiction de traitement. Il parait donc, en la matière, difficile de solutionner cette problématique. La réutilisation de données sa santé à d'autres fins que celles prélégitimées semble compromise, particulièrement dans un contexte de renforcement des droits et libertés de la personne à l'égard de l'exploitation de ses informations à caractère personnel.

942. Pour autant, la protection des droits et libertés des personnes concernées par le traitement de leurs données à caractère personnel et le principe de « réutilisation des informations du secteur public » résultant de la directive de 2003 ne sont pas formellement antinomiques. Effectivement, la loi relative à l'informatique aux fichiers et aux libertés ayant vocation à régir le traitement de données à caractère personnel, elle ne s'applique donc pas aux données *ab initio* ou *in fine* non identifiantes. Le principe de l'accès aux données, reposant sur l'utilisation des données publiques peut, par conséquent, concerner des données non-identifiantes.

943. À ce titre, l'article 13 de la loi du 17 juillet 1978[657] abrogé par l'ordonnance de 2016 disposait que « les informations publiques

[657] Abrogé par l'ordonnance n° 2016-307 du 17 mars 2016 portant codification des dispositions relatives à la réutilisation des informations publiques dans le Code des relations entre le public et l'administration. Cette ordonnance reprend l'essentiel des dispositions 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 au sein du Code des relations

comportant des données à caractère personnel peuvent faire l'objet d'une réutilisation soit lorsque la personne intéressée y a consenti, soit si l'autorité détentrice est en mesure de les rendre anonymes ou, à défaut d'anonymisation, si une disposition législative ou réglementaire le permet.

944. *« La réutilisation d'informations publiques comportant des données à caractère personnel est subordonnée au respect des dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique et aux libertés. »*

945. De la même manière, les nouvelles dispositions des articles du Code des relations entre le public et l'administration confirme, concernant le droit de communication, que la transmission des informations doit respecter les droits de propriété littéraire et artistique[675], et ne pas porter atteinte à la sécurité à des systèmes d'information des administrations[658], au comportement des personnes *« dès lors que la divulgation de ce comportement pourrait [leur] porter préjudice »* [659], ainsi qu'à leur sécurité, à la protection de leur vie privée ou encore au secret médical.

946. Il en résulte que, l'anonymisation, qui constitue une condition légale de l'accès et de la mise à disposition de données au public, semble la solution à cet obstacle prétendument indissoluble. Par conséquent, pour être réutilisables, les données ne doivent, en principe, pas contenir d'information susceptible de permettre directement ou indirectement d'identifier une personne. Les informations et données publiques comportant des données à caractère personnel doivent, par conséquent,

---

entre le public et l'administration entré en vigueur le 1er janvier 2016 675 CRPA, art. L. 311-4.

[658] CRPA, art. L. 311-5.

[659] CRPA, art. L. 311-6.

faire l'objet d'un traitement préalable dans le but de respecter les dispositions relatives à l'informatique aux fichiers et aux libertés en garantissant l'anonymat des personnes mentionnées, au sein de ces documents.

947. En ce qui concerne, plus spécifiquement, *« les données du système national des données de santé qui font l'objet d'une mise à disposition du public* ». Il convient de rappeler que le SNDS constitue la fusion de plusieurs bases de données. De ce fait, ce système est constitué du SNIIRAM contenant les données de l'assurance maladie, du PMSI contenant les données issues de l'activité des établissements de santé, du CepiDC, contenant les données sur les causes de décès, les données liées au handicap et qui sont issues des maisons départementales des personnes handicapées (MDPH), ainsi qu'un échantillon représentatif des données de remboursement par bénéficiaire issues des organismes d'assurance complémentaire.

948. Ainsi, les données de santé exploitées et conservées au sein de chacune de ces bases de données sont préalablement collectées par les acteurs du système de santé dans le respect des dispositions relatives à la loi Informatique et Libertés, puis, dans le cadre du SNDS, sont traitées et conservées, conformément aux dispositions de l'article 193 de la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé. Par conséquent, afin d'être rendues accessibles, elles font l'objet d'un procédé d'anonymisation préalable *« pour prendre la forme de statistiques agrégées ou de données individuelles constituées de telle sorte que l'identification, directe ou indirecte des personnes concernées y est impossible »*. Par ailleurs, *« la réutilisation de ces données ne peut avoir ni pour objet ni pour effet d'identifier les personnes concernées*[660] *»*. Par conséquent, le système national des données de santé ne contient, en théorie, aucune donnée présentant directement un caractère personnel tel que *« les noms, prénoms des personnes, ni leur numéro d'inscription au*

[660] C. santé publ, art. L. 1461-2.

répertoire national d'identification des personnes physiques, ni leur adresse »[661].

949. Par conséquent, l'article 193 précité qui pose le principe de l'utilisation exclusive de données médico-administratives anonymisées, écarte, de prime abord, toute atteinte aux droits et libertés des personnes concernées par le traitement de leurs données. Par ce biais, il évite également l'application de la réglementation relative à l'informatique, aux fichiers et aux libertés.

950. Il demeure toutefois, une exception en ce qui concerne la réutilisation des données d'activité des professionnels de santé. S'agissant de données liées à l'activité professionnelles, l'utilisation de ces données ne peut, en principe, pas être de nature à porter atteinte à la vie privée des professionnels. Celles-ci peuvent, par conséquent, être réutilisées dans les conditions de l'article 13 de la loi du 17 juillet 1978. Notons toutefois que cette entorse sérieuse aux dispositions de la loi du 6 janvier 1978 ainsi qu'aux principes de la mise à disposition de données publique, ne peut toutefois pas aboutir à « la constitution et l'utilisation à des fins de prospection ou de promotion commerciales de fichiers composés à partir de données issues directement ou indirectement des prescriptions médicales ou des informations médicales mentionnées à l'article L. 161-29 du code de la sécurité sociale, dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel prescripteur »[662].

951. Exception faite de l'exception susmentionnée, si le SNDS ne contient aucune donnée directement identifiantes, il est désormais impossible, compte tenu des progrès technologiques, de certifier qu'il ne comporte pas de données permettant indirectement d'identifier une ou plusieurs personnes. En effet, en raison des différentes travaux d'analyse

[661] C. santé publ, art. L. 1461-4.-I.

[662] C. santé publ, art. L. 4113-7.

menés ces dernières années par des juristes, des ingénieurs, mais aussi par la CNIL et les institutions des progrès ont été réalisés dans la définition des notions mais aussi des critères permettant d'apprécier le caractère indirectement identifiant d'une ou plusieurs données. Les différentes recommandations, articles et rapports précités ont démontré que les critères d'appréciation permettant de distinguer une données identifiante d'une donnée non identifiante, ne concédaient pas de pouvoir affirmer avec certitude qu'aucune ré-identification ultérieure demeure possible.

952. En effet, le caractère indirectement identifiant des données est par nature difficile à appréhender et la qualification n'est raisonnablement possible qu'*a posteriori*, c'est-à-dire, après qu'une donnée individuelle ou qu'un échantillon ou jeu de données *a priori* anonymes est pu être rattaché à une personne identifiée. La récente reconnaissance de la notion de donnée pseudonyme par le RGPD et sa différenciation avec la notion de donnée non identifiante est révélateur de cette difficulté.

953. **De la donnée anonyme et de la donnée pseudonyme.** Pour qu'une donnée soit considérée comme anonyme et non comme une donnée pseudonyme, le G29 se fonde sur la définition de la donnée à caractère personnel telle qu'elle est énoncée au sein de la Directive de 1995. Ainsi, l'anonymat se veut être absolu et strict. Ce faisant, le G29 prône le risque zéro et considère que le procédé d'anonymisation utilisé ne doit plus permettre l'individualisation des données relatives à une personne. Pour ce faire, il énonce que le procédé d'anonymisation utilisé doit garantir, de façon certaine, qu'aucune corrélation entre différents ensembles de données anonymisées se rapportant à un même personne ou à un même groupe de personnes ne demeure possible. Enfin, pour le G29, toute inférence doit être exclue, c'est-à-dire qu'il doit être impossible, à partir des données anonymisées, de rechercher et de déduire avec une forte probabilité un type de données[663] à partir des valeurs d'un ensemble

[663] Dans le domaine de l'informatique, un type de donnée peut être défini comme la nature des valeurs que peut prendre une donnée.

d'autres types[664]. Autrement dit, il doit être impossible « de déduire, avec un degré de probabilité élevé, la valeur d'un attribut à partir des valeurs d'un ensemble d'autres attributs »[665].

954. Le G29 se livre par conséquent à une interprétation stricte de la notion d'anonymisation des données. Il adopte une approche fondée à la fois sur des critères technique objectifs *« mais également des considérations subjectives telles que le facteur relatif à l'utilité de la tâche ou la motivation d'éventuels attaquants »*[666]. Il en résulte que si l'une de ces conditions fait défaut une même technique *« est susceptible d'être qualifiée d' "anonymisation" ou de "pseudonymisation" selon le contexte dans lequel elle est mise en œuvre »*[667]

955. Les procédés décris par le G29, lorsqu'ils permettent une anonymisation complète et irréversible rendent les données inexploitables, en ce qu'elle affecte leur utilité pratique. Ainsi, le plus difficile, du point de vue de la protection des données, est de réduire les risques de ré-identifications de manière à protéger la vie privée des personnes sans nuire à l'utilité des données rendues accessibles à des fins de recherche, d'analyse statistique ou d'évaluation[668].

956. L'objectif formellement assumé au sein de la loi de modernisation de notre système de santé étant la mise à disposition de données exploitables afin de contribuer à l'efficience du système de santé et de la qualité soins dispensés[669], les données conservées au sein du SNDS, continuent de bénéficier d'une richesse informationnelle substantielle. De

---

[664] E. DROUARDDrouard, C. MAROLLAMarolla, « Anonymisation et internet des objets : une « première » du Conseil d'État qui fera date », Lamy *D*roit du numérique, n° 135, 1er mars 2017.

[665] Groupe de travail de l'article 29 (G29) sur la protection des données, Avis nº 05/2014 sur les techniques d'anonymisation publié le 10 avril 2014, p. 13.

[666] E. DROUARDDrouard, C. MAROLLAMarolla, art. préc.

[667] *Ibid*.

[668] G29, Avis préc. p. 13.

[669] C. santé publ, art. L. 1461-1, III.

ce fait, bien qu'elles aient fait l'objet d'opérations d'anonymisations, leur traitement et notamment les opérations d'agrégation peuvent éventuellement conduire à la ré-identification des personnes[670][671].

957. Dominique Blum, praticien hospitalier, a ainsi exposé, en 2012, que « 89 % des personnes hospitalisées une fois en 2008 et 100 % de celles hospitalisées deux fois sont théoriquement identifiables grâce au fichier PMSI[672] (Programme de médicalisation des systèmes d'information), qui contient les données d'hospitalisation de plus de 23 millions de séjours à l'hôpital (…) Il a démontré que le fichier des moyens séjours permet, lui aussi, de retrouver des informations cachées comme les dates de séjour, ouvrant la voie à des ré-identifications »[673].

958. Plus récemment, entre les mois de septembre 2016 et mars 2017, après avoir pris connaissance du projet de rapport de la Cour des comptes portant sur les données à caractère personnel, la CNIL a diligenté des contrôles sur place afin de vérifier la conformité du SNIIRAM à la loi du 6 janvier 1978 modifiée. Suite à ces opérations de contrôle le 8 février 2018 le bureau de la CNIL a ainsi estimé « que le risque pour la sécurité des données est particulièrement élevé compte tenu du volume de données enregistrées dans le SNIIRAM et du nombre important de destinataires des données »[674]. Elle a mis en demeure la CNAMTS de prendre *« toute mesure pour garantir la sécurité et la confidentialité des données à caractère personnel traitées et en particulier »* sous un délai de trois mois à compter

[670] Voir en ce sens, les travaux menés par Cynthia Dwork, chercheuse chez Microsoft. D. LAROUSSERIE,Larousserie « L'anonymat, un bien fragile »,» Le Monde science et techno, 7 avril

[671] . L'article est consultable à l'adresse suivante : www.lemonde.fr/sciences

[672] Les informations considérées correspondent au code FINESS de l'établissement, au code géographique du domicile, au mois et à l'année de naissance du patient, au sexe, ainsi qu'au mois de sortie et à la durée du séjour. Voir en ce sens, P.-L. BRAS, A. LOTH, Rapport sur la gouvernance et l'utilisation des données de santé, septembre 2013.

[673] D. LAROUSSERIE,Larousserie *art. préc.*www.lemonde.fr/sciences

[674] CNIL, déc., 8 févr. 2018, Décision n° MED-2018-006 mettant en demeure la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés.

de la notification de sa décision. *« En choisissant de préserver l'utilité des données, les risques sont plus forts »*[675], ils doivent donc être compensés par des mesures de nature juridique.

959. S'agissant de données de santé, dès lors qu'elles présentent un risque de ré-identification des assurés, leur accès doit, en principe, être restreint[676]. En effet, la capacité de rapprocher un fichier ou un ensemble de données qu'on cherche à protéger d'une ré-identification au moyen, par exemple d'un rapprochement voir d'une interconnexion opérée avec d'autres fichiers dépend du niveau de sécurité qui entoure l'accès au fichier ou à la base de données.

960. De ce fait, comme cela avait été préconisé par Messieurs les sénateurs G. Gorce et F. Pillet dans le cadre du rapport au Sénat n°649 sur *« l'open data et la protection de la vie privée »*[677], le législateur a recherché à créer un équilibre entre la protection de la vie privée et l'utilisation de la donnée, sans pour autant concéder à un compromis inutile au détriment des droits et libertés des personnes concernées par le traitement. L'article 193 se dissocie ainsi d'un raisonnement exclusivement binaire consistant en l'identification ou l'anonymat de la personne comme condition *ratione materiae* d'application de la loi informatique et liberté ou des dispositions relatives à l'accessibilité des données. Ce faisant, l'article 193 nuance une réponse qui pouvait initialement se résumer en la mise à disposition ou le rejet pur et simple de la mise à disposition d'une ou plusieurs données. Pour ce faire, le législateur a privilégié au sein de la loi de modernisation de notre système de santé une approche par les risques

---

[675] H. TANGHE, P. O. GIBERT, « Big data et protection sociale : L'enjeu de l'anonymisation à l'heure du big data », Revue française des affaires sociales 2017/4, p. 79.

[676] C. CASTETS-RENARD, *« Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data* »,». Revue Lamy Droit de l'immatériel, nº 108, 1er oct. 2004.

[677] G. GORCE, F. PILLET, Rapport d'information sur l'open data et la protection de la vie privée, n° 469, Sénat, Session ordinaire de 2013-2014, p. 61.

961. Ainsi, compte tenu du risque d'atteintes à la vie privée pouvant résulter d'une éventuelle réversibilité de l'anonymisation et des détournements consécutifs à une éventuelle exploitation commerciale des données ré-identifiée, il a privilégié, au sein de l'article 193 de la loi de 2016 un système d'accès aux données en fonction du risque.

962. De cette manière, la mise à disposition de données conservées au sein du SNDS se trouve organiser en deux grandes catégories. En conséquence, seules les bases de données composant le SNDS qui sont suffisamment agrégées pour ne contenir que des données statistiques ou des données individuelles appauvries ne présentant aucun risque de ré-identification directe ou indirecte des personnes ont vocation à être accessibles gratuitement par le public, sans formalité spécifique et sans qu'il soit nécessaire pour les accédant d'obtenir une autorisation préalable.

963. Le législateur a toutefois trouvé nécessaire de rappeler que *« la réutilisation de ces données ne peut avoir ni pour objet ni pour effet d'identifier les personnes concernées »*[678]. On peut réellement s'interroger sur la nécessité d'une telle précision, sur la capacité des bénéficiaires d'un droit d'accès à procéder à la ré-identification de données agrégées ainsi que sur les pouvoirs et moyens de contrôle concernant tout traitement ayant pour objet ou pour effet d'identifier les personnes concernées par le traitement de leurs données.

964. *A contrario*, les données pseudonyme, par ce qu'elles sont susceptibles de représenter un risque d'atteinte pour la vie privée des personnes en raison du fait qu'elles peuvent éventuellement permettre indirectement l'identification des personnes par la combinaison d'une ou de plusieurs variables, font l'objet de restrictions d'accès et de conditions d'utilisation plus strictement réglementées.

[678] C. santé publ, art. L. 1461-2.

965. Cet accès conditionnel est dérogatoire du droit commun de l'*open data* fondé sur la libre mise à disposition des données. Ainsi, l'accès à ces données s'effectue « dans des conditions assurant la confidentialité et l'intégrité des données et la traçabilité des accès et des autres traitements »[679]. Un référentiel a été élaboré sur la base d'une analyse de risques rigoureuse de façon à mettre en place les mesures de sécurité adéquates. Il est défini par arrêté des ministres chargés de la santé, de la sécurité sociale et du numérique, pris après avis de la CNIL.

966. De la sorte, ces données ne peuvent faire l'objet d'un traitement qu'à des fins de recherche, d'étude, d'évaluation, d'information dans le domaine de la santé, de sécurité sanitaire et à condition que ces finalités répondent à un motif d'intérêt public. Le responsable du traitement doit obtenir, au préalable, l'autorisation de la CNIL et requiert la soumission d'informations détaillées à l'INDS avant et après que la recherche, l'étude ou l'évaluation ait été réalisée.

967. Il ne s'agit plus, à proprement parler, d'*open data* puisque plusieurs opérations de contrôle sont préalablement réalisées par différents organismes aussi bien en ce qui concerne le bénéficiaire de la mise à disposition de données mais aussi sur la finalité du traitement projeté et les modalités d'accès aux données sensibles.

968. Cependant, par ce moyen, des données qui étaient initialement écartées sont désormais accessibles et des utilisateurs qui se voyaient initialement refusé l'accès aux données peuvent désormais les exploiter dans l'intérêt public.

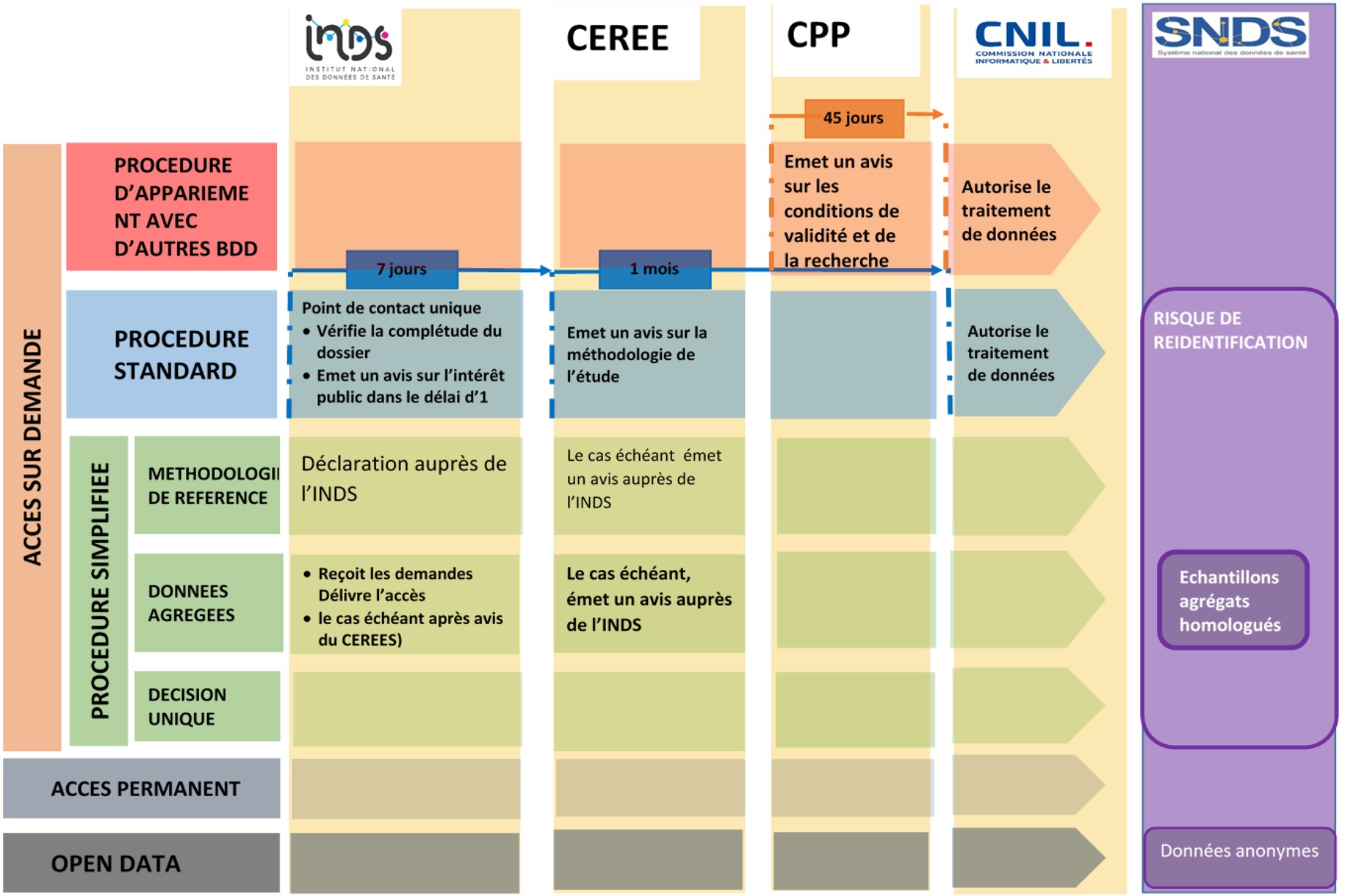
969. Notons qu'un décret en Conseil d'État autorise un accès permanent à ces données[680], aux établissements publics ou aux organismes

[679] C. santé publ, art. L. 1461-1, IV, III.

[680] Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».» 698 C. santé publ, art. L. 1461-3, 2°.

chargés d’une mission de service public ainsi qu’aux services de l’État, dès lors que la mise en œuvre de traitements sur ces données est nécessaire à l'accomplissement de leurs missions[698].

970. Leur mise à disposition ne sera gratuite que pour l’autorité publique ou les recherches réalisées exclusivement pour les besoins de services publics administratifs.


INDS
INSTITUT NATIONAL DES DONNÉES DE SANTÉ
CEREE
CPP
CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS
SNDS
Système national des données de santé
ACCES SUR DEMANDE
PROCEDURE D'APPARIEMENT AVEC D'AUTRES BDD
45 jours
Emet un avis sur les conditions de validité et de la recherche
Autorise le traitement de données
7 jours
1 mois
PROCEDURE STANDARD
Point de contact unique
• Vérifie la complétude du dossier
• Emet un avis sur l'intérêt public dans le délai d'1
Emet un avis sur la méthodologie de l'étude
Autorise le traitement de données
RISQUE DE REIDENTIFICATION
PROCEDURE SIMPLIFIEE
METHODOLOGIE DE REFERENCE
Déclaration auprès de l'INDS
Le cas échéant émet un avis auprès de l'INDS
DONNEES AGREGEES
• Reçoit les demandes Délivre l'accès
• le cas échéant après avis du CEREES)
Le cas échéant, émet un avis auprès de l'INDS
Echantillons agrégats homologués
DECISION UNIQUE
ACCES PERMANENT
OPEN DATA
Données anonymes

971. § 2. La nature des utilisateurs comme critère

972. **La nature des utilisateurs du SNDS un critère discriminant.** Antérieurement au 1er avril 2017, date d'entrée en vigueur du Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé *« système national des données de santé », le SNIIRAM, excluait les demandeurs privés à but lucratif. Ainsi, « aucun organisme de recherche, université, école ou autre structure d'enseignement lié à la recherche poursuivant un but lucratif ne [pouvait] accéder aux informations [du SNIIRAM] »*[681]. L'accès était toutefois autorisé aux Unions des organismes d'assurance maladie complémentaire (UNOCAM) et les laboratoires pharmaceutiques conservaient la possibilité de commanditer la réalisation d'études dont la réalisation et la demande était présentée par un laboratoire de recherche public.

973. La loi de modernisation de notre système de santé autorise désormais les organismes à but lucratif à accéder au SNDS. Cependant, contrairement aux personnes morales de droit public ces organismes ne bénéficient que d'un droit d'accès temporaire au système (A). Les personnes morales de droit public, conservent, pour leur part, un droit d'accès permanent aux données médico-administratives (B).

A. Un accès temporaire pour les organismes à but lucratif

974. Dans l'attente de l'entrée en vigueur du SNDS, le Conseil d'État, saisi sur une question de droit d'accès, a dans un arrêt « *Celtipharm* » en date du 20 mai 2016[682], remis en question ce principe d'interdiction d'accès imposée à l'encontre des organismes à but lucratif. Pour ce faire,

[681] Arrêté du 19 juillet 2013 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, art. 4.

[682] CE, 20 mai 2016, n° 385305.

les membres du Conseil ont prononcé l'annulation de la décision implicite du ministre des affaires sociales et de la santé consistant à refuser l'abrogation des dispositions du 3° du III de l'article 4 de l'arrêté du 19 juillet 2013 rendant accessibles les données du SNIIRAM aux organismes à but lucratif.

975. En l'espèce le Conseil d'État a considéré que la décision implicite ainsi que le 3° du III de l'article 4 de l'arrêté du 19 juillet 2013 étaient entachés d'illégalités. Le Conseil a considéré que les dispositions de l'article L. 161-28-1 du Code de la sécurité sociale ainsi que les articles 63 à 66 de loi du 6 janvier 1978, en vigueur à la date de la décision attaquée, ne prévoyait pas une telle exclusion.

976. Le Conseil d'État a également considéré que les dispositions des articles examinés garantissaient que les données issues du SNIIRAM ne pouvaient être communiquées que sous la forme de statistiques agrégées ou de données non identifiantes[683] et qu'il ne pouvait y être dérogé que sur autorisation préalable de la CNIL après qu'elle ait vérifié que le traitement envisagé ne comporte pas de données nominatives et de numéro d'inscription au Répertoire national d'identification des personnes physiques (NIRPP) et que le demandeur ait justifié d'éléments suffisants pour attester de la nécessité de disposer de certaines informations parmi l'ensemble des données à caractère personnel dont le traitement est envisagé. La CNIL peut ainsi interdire la communication de ces informations par l'organisme qui les détient et n'autoriser le traitement que des données ainsi réduites.

977. Compte-tenu de la décision du Conseil d'État du 20 mai 2016 et dans l'attente de l'application des dispositions de la loi de modernisation de notre système de santé, adoptée le 26 janvier 2016, un nouvel arrêté du 6 octobre 2016 est venu modifier l'arrêté du 19 juillet 2013. Il reprend les

[683] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 63.

termes de l'arrêt du 20 mai 2016 et substitue ainsi à l'ancien régime fondé sur une interdiction d'accès, de principe, pour les organismes de recherche poursuivant un but lucratif, un régime d'autorisation préalable. Il étend ainsi l'accès aux données de santé issues du SNIIRAM à ces organismes.

978. Depuis le 1er avril 2017, les dispositions de la loi de 2016 s'appliquent. Toute personne morale de droit public ou de droit privé, poursuivant ou non un but lucratif, peut accéder aux données du système national sur autorisation préalable de la CNIL à la double condition qu'elle est pour dessein de réaliser, à partir des données, une étude, une recherche ou une évaluation et que l'acte projeté représente un intérêt public[684].

979. La notion d'intérêt public est appréciée par la Commission, mais l'article L. 1462-1 3° du Code de la santé publique lui laisse la possibilité de saisir le comité d'expertise sur l'intérêt public placé auprès de la Présidence de l'INDS pour qu'il donne un avis sur cette exigence. L'Institut devrait ainsi être amené, par ce moyen, à définir sa propre doctrine concernant l'appréciation de ce caractère d'intérêt public.

980. Sur la notion d'intérêt public, notons que ni la loi de modernisation de notre système de santé, ni le décret de 2016 n'apporte quelques éléments permettant de définir cette notion. Cette notion est également employée à dix reprises au sein de la Directive de 1995 transposée dans notre droit national français par la loi du 6 août 2004 et à soixante-neuf reprises au sein du RGPD. Elle ne résulte pas de la Directive de 1995 puisqu'elle est employée, *ab initio,* dans le texte de 1978 au sein de l'article de la loi relative à l'informatique, aux fichiers et aux libertés.

[684] C. santé publ, art. L. 1461-3.

981. *« Il est interdit de mettre ou conserver en mémoire informatisée, sauf accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales des personnes.*

982. *(..) Pour des motifs d'intérêt public, il peut aussi être fait exception à l'interdiction ci-dessus sur proposition ou avis conforme de la commission [*nationale de l'informatique et des libertés*] par décret en Conseil d'État. »*

983. Il ressort du rapport intitulé « *Expertise juridique sur l'intérêt public dans le contexte des données de santé »*[685] par le cabinet Simmons & Simmons à la demande de l'INDS, que l'intérêt public serait, dans ce cadre, « essentiellement appréhendée par le prisme de l'intérêt général »[686]. En effet, l'article 54 du projet de loi portant modernisation de notre système de santé dans sa version initiale, *« faisait référence, en ce qui concerne la demande d'accès aux données de santé, aux traitements ayant "une finalité d'intérêt général". Ce n'est que guidé par « souci de cohérence du dispositif avec celui existant dans le cadre de la LIL [que] les parlementaires [ont substitué] la notion d'intérêt public à celle d'intérêt général postérieurement au passage du texte devant la Commission des affaires sociales ». La substitution de la notion « d'intérêt public » à la notion « d'intérêt général » a été un sujet de débat important en commission mais il a été choisi de privilégier la notion d'intérêt public « par cohérence avec les directives européennes et avec la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cela permet*

[685] INDS, Expertise juridique sur l'intérêt public dans le contexte des données de santé, 29 juin 2017.

[686] *Ibid*., p. 27 à 29.

d'être très précis quant au type d'organismes qui ont accès aux données de santé »[687].

984. En conclusion, il ressort du rapport susmentionné, que la notion d'intérêt public française est singulière et que des divergences entre les pays expliquent sans doute le fait que la Directive de 1995 ainsi que le RGPD n'aient pas pris position sur une définition commune de l'intérêt public, mais aient laissé aux États-membres le soin d'en déterminer eux-mêmes les contours. En ce qui concerne notre droit national, le rapport préconise au Comité d'expertise sur l'intérêt public (CEIP), place auprès de l'INDS de recourir à la méthode du faisceau d'indices en appréciant, au regard des éléments de la demande, trois critères principaux que sont, le critère organique, c'est-à-dire la nature juridique du demandeur ou du commanditaire, ainsi que son objet, la finalité du traitement et en fin le critère financier.

985. Ainsi, concernant l'appréciation de la notion d'intérêt public à partir du critère organique, si la demande de traitement de données est présentée exclusivement par une personne publique, « sans qu'aucune personne privée ne puisse être identifiée comme co-demandeur ou destinataire final de la recherche ou de l'étude, constitue un indice favorable à l'existence d'un intérêt public »[688]. *A contrario,* la demande de traitement de données présentée exclusivement par une personne privée entrainera une présomption d'intérêt privé justifiant un examen particulier du dossier pour apprécier, au regard des autres critères dégagés, si l'usage prétendu répond à un motif d'intérêt public. Il en est de même lorsque la demande déposée le sera dans le cadre d'un montage qualifié, par ce rapport, de mixte où le commanditaire et une personne privée et le dossier est déposé par une personne morale de droit public.

---

[687] Compte rendu intégral, Troisième séance du vendredi 10 avril 2015, Assemblée nationale, Session ordinaire de 2014-2015.

[688] INDS, Rapport préc. p. 45.

986. En synthèse, en ce qui concerne le critère de la finalité, les conclusions du rapport renvoient au concept de bénéfice collectif. Par conséquent, la finalité de l'étude, de la recherche ou de l'évaluation doit produire un bénéfice collectif. Au regard de l'absence de dispositions implicites ou explicites dans la loi de 2016, ce bénéfice collectif ne va pas jusqu'à exclure, en raison d'un principe d'exclusivité, les intérêts particuliers du commanditaire. *« À défaut, l'objectif d'innovation ou de développement des connaissances médicales, recherché aussi par l'ouverture de l'accès aux données de santé, risquerait d'être compromis ou limité »*[689]. Autrement dit, le demandeur ou le destinataire de l'étude peut poursuivre, à condition de ne pas entrer dans le champ des interdictions figurant au V de l'article L. 1461-1 du Code de la santé publique des sous finalités de nature commerciale dès lors que dans un rapport de proportionnalité, l'intérêt public se trouve prépondérant.

987. Enfin, au sujet du critère financier, la nature du financement, c'est-à-dire l'origine des fonds servant au financement de la recherche, de l'étude ou de l'évaluation envisagée est un indice susceptible de permettre au CEIP de caractériser l'intérêt public.

988. *« Ainsi, un financement public (total ou majoritaire) sera considéré comme un indice en faveur de l'intérêt public, tandis qu'un financement essentiellement sur fonds privés pourra, selon les cas, induire un doute sur l'existence réelle d'un intérêt public, mais sans nécessairement l'exclure si les autres critères du faisceau d'indices sont favorables. »*[690]

[689] *Ibid.*

[690] *Ibid.*, p. 47.

989. En ce qui concerne les entreprises, établissements ou organismes qui sont placés sous le contrôle de l'Agence national de sécurité du médicament (ANSM) ainsi que des institutions de prévoyance, des mutuelles, des sociétés d'assurance et des intermédiaires d'assurance, ceux-ci peuvent désormais déposer une demande d'accès afin de réaliser des traitements à des fins de recherche, d'étude ou d'évaluation à partir des bases de données du SNDS[691].

990. Toutefois, compte tenu de leur nature juridique et des risques susceptibles de découler pour les droits et libertés des personnes dont les données font l'objet d'un traitement, les dispositions du II de l'article L. 1461-3 du Code de la santé publique interdit expressément le traitement de ces données à des fins d'exclusion de garanties ou de modulation des cotisations et des primes des polices d'assurance d'un individu ou d'un groupe d'individus. Il subordonne également, l'accès aux données du SNDS à la démonstration préalable que les modalités de mise en œuvre du traitement rendent impossible une telle utilisation ainsi que toute utilisation des données à des fins de promotion des produits mentionnés mais exclusivement en direction des professionnels de santé ou d'établissements de santé. Au regard de ce qui précède, les traitements concernant des données du système national des données de santé, dont la finalité présenterait un intérêt public et qui serait destiné à des actions de promotion à destination du grand public seraient autorisés. Les dispositions précédemment citées semblent le confirmer. Ainsi, si les conditions d'intérêt public sont satisfaites, un tel traitement serait en principe licite. Compte tenu de l'obligation faite à ces établissements, organismes et entreprises, de déposer une demande d'autorisation préalable, il est raisonnable de s'interroger sur le caractère contestable d'un rejet d'autorisation qui serait fondée sur ce motif. Eu égard à la mise en œuvre récente du SNDS, nous ne disposons pas de suffisamment

[691] C. santé publ, art. L. 1461-3.

d'éléments pour apprécier les risques de cette limitation de l'interdiction et les suites qui seraient réservées à de telles requêtes.

991. Les dispositions du II de l'article L. 1461-3 du Code de la santé publique semblent rédigées comme des conditions alternatives. Ainsi, pour les industriels de produits de santé et les organismes de complémentaires santé, les données du SNDS leur serait directement accessible à la condition qu'ils soient en capacité de démontrer que les modalités de mise en œuvre du traitement rendent impossible toute utilisation des données pour l'une des finalités interdites. *A contrario,* lorsque ils seraient dans l'incapacité de le prouver, ils devraient recourir à un laboratoire de recherche ou à un bureau d'études, publics ou privés afin qu'il procède à la réalisation de ce traitement.

992. On s'interroge sur la portée d'une telle mesure puisqu'elle permet la réalisation de recherches, d'études ou d'évaluations malgré la persistance de suspicions concernant l'utilisation des données du SNDS à des fins contraires aux droits et libertés des personnes. Compte tenu des risques, le doute subsistant devrait nécessiter, une réponse juridique plus appropriée. Il aurait été préférable en l'absence de garantie quant à l'utilisation des résultats du traitement ou que toute suspicion d'une mauvaise utilisation des données entraine une interdiction de principe de procéder au traitement escompté. Ainsi, la possibilité de recourir aux services d'un laboratoire de recherche ou d'un bureau d'études, publics ou privés, pour réaliser le traitement ne laisse recours qu'à une réponse juridique non plus *a priori* mais *a posteriori* en cas de mésusage des données du SNDS.

993. La loi de 2016 ainsi que l'arrêté du 17 juillet 2017 exigent cependant du responsable de traitement mais aussi, des bureaux d'études et des laboratoires de recherches des garanties supplémentaires. Ainsi, l'article 5 alinéa 1 précise, à toute fin utile, que « *le protocole d'analyse de la recherche, de l'étude ou de l'évaluation ne doit pas avoir pour but de produire un résultat spécifié à l'avance* ». Par ailleurs, *« les responsables*

de ces laboratoires de recherche et des bureaux d'études doivent présenter à la Commission nationale de l'informatique et des libertés un engagement de conformité à un référentiel [pris par arrêté après avis de la Commission] incluant les critères de confidentialité, d'expertise et d'indépendance »[692].

994. La ministre des Solidarités et de la Santé a ainsi arrêté le 17 juillet 2017 le référentiel déterminant les critères de confidentialité, d'expertise et d'indépendance pour les laboratoires de recherche et bureaux d'études. Celui-ci a été publié au Journal officiel (JO) du 25 juillet 2017. Afin d'apporter des garanties supplémentaires concernant l'indépendance de ces sous-traitants, le référentiel prévoit notamment que ceux-ci doivent être en mesure d'établir qu'ils ne sont pas en situation de dépendance économique à l'égard du responsable de traitement. Pour ce faire, l'arrêté introduit l'obligation pour ces tiers de confiance, de remettre, à l'INDS une déclaration d'intérêts et d'indépendance économique[693], en rapport avec l'objet du traitement, conforme à un modèle-type fixé en annexe de l'arrêté. Cette déclaration doit être complétée par *« le responsable du laboratoire de recherche ou du bureau d'études et par chacune des personnes impliquées dans la recherche, étude ou évaluation. »*[694].

995. L'arrêté reprend en ce sens, les dispositions de l'ordonnance n° 201749 du 19 janvier 2017 relative aux avantages offerts par les personnes fabriquant ou commercialisant des produits ou des prestations de santé

---

[692] C. santé publ, art. L. 1461-3.

[693] Pour apprécier la notion de conflit d'intérêt, il convient également de se référer à la définition donnée par l'OCDE à l'occasion de la 29ème session du Comité de la gouvernance publique ayant eu lieu à Paris en avril 2004. Ainsi, l'OCDE définit la notion comme *« un conflit entre la mission publique et les intérêts privés d'un agent public, dans lequel l'agent public possède à titre privé des intérêts qui pourraient influencer indûment la façon dont il s'acquitte de ses obligations et de ses responsabilités ».*

[694] Arrêté du 17 juillet 2017 relatif au référentiel déterminant les critères de confidentialité, d'expertise et d'indépendance pour les laboratoires de recherche et bureaux d'études. Annexe : Formulaire de déclaration des intérêts du laboratoire de recherche ou du bureau d'études. 713 Arrêté du 17 juillet 2017 préc. art.) 5 al. 5.

intègre au sein du Code de la santé publique un article L. 1453-3 interdisant *« pour les personnes mentionnées à l'article L. 1453-4, de recevoir des avantages en espèces ou en nature, sous quelque forme que ce soit, d'une façon directe ou indirecte, proposés ou procurés par les personnes produisant ou commercialisant des produits mentionnés au II de l'article L. 5311-1, à l'exception de ceux mentionnés aux 14°, 15° et 17°, ou qui assure des prestations de santé ».*

996. Cette déclaration a pour objet de confirmer que le responsable du laboratoire de recherche ou du bureau d'études ainsi que ses salariés ou les prestataires auxquels il a recours et qui sont impliqués dans la mise en œuvre de la recherche l'étude ou l'évaluation envisagée ne disposent d'aucun liens d'intérêts de toute nature, directs ou par personne interposée que *« la personne impliquée dans le traitement a, ou qu'elle a eus, pendant les trois années précédant la date de soumission de la demande d'autorisation à la Commission nationale de l'informatique et des libertés, avec des entreprises, des établissements ou des organismes dont les activités, les techniques et les produits entrent dans le champ de l'objet du traitement dans lequel la personne est impliquée »*[713].

997. Afin de préserver l'indépendance des bureaux d'études et laboratoires de recherches concernés, ces mesures sont accompagnées d'exigences complémentaires concernant notamment la rémunération de la prestation, celle-ci doit *« dépendre uniquement de la nature et du volume des prestations définies au sein du contrat et ne pas être conditionnée par les résultats de la recherche ».* Enfin, l'accès au SNDS est subordonné, avant le début de la recherche, à la communication, par le responsable de traitement, à l'INDS, en sus des informations susmentionnées comprenant l'autorisation de la CNIL, la déclaration des intérêts du demandeur en rapport avec l'objet du traitement, le protocole d'analyse, précisant notamment les moyens d'en évaluer la validité et les résultats ainsi que son engagement de communiquer dans un délai raisonnable, après la fin de la recherche, de l'étude ou de l'évaluation, la

méthode ainsi que les résultats de l'analyse et les moyens d'en évaluer la validité.

998. Suite à la communication des résultats de la recherche, de l'étude, de l'évaluation par le commanditaire, l'INDS publie, à des fins d'intérêt public, sans délai l'autorisation de la CNIL, la déclaration des intérêts, puis les résultats et la méthode.

999. Notons par ailleurs que les responsables du laboratoire de recherche ou du bureau d'études, de même que leurs salariés et prestataires, mettant en œuvre le traitement ou autorisés à accéder aux données, sont également soumis au secret professionnel ainsi qu'à une obligation de confidentialité. Cette obligation se matérialise par la signature d'un engagement de confidentialité conforme au référentiel de sécurité applicable au SNDS portant notamment sur la non-diffusion des données indirectement identifiantes[695]. L'utilisation de la notion de secret professionnel et le renvoi à la signature d'un engagement de confidentialité témoigne que la confusion entre les deux notions perdure[696].

1000. En conclusion, ce dispositif semble de nature à garantir l'« intégrité et l'objectivité » des recherches, études et évaluations menées. Elle institue un équilibre entre l'accès aux industriels de la santé et aux organismes complémentaires pour lesquels il subsisterait un intérêt à mener des recherches, des études ou des évaluations à partir des données du SNIIRAM et d'autre part, la protection des personnes concernées d'une mauvaise utilisation des données susceptible d'engendrer un risque élevé pour leurs droits et libertés, en particulier lorsque les résultats de l'étude,

[695] Arrêté du 17 juillet 2017 préc. art. 3 et C. santé publ, art. L. 1461-1, IV, 2°.

[696] Sur *« la confusion entre secret professionnel et confidentialité »* se référer à C. ZORN, *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé*, avant-propos B. Py, préf. I. de Lamberterie, PUN, 2010, p. 64, n° 32..

l'évaluation ou la recherche empêcheraient ces personnes d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

1001. B. Un accès permanent réservé aux personnes publiques

1002. **Un accès antérieur trop restreint.** Nous l'avons évoqué lors de nos précédents développements, un accès permanent existait antérieurement à l'adoption de la loi de modernisation de notre système de santé. Toutefois, celui-ci était limité à un double titre. D'une part, son périmètre était restreint puisqu'il concernait uniquement les données conservées au sein du SNIIRAM. Ainsi, ce système complexe était initialement conçu simplement dans le but de procéder au versement des prestations aux assurés sociaux et non dans l'objectif de pouvoir réaliser des études, évaluations et recherches. C'est pourquoi, il ne permettait pas que des requêtes puissent directement y être effectuées. D'autre part, cet accès permanent ne concernait que deux catégories de données, les données individualisées mais demeurant anonymes complètes ou échantillonnées et constituant l'EGB et les données non individualisées constituant quinze bases de données thématiques appelées *« datamarts »* organisées autour de trois grands thèmes, l'offre de soins composé des professionnels et établissements de santé, des dépenses (DAMIR), des bénéficiaires et de leur parcours déduit à partir des données des professionnels de santé et des actes réalisés.

1003. Cet accès permanent à la totalité de la base était réservé aux organismes gestionnaires de l'assurance maladie et aux agences publiques exerçant une mission de veille dans le domaine de la santé. Ainsi était surtout bénéficiaires de cet accès, l'Agence de biomédecine, Agence technique de l'information sur l'hospitalisation, l'Institut des données de santé etc.

1004. Les organismes et administrations bénéficiaires d'un droit d'accès permanent étaient désignés par un arrêté du ministre chargé de santé après avis motivé de la CNIL. Nous l'avons précédemment exposé, depuis 2002 la liste des organismes habilités a été régulièrement révisée. Elle a fait ainsi l'objet de sept arrêtés successifs[697]. Afin de limiter le risque d'atteinte à la vie privée pouvant résulter d'une ré-identification à partir des données pseudonymisées, seuls les Caisses des régimes de base d'assurance maladie, le CNSA, l'institut de veille sanitaire (InVS) ainsi que l'ANSM et la HAS bénéficiaient d'un droit d'accès à l'ensemble des données de la base. Cet accès comprenait, le suivi des dépenses, le suivi d'activité par offreur de soins, l'EGB et les données individuelles exhaustives. Cette limitation des personnes autorisées était accompagnée de mesures de nature technique consistant en l'identification et l'authentification des utilisateurs, la sécurisation de l'accès au moyen d'un mot de passe ainsi que la traçabilité des actions réalisées dans le système.

1005. Le croisement de données sensibles était interdit par le système de gestion des profils à moins que l'utilisateur ne bénéficie d'une habilitation spécifique. Enfin les traitements portant sur moins de dix individus étaient simplement interdits.

1006. Un nouvel accès permanent La loi de modernisation de notre système de santé reprend ce régime particulier d'accès aux données médico-administratives au profit des membres de l'ancien IDS. Il bénéficie dorénavant à certains services de l'État, ainsi qu'aux établissements publics ou organismes chargés d'une mission de service public. Ceux-ci doivent être désignés au sein du décret n°2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé - *système national des données de santé*- pris en Conseil d'État après avis de la CNIL. Ce décret se substitue à l'ancien arrêté SNIIRAM.

---

[697] Se référer au tableau : « *Liste des organismes ayant accès aux bases de données du SNIIRAM (arrêté du 19 juillet 2013)* » figurant au chapitre 2 relatif à la systémisation de l'accessibilité.

1007. **Un accès de droit commun intégral soumis à l'autorisation préalable de la CNIL**. L'accès à l'ensemble des données du système national doit toutefois être proportionné à la mission de service public de ces services, établissements ou organismes. S'agissant des données indirectement nominatives, le régime commun demeure l'accès subordonné à l'autorisation préalable de la CNIL réservé à la recherche, aux études et évaluations d'intérêt public.

1008. Un accès à l'intégralité du système restreint à l'Etat et aux établissements et organise chargés d'une mission de service public. Ce droit d'accès à l'intégralité du système se trouve toutefois circonscrit à certains services de l'État et établissements publics ou organismes chargés d'une mission de service public. Ceux-ci doivent également être désignés, non plus par un simple arrêté mais par décret en Conseil d'État pris après avis de la CNIL[698]. Bien que l'avis de la Commission et du Conseil d'État ne soit pas contraignant, notons que leur consultation préalable constitue une garantie supplémentaire en comparaison à un arrêté simple. En effet, le Conseil d'État peut par ce moyen, émettre un avis sur la régularité juridique du projet de décret et son opportunité et, bénéficier pour cela de l'expertise préalable de la Commission sur les nouvelles autorisations d'accès permanent envisagées. Il peut, par ailleurs, soutenir les observations et recommandations de la CNIL relatives aux conditions d'accès est aux mesures de réduction des risques de ré-identification et de préservation de la sécurité et de la confidentialité des données.

1009. Les services de l'État, établissements publics et organismes chargés d'une mission de service public bénéficient d'un droit d'accès permanent au visa du paragraphe III de l'article L. 1461-3 du Code de la santé publique. Ils sont autorisés à accéder à certaines données à caractère personnel indirectement nominatives dans les limites définies aux articles R. 1461-13 et R. 1461-14 du Code de la santé publique et, en

[698] C. santé publ, art. L. 1461-7.

fonction des exigences des missions de service public qu'ils accomplissent. Sont notamment concernées l'ANSM, la HAS, les ARS[699]. Notons toutefois, que les fédérations hospitalières qu'il s'agisse de la FHF, de la FHP, de la Fehap ou encore d'Unicancer, ne figurent pas parmi la liste des établissements publics et organismes chargés d'une mission de service public bénéficiant d'un droit d'accès permanent. Les fédérations disposaient auparavant, dans le cadre de l'IDS, d'un accès permanent au SNIIRAM et les établissements représentés par ces fédérations alimentent le PMSI. Cependant, elles se trouvent désormais soumis au régime d'autorisation temporaire et à l'obligation de prouver l'intérêt public de leurs études, recherches et évaluations et d'obtenir une autorisation préalable de la CNIL en déposant une demande auprès de l'INDS. Ainsi, leur accès s'en trouve désormais restreint et conditionné.

1010. Pour les autres organismes et services, qui bénéficient d'un accès permanent, l'étendue de cette autorisation est les modalités du traitement sont définies de manière à éviter un accès non raisonné qui représenterait un risque pour les personnes dont les données sont traitées. À cette fin, deux variables sont utilisées afin de moduler l'étendue de leur autorisation d'accès, la profondeur historique des données, ainsi que la sensibilité des données, entendue comme l'occurrence d'aboutir à l'identification indirecte des personnes. En fonction des finalités sanitaires ou sociales du traitement, les organismes et services ne vont pas se voir autoriser à accéder à la même profondeur historique des données utilisées, à la même aire géographique ou aux mêmes caractéristiques d'une population déterminée. De la même manière, ces organismes et services, pourront se voir autoriser « d'utiliser de manière simultanée dans un même traitement, plusieurs variables » constituant des identifiants potentiels, dont la combinaison accroît le risque de ré-identification alors que d'autres se verront refuser cette faculté.

[699] Voir également en ce sens les dispositions de l'art. L. 1435-6 du Code de la santé publique.

1011. Compte tenu du fait que les services et organismes bénéficiant d'un droit d'accès ne seront pas soumis à l'obligation de solliciter une autorisation préalable, le décret souligne finement l'étendue de leur autorisation, leurs conditions d'accès aux données et la gestion de ces accès, afin que l'ouverture des données de santé s'accomplisse dans le respect de la vie privée. Ainsi, si, nous nous livrons à une analyse combinée des articles R. 1461-13 et R. 1461-14 du Code de la santé publique, l'étendue des autorisations d'accès permanent aux données du SNDS est composée de cinq échelons. Le premier est constitué par un accès restreint aux données agrégées et semi-agrégées reconnu aux Unions régionales de professionnels de santé (URPS), l'Agence nationale d'appui à la performance (ANAP), l'Autorité de sûreté nucléaire (ASN), le Fonds de financement de la couverture maladie universelle (fonds CMU), la Direction des soins (DS), le Haut Conseil pour l'avenir de l'assurance maladie (HCAAM), l'Institut national du cancer (INCa), l'Institut de radioprotection et de sûreté nucléaire (IRSN), l'Observatoire français des drogues et toxicomanies (OFDT), bénéficiant également d'un accès restreins aux échantillons avec croisement de deux identifiants.

1012. Un accès restreint aux échantillons avec croisement des identifiants potentiels ainsi qu'aux données semi-agrégées et agrégées est octroyé à l'INSERM ainsi qu'aux CHU.

1013. En ce qui concerne l'accès standard, la profondeur maximale historique des données du système national des données de santé sur lesquelles peuvent porter les traitements sont limités à cinq ans, en plus de l'année en cours. Cet accès est réservé à la Direction générale de la santé (DGS), la Direction générale de l'offre de soins (DGOS), la Caisse centrale de la mutualité agricole (CCMSA), la Caisse nationale du régime social des indépendants (CNRSI), l'INDS, l'Institut national d'études démographiques (INED), la Fédération nationale des observatoires de santé (FNORS) et les Observatoires régionales de santé (ORS) sur leur périmètre régional, les ARS, les organismes locaux et régionaux de l'assurance maladie obligatoire sur leur périmètre d'intervention et le

service de santé des armées sur le champ couvert par la caisse nationale des militaires.

1014. Cette profondeur historique est portée à 19 ans plus l'année en cours, lorsque le traitement porte sur l'EGB. Les ARS, l'ATIH, la Caisse nationale de l'assurance maladie des travailleurs salariés (Cnamts), la Caisse nationale de solidarité pour l'autonomie (CNSA), la direction de la recherche, des études, de l'évaluation et des statistiques du ministère chargé de la santé et des affaires sociales (DREES), l'Institut de recherche et de documentation en économie de la santé (IRDES), peuvent accéder à une profondeur historique de 9 années, en plus de l'année en cours. S'agissant de l'Agence nationale de santé publique (ANSP), l'ANSM, l'Agence de la biomédecine, l'INCa, l'Établissement français du sang (EFS) et la HAS, celle-ci est limité à 19 ans, en plus de l'année en cours. Compte tenu de ces éléments, ce n'est donc pas moins d'une trentaine d'organismes qui peuvent dorénavant accéder, de manière permanente, au SNDS.

1015. Cette situation démontre que la réforme s'inscrit bien dans une logique d'ouverture des bases de données nationales. Concernant les organismes demandeurs, la CNIL, saisie par la ministre des Affaires sociales et de la Santé d'une demande d'avis concernant le projet de décret relatif au Système national des données de santé, a observé, dans une délibération en date du 13 octobre 2016[700], que ce sont plus de deux mille utilisateurs potentiels qui auront, à terme, accès au SNDS.

1016. Avec l'intégration des URPS[701], ce nombre pourrait être porté à trois mille utilisateurs.

1017. Elle note qu'à terme, sur l'ensemble des utilisateurs, cinq cents seront issues d'organismes que ne possédaient pas, sous l'égide de

[700] CNIL, délib., 13 oct. 2016, n° 2016-316 portant avis sur un projet de décret en Conseil d'Etat relatif au Système national des données de santé.

[701] C. santé publ, art. R. 1461-12, 22°.

la réglementation antérieure, d'accès direct aux données du SNIIRAM ou du PMSI.

CONCLUSION DU CHAPITRE 2

1019. L'article 193 de la loi de modernisation de notre système de santé facilite l'accès au Système national des données de santé en organisant la gestion des demandes d'accès autours interlocuteur unique l'INDS. Il a pour triple objectif d'améliorer les politiques publiques en santé, l'information des patients et de faire progresser la recherche médicale.

1020. Afin de garantir la sécurité des données personnes qu'il contient aucune donnée contenue par le SNDS ne permet d'identifier directement la personne. Ce caractère indirectement identifiant des données permet de soumettre les traitements ayant recours aux données du SNDS aux dispositions de la loi relative à l'informatique aux fichiers informatique et liberté ainsi qu'au RGPD et d'agissant de données produites par le système de soins au code de la santé publique.

1021. L'accès aux données et organisé autour du risque de ré-identification. Ainsi, les services de l'État, établissements publics, et organismes chargés d'une mission de service public bénéficient d'un droit d'accès permanent au système alors que les autres demandeurs, publics ou privés, à but lucratif ou non lucratif, ils ne peuvent accéder que ponctuellement et sur projets accordé par l'INDS après autorisation de la CNIL

1022. L'accès au SNDS semble respecter l'équilibre entre la disponibilité de l'information et protection des droits des personnes car il nécessite le respect des obligations de sécurité que nous avions présenté en amont de notre étude et notamment l'authentification forte des personnes qui accèdent aux données afin de pouvoir contrôler les actions réalisées sur les données disponibles en accès. Il semble mettre en œuvre

des mesures de nature technique et juridique permettant de limiter le risque d'atteinte à la vie privée grâce au référentiel de sécurité qui encadre son utilisation [702] . Si l'accès semble facilité dans sa dimension organisationnelle, la multiplication des procédures simplificatrices et dérogatoires représente un risque de voir la situation antérieure

[702] Arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé

CONCLUSION DU TITRE I

1024. **Une circulation indispensable pour le patient et la pérennité du système de santé**. Une étude de l'OCDE de 2017 révéle que près de 30 % des dépenses de santé relèveraient du gaspillage. Ces dernières sont la conséquence d'actes inutiles, d'errances thérapeutiques, de mauvaise coordination des soins[703]. Cette étude démontre que partage et l'accès à la donnée de santé constitue une source d'efficacité et facilite la gestion du patient. La refonte de l'article L. 1110-4 du Code de la santé publique répond à la fois dans l'intérêt de la personne et du système de santé une à cette problématique.

1025. **Une circulation favorable à l'amélioration de la santé de la population.** Les dispositions de l'article 193 de la loi de modernisation de notre système de santé qui créent le SNDS et organisent l'accès à des fins d'étude et de recherche à partir des données recueillies ou produites par le système de santé offrent la possibilité de comprendre les maladies et de développer des réponses adaptées et innovantes. S'agissant de données de vie réelles, l'accès et l'étude de ces données est également indispensable à la sécurité sanitaire.

[703] Wasteful spending on health in numbers. OCDE. 2017

TITRE II. Le fondement d'une sante personnalisée

« Depuis une quinzaine d'années, la médecine personnalisée est le nouvel horizon des politiques de santé à l'échelle internationale. Sa définition ne fait toutefois l'objet d'aucun consensus. »[704]

1027. **La médecine personnalisée une médecine protéiforme.** La médecine personnalisée est une médecine protéiforme pouvant consister en la consolidation du dialogue médecin- patient par la réalisation de consultations préalables plus longue et personnalisée, afin de définir un parcours individualisé ainsi qu'un traitement plus adapté au patient[705]. Il peut également s'agir d'une médecine plus prédictive construite sur une caractérisation fine du patient, c'est-à-dire de profilage du risque, nécessitant à titre d'exemple une analyse génétique[706]. Cette médecine peut également consister en l'utilisation de moyens de prévention individuelle. L'ensemble de ses déclinaisons ont pour point commun de requérir une analyse fine du patient.

1028. **Une médecine métamorphosant son rapport à la technologie.** « *Même si l'adoption par les patients et les professionnels de*

[704] X. GUCHET. La médecine personnalisée : Un essai philosophique. Les belles lettres, 13 mai 2016

[705] D. Bourcier, P. de Filippi. « Vers un droit collectif sur les données de santé ». RDSS 2018. p.

444. Voir également. Source : pwc France. Médecine personnalisée : vers une santé à la carte ?

(https://www.pwc.fr/fr/decryptages/humain/medecine-personnalisee-vers-sante-a-la-carte.html).

Source : Paris innovation review. Médecine personnalisée: la révolution est en marche (http://parisinnovationreview.com/article/medecine-personnalisee-la-revolution-est-en-marche).

[706] Source : Encyclopedia Universalis (https://www.universalis.fr/encyclopedie/medecine-medecinepredictive/)

santé est variable et des barrières ou des facteurs favorisants ont été identifiés, la notion de médecine personnalisée et de mesure de soi (quantified-self) est en train de se développer »[707] Son développement résulte du fait que cette pratique médicale bénéficie d'un environnement technique et juridique propice. En ce qui concerne la technique, *« en octobre 2013, l'autorité de régulation américaine des médicaments et des dispositifs médicaux […] a précisé ce que recouvrait la médecine personnalisée et sur quelles données elle se fondait.»* Les principales causes de son succès, repose sur les dernières avancées technologiques réalisée en matière de miniaturisation des capteurs et sur la diminution de leur coût de production.

1029. Avec le développement de l'utilisation du *smartphone,* la captation et l'analyse des données physiologiques et de bien-être sont devenues une chose commune. Il en est de même du recours aux « *plateformes en ligne, qui recueille et partage des informations de santé, […], et développent des pratiques de self-monitoring »*[708] En ce qui concerne l'environnement juridique, la réglementation nationale et communautaire est favorable à l'acceptation de la circulation des données à caractère personnel, à partir du moment où celle-ci est sécurisée. La médecine personnalisée bouleverse donc le cadre traditionnel du soin en s'inscrivant dans la m-santé[709]. Au moyen de dispositifs connectés, l'individu enregistre lui-même, en continu, ses paramètres et peut suivre ses constantes ainsi que son état de santé. Au regard de l'analyse et des référentiels réalisés par la HAS et la CNIL avec le concours de l'ANSSI, Il semble que la médecine personnalisée considère de manière

[707] Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou mHealth). HAS, octobre 2016. p. 7.

[708] *Ibid.*

[709] L'Organisation mondiale de la santé définie, la m-santé par « des pratiques médicales et de santé publique supportées par des appareils mobiles, tels que les téléphones mobiles, les dispositifs de surveillance des patients, les PDA et autres appareils sans fil. » 8. World Health Organization. mHealth. New horizons for health through mobile technologies : second global survey on eHealth.

Geneva: WHO; 2011. www.who.int/goe/publications/goe_mhealth_web.pdf

indifférenciée les objets connectés utilisés à des fins de bien-être ainsi que les dispositifs médicaux en n'opérant aucune distinction entre les données produites par ces outils[710].

1030. **Une évolution du rapport au soin.** Cette médecine 2.0 appartient à la santé personnalisée à laquelle elle emprunte l'autonomisation de la personne, l'individualisation de l'approche et son caractère préventif. Elle s'inscrit dans l'évolution horizontale de la relation médecin-patient initiée par la loi du 4 mars 2002. Dans le cadre de cette activité médicale, le médecin va utiliser les objets connectés à des fins de diagnostic ou de traitement. Il va également voir son rôle évoluer pour, dans le cadre d'une démarche de prévention, tendre vers celui de *coach* de santé.

1031. **Un besoin de cohérence.** A la croisée des chemins entre la prise en charge formalisée réalisée par le système de santé et le bien-être qui repose exclusivement sur l'autodétermination de la personne et sur son hygiène de vie, la santé personnalisée questionne le droit sur la place de la personne dans le soin (Chapitre 1), sur les limites de son autonomisation et les frontières entre le bien-être et la santé. Elle invite également à l'analyse du régime de protection de la personne applicable à cette nouvelle conception du soin (Chapitre 2).

[710] Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou mHealth). HAS, octobre 2016.

CHAPITRE 1. L'INDIVIDU ACTEUR DE SON BIENETRE

1033. **Le bien être une composante de la santé personnalisée.** Le préambule de la Constitution de l'Organisation mondiale de la santé intégré la notion de bien être dans la définition de la santé *« La santé est un état de complet bien-être physique, mental et social, et ne consiste pas seulement en une absence de maladie ou d'infirmité. »* Il est aujourd'hui établi que la pratique régulière d'activité physique agit favorablement sur plusieurs aspects de la santé physique, psychologique et sociale. L'activité physique fait par ailleurs, l'objet de campagnes locales[711] régionales[712] et, nationale. Cette approche de la santé sous l'angle de la prévention est depuis la loi de modernisation de notre système de santé du 26 janvier 2016 intégrée au sein du Code de la santé publique. Ainsi, les personnes souffrant d'une affection de longue durée peuvent se voir désormais prescrire, par leur médecin traitant, une activité physique adaptée au sens de l'article L. 1172-1 du Code de la santé publique[713]. Cette mesure concerne 11 millions de Français atteints par exemple de diabète, de cancer, obésité, etc[714].

1034. L'adoption rapide des applications et objets connectés[715] par la population permet désormais à tout un chacun de devenir un

---

[711] G. UTARD. *« Grand Nancy - Déplacements Et si marcher vous rapportait ? »* L'Est Républicain, 27.09.2018.

[712] Les directions régionales de la jeunesse de la santé et des sports multiplient les campagnes de promotion de l'Activité Physique pour la Santé. A titre d'exemple,

[713] C. santé publ. art. D. 1172-1 à D. 1172-5.

[714] Décret n°2016-1990 du 30 décembre 2016 relatif aux conditions de dispensation de l'activité physique adaptée prescrite par le médecin traitant à des patients atteints d'une affection de longue durée

[715] « *D'une façon générale, on parle d'objet connecté pour désigner divers capteurs de données physiques qui, avec la démocratisation des terminaux mobiles et tactiles connectés à internet, peuvent transmettre l'information captée et quantifiée à tout moment. Appliqué au corps, ce mouvement, également appelé "quantified self " (mesure de soi) consiste à enregistrer régulièrement via une application des données physiologiques : poids, taille, tension, rythme cardiaque, glycémie, etc* »F. Eon. Objets connectés : Comment concilier amélioration de la

véritable acteur de son bien-être et de sa santé. En permettant à l'utilisateur de bénéficier de l'information dans un format compréhensible prenant généralement la forme d'un graphique, de pourcentages, etc. la santé n'est plus le monopole du médecin. L'individu peut par son hygiène de vie influencer directement sur son état de santé devenant un véritable acteur de son bien-être. Le chercheur invite à étudier si les données produites par des dispositifs connectés constituent des données de santé, (Section 1). Lors de qu'il a recours à une application de bien-être, les traitements mis en œuvre afin d'évaluer ses performances ou ses habitudes de vie impliquent nécessairement son consentement préalable (Section 2).

santé publique et respect de la vie privée ? », Revue Lamy Droit de l'Immatériel, n°125, 1er avril 2016.

Section 1. Du bien-être à la santé

1036. **Le bien-être une activité productrice de données de santé.** Le Règlement 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, définit la donnée de santé de façon à inclure les données physiologiques. Antérieurement, en l'absence de définition textuelle donnée de santé, le traitement de données de bienêtre ne constituait pas *a priori* un traitement de données de santé. En raison de ce vide juridique, les fournisseurs de dispositifs connectés, échappaient à l'interdiction de principe de tout traitement de données sensibles. Le seul moyen de régulation *a priori* consistait en l'obligation de déclarer préalablement le traitement auprès services de la CNIL. Le traitement de données de bien-être était donc réalisé dans le cadre du droit commun de la protection des données. En l'absence de mesures coercitives les responsables de traitement et les sous-traitants, ne procédaient pas à la mise en œuvre spontanée de mesures appropriées à la nature de ces données. Par ailleurs celles-ci pouvaient, en raison de l'absence de pouvoirs de contrôles effectifs et de sanctions adaptés faire l'objet d'usages pouvant porter atteintes aux droits et libertés de la personne. Ces données sont désormais susceptibles de constituer des données de santé.

1037. Si les données physiologiques produites par les dispositifs médicaux demeurent des données de santé (paragraphe 1) les données produites par des objets connectés dès lors qu'elles apportent un élément de connaissance sur la santé de la personne constituent des données de santé qui peuvent être traitées en dehors de toute prise en charge par le système de santé (paragraphe 2)

§ 1. Une donnée produite par un dispositif médical

1039. Ces dix dernières années ont été marquées par de grandes innovations en matière de technologies de l'information et de la communication. Le secteur de la santé n'a pas été épargné par ce contexte. En raison de la convergence entre la médecine personnalisée et la pratique consistant en la mesure de soi, ainsi que le développement des applications spécialisées, il existe désormais une zone grise entre les dispositifs médicaux et les objets connectés utilisés à des fins de bien-être, il s'agit des dispositifs de santé mobile ou m-santé[716]. Ces systèmes ne constituent pas des dispositifs médicaux ou encore des applications et objets connectés utilisés à des fins de bien-être, elles sont utilisées à des fins de médecine personnalisée sans pour autant disposer *« de finalité médicale déclarée »*[717].

1040. Ces dispositifs, parce qu'ils sont mis directement à disposition du grand public, connaissent un essor considérable. Cette mutation engendre des réflexions ainsi qu'un « *changement de paradigme de l'évaluation ou de la régulation/certification [et] pose la difficulté d'outils d'évaluations adaptés, spécifiques et flexibles dans le temps »*[718] notamment en ce qui concerne la fiabilité, la qualité de ces applications et objets de m-santé ainsi que la sécurité des utilisateurs, que ce soit au niveau des atteintes potentielles à la vie privée ou à l'intégrité physique[719].

---

[716] L'organisation mondiale de la santé (OMS) définie la santé mobile comme des *« pratiques médicales et de santé publique supportées par des appareils mobiles, tels que les téléphones mobiles, les dispositifs de surveillance des patients, les PDA et autres appareils sans fil. »*. Voir en ce sens, World Health Organization. mHealth. New horizons for health through mobile technologies : second global survey on eHealth. Geneva: WHO, 2011.

[717] Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou mHealth). HAS, octobre 2016. p. 10.

[718] Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou mHealth). HAS, octobre 2016.

[719] L'Organisation mondiale de la santé (OMS) s'est livrée lors d'une étude relative à la e-santé en europe, à une analyse des systèmes mis en œuvre pour

L'utilisation de ces objets dans le cadre d'une prise en charge sanitaire, posent également la question de la responsabilité qui peut être, selon le cas d'espèce, partagée ou non entre le fabricant et le professionnel de santé utilisateur. *« L'agence nationale de sécurité du médicament et des produits de santé (ANSM), autorité compétente en matière de DM notamment pour la surveillance du marché et la « vigilance » de ces produits, propose sur son site Internet des éléments d'appréciation aidant à déterminer si une App en santé relève du statut du DM ou non au regard de sa finalité. Elle indique notamment les conséquences ainsi que la marche à suivre pour commercialiser les Apps qualifiées de DM (marquage CE, réalisation d'une analyse de risque et constitution de documentation technique, etc.) »*[720]

1041. Le droit considère certaines applications et objets connectés comme pouvant être des dispositifs médicaux. Cependant, toutes les applications et objets connectés, ne constituent pas nécessairement des dispositifs médicaux. Le Code de la santé publique définit à l'article L. 5211-1 les dispositifs médicaux comme *« tout instrument, appareil, équipement, matière, produit, à (…), ou autre article utilisé seul ou en association, y compris les accessoires et logiciels nécessaires au bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins médicales (…). Constitue également un dispositif médical le logiciel destiné par le fabricant à être utilisé spécifiquement à des fins diagnostiques ou thérapeutiques ».*

évaluer la qualité, la sécurité et la fiabilité des dispositifs de m-santé. Voir en ce sens, « *De l'innovation à la mise en œuvre : la cybersanté dans la Région européenne »*, OMS, 2016. Voir également, Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou mHealth). HAS, octobre 2016.

[720] Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou mHealth). HAS, octobre 2016. p. 12.

1042. *« Les objets connectés permettant de suivre et mesurer des paramètres physiologiques et/ou vitaux […] Elles sont censées permettre une approche préventive, extrêmement personnalisée et complémentaire à l'approche curative du système de santé actuel »*[721].

1043. Il en résulte qu'un *« objet connecté en matière de santé peut constituer un dispositif médical. En effet, cette réglementation des dispositifs médicaux peut concerner les applications de santé issues de dispositifs mobiles et les objets connectés dès lors qu'un dispositif médical vise tout appareil, équipement ou logiciel »*[722] destinés par le fabricant à être utilisés, seuls ou en association, chez l'homme pour une ou plusieurs finalités médicales précises. Ces finalités comprenant notamment le diagnostic, la prévention, le contrôle, la prédiction, le pronostic, le traitement ou l'atténuation d'une maladie, d'une blessure ou d'un handicap ou la compensation de celui-ci ainsi que l'investigation, c'est-à-dire l'étude d'un état physiologique[723].

1044. Le Règlement 2017/745 ne modifie pas fondamentalement la définition de dispositif médical, déjà présente au sein de la Directive de 1993[724]. Ainsi, la condition selon laquelle, il appartient au fabricant, de déterminer et de revendiquer la finalité médicale du dispositif qu'il souhaite commercialiser demeure. Les dispositifs médicaux, contrairement aux objets connectés destiné au bien-être font

[721] C. Jay, le risque sante et la souscription d'assurance du crédit. Thèse. Nancy. 2017, p. 152.

[722] A. Mendoza-Caminade *« Big data et données de santé : quelles régulations juridiques ? »*, Revue Lamy Droit de l'Immatériel, Nº 127, 1er juin 2016.

[723] Règl. n° 2017/745 du Parlement européen (PE) et du Conseil (Cons. UE), 5 avr. 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, article (art.) 2, paragraphe (§) 1.

[724] Directive (Dir.) n° 93/42/CEE du Conseil, du 14 juin 1993, relative aux dispositifs médicaux, article (art.) 1, paragraphe (§) 2, a).

l'objet de procédures d'évaluation de leur conformité définies au sein du Règlement 2017/745 afin de permettre aux fabricants de démontrer le respect des exigences. Cette conformité est matérialisée par un marquage CE spécifique en fonction de la classe à laquelle appartient le dispositif. Une fois marqué ces dispositifs vont entrer dans le champ de compétence de l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) qui va pouvoir opérer des contrôles sur le respect, par les fabricants, des spécifications techniques minimales.[725]

1045. *« C'est pour ces raisons que les produits grand public, destinés avant tout au bien-être, se sont développés bien plus rapidement que les objets destinés à la prise en charge médicale des personnes. »*[726] De ce fait, il existe de nombreux produits qui peuvent être déclinés et commercialisés soit, en qualité de dispositif médical et, dans ce cadre, vont être mis à disposition du patient lors d'une prise en charge classique soit, sous la forme d'objets connectés dits de bien-être qui sont destinés au grand public et peuvent être acquis par le consommateur, à partir de plateformes d'achats ou auprès de la grande distribution.

1046. À titre d'exemple, les systèmes de pesée destinés à l'équipement des professionnels de santé constituent des instruments de pesage à fonctionnement non automatique (IPFNA). Il s'agit de dispositifs médicaux qui sont soumis au respect de la métrologie légale afin de permettre la réalisation d'examens médicaux[727]. *A contrario*, les systèmes commercialisés en faveur du grand public, qu'ils s'agissent, d'objets connectés ou non, ne sont pas soumis à cette obligation.

---

[725] Loi n° 2011-2012 du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé

[726] C. Jay, le risque sante et la souscription d'assurance du crédit. Thèse. Nancy. 2017, p. 153.

[727] Directive (Dir.) n° 2014/32/UE du Parlement européen (PE) et du Conseil (Cons. UE), du 26 février relative à l'harmonisation des législations des Etats membres concernant la mise à disposition sur le marché d'instruments de mesure (refonte).

1047. De la même manière, l'ANSM considère au regard de la définition posée par les textes, que certaines applications de télémédecine, ne constituent pas des dispositifs médicaux. Ainsi l'acte de télé-suivi réalisé dans le cadre de la pratique de la télémédecine[728] peut recourir à une application *« reliée à une plateforme qui permet le télé-suivi du patient depuis son domicile. […] Le logiciel permet le recueil de données des patients suite aux réponses à des questionnaires ou via une communication grâce à des objets connectés (balances, tensiomètres…). Les données des patients transitent par un serveur et sont transmises vers un centre de télé-accompagnement où les patients sont suivis par des professionnels de santé. Le médecin peut ainsi suivre à distance l'état de santé du patient et planifier des rendez-vous, et reçoit, par ailleurs, des rapports mensuels de l'état du patient et peut, si besoin, modifier des protocoles établis. La destination de cette application est le suivi à distance des patients à domicile et la planification/modification des soins par le personnel soignant. […] »*[748]

1048. Pour l'ANSM, *« cette application correspond donc à une base de données permettant le stockage et la communication d'informations saisies par le patient vers le médecin »*. Elle ne possède donc pas de fonctions particulières permettant de générer une action spécifique à des fins diagnostiques ou thérapeutiques. Elle ne répond pas, par conséquent, à la définition de dispositif médical mais correspond à une application de m-santé.

---

[728] La télémédecine est définie à art. L. 6316-1 du Code de la santé publique (C. santé. publ.) comme *« une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication […] qui met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de santé, parmi lesquels figure nécessairement un professionnel médical et, le cas échéant, d'autres professionnels apportant leurs soins au patient. »* Les actes constituant cette pratique médicale sont décrits à l'article R. 6316-1 C. santé publ.. Ces actes inclus *« la télésurveillance médicale, qui a pour objet de permettre à un professionnel médical d'interpréter à distance les données nécessaires au suivi médical d'un patient et, le cas échéant, de prendre des décisions relatives à la prise en charge de ce patient. L'enregistrement et la transmission des données peuvent être automatisés ou réalisés par le patient lui-même ou par un professionnel de santé »* 748 Disponible sur le site : www.ansm.sante.fr

1049. Un dispositif médical connecté est, en règle générale, *« connecté à un SIS directement ou à distance (par exemple via Internet). Ce dispositif intègre des matériels (serveur, périphériques, dispositif électronique spécifique, ...), des logiciels (systèmes d'exploitation, logiciel embarqué, microgiciel) et des données (fichiers, bases de données, ...) et qui assure, dans un processus de soin, une fonction de traitement médical, d'analyse médicale, de surveillance médicale, de diagnostic ou de supervision. »* [729] Les données produites par ces dispositifs médicaux connectés permettent le plus souvent d'effectuer des mesures de fréquence cardiaque, de température, de SpO2, etc. Il s'agit de données issues de la captation de constantes physiologiques. Ces valeurs sont transmises de manière régulière ou continue mais demeurent des données brutes jusqu'à leur intégration au dossier du patient.

1050. Lorsqu'elles sont incorporées et conservées au sein des systèmes d'information ou du système d'information des établissements de santé ou des cabinets médicaux. Elles sont, par ce moyen, associées aux autres données concernant le patient et permettent de l'identifier et d'en déduire des informations sur son état de santé. Ces données constituent alors une donnée à caractère personnel relatives à la santé et sont soumises aux dispositions du Règlement 2016/679[730].

[729] 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). ASIP Santé. novembre 2013. v1.0. p. 6.

[730] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, considérant 35.

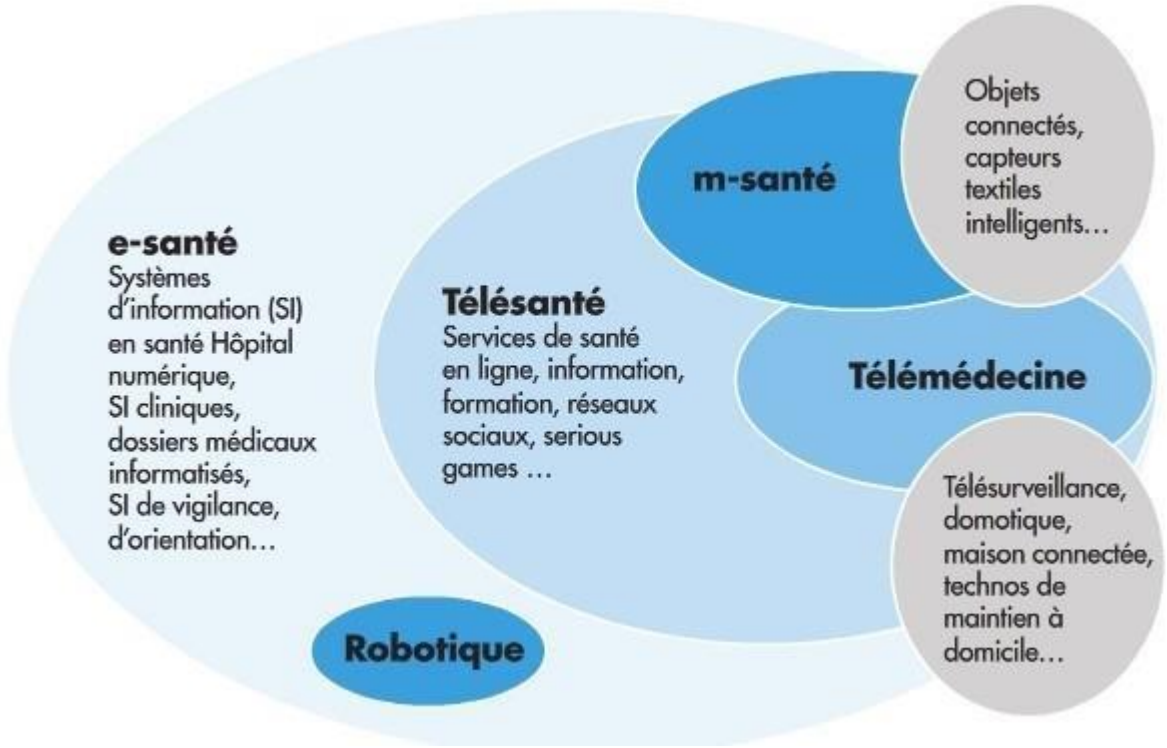


Figure 7 : Les objets connectés de santé, au croisement de la m-santé, de la télémédecine, de la télésanté et de la e-santé. Source : CNOM

§ 2. Un élément de connaissance sur l'état de santé

1051. Nous l'avons préalablement démontré, à l'image de la définition retenue par Cour de justice de l'union européenne (CJCE), le RGPD a retenu, une interprétation extensive, de la donnée à caractère personnel relative à la santé mettant fin au floue entretenu entre le concept de bien-être et de santé. À titre d'information, la CJCE, en 2003, dans le cadre de l'arrêt Bodil Lindqvist précédemment cité[731], avait considéré que les termes « *données relatives à la santé* » employés à l'article 8 paragraphe 1 de la Directive de 1995[732], devaient être interprétés de

[731] CJCE, 6 nov. 2003, Bodil Lindqvist, C-101/01.

[732] Dir. n° 95/46/CE PE et Cons., 24 oct.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, JOCE L 281 du 23 nov. 1995 p. 31.

manière à comprendre « des informations concernant tous les aspects, tant physiques que psychiques de la santé d'une personne. »

1052. Compte tenu du considérant (35) du RGPD, la définition de l'article 4 du Règlement inclus dans la catégorie des données sensibles les données physiologiques collectées ou produites par les applications et dispositifs connectés. Les dispositifs à destination du grand public, repose le plus souvent sur une utilisation dans le cadre d'une activité strictement personnelle ou domestique[733]. Cette circonstance est de nature à exclure l'utilisation de dispositifs connectés à des fins strictement personnel du champ d'application matériel du Règlement. Toutefois, le Règlement général, s'applique aux responsables de traitements ainsi qu'aux sous-traitants qui fournissent les moyens de traiter ces données physiologiques pour de telles activités.

1053. Nous l'avons précédemment précisé, jusqu'à l'entrée en vigueur du RGPD, les informations recueillies ou produites par les capteurs des dispositifs de bien-être n'étaient pas considérées comme constituant des données à caractère personnel relatives à la santé. *« Ces objets permettent à une personne de capter des données issues de son corps ou liées à celui-ci, comme sa tension, son rythme cardiaque, pour une meilleure connaissance de soi. Ils conduisent les personnes à livrer elles-mêmes des données de santé mobiles via internet. »*

1054. Ainsi, bien qu'elles puissent permettre d'enregistrer des constantes pouvant donner lieu à un diagnostic de l'état de santé d'une personne, les traitements de données physiologiques mis en œuvre au moyen de ces dispositifs, ne se trouvaient pas régies par les dispositions applicables aux données sensibles. Elles ne bénéficiaient pas de ce régime particulièrement protecteur, interdisant, par principe toute opération de traitement sur ces données sauf à entrer dans le champ des exceptions et à

[733] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, art. 2, paragraphe (§) 2),),„), c).)).)

préalablement demander l'autorisation à la CNIL et, à démontrer les mesures de sécurité et de confidentialité appropriées.

1055. Tirant profit de l'absence de définition a priori des données de santé, les organisations conservant ces données hybrides ont cultivé cette ambigüité afin d'échapper aux dispositions applicables aux hébergeurs de données de santé. Par la même occasion, ils ont parfois exploité ces données à d'autres fins que celles portées à la connaissance des utilisateurs de ces dispositifs.

1056. Notons que cette distinction fictive entre la donnée à caractère personnel relative à santé et la donnée de bien-être reste toutefois surprenante. En effet, si l'on se réfère à la définition de la santé de l'Organisation Mondiale de la Santé (OMS) la notion de bien-être figure dans celle de la santé, il s'agit par ailleurs de l'une de ses composantes fondamentales. Ainsi *« La santé [serait] un état de complet bien-être physique, mental et social, et ne [consisterait] pas seulement en une absence de maladie ou d'infirmité »*[734]. Il est donc surprenant que les institutions et juridictions ne se soient pas référées à cette définition.

1057. La Commission européenne face au développement de ces dispositifs a élaboré le 10 avril 2014 un livre *« Livre vert desur la santé mobile*[735]*. Elle y rappelle qu'« en Europe, la protection des données à caractère personnel est un droit fondamental consacré par l'article 8 de la Charte des droits fondamentaux de l'Union européenne ainsi que par l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne (TFUE) »*.[736] Pour mettre fin à ces abus, elle insiste dans ce

[734] Préambule à la Constitution de l'Organisation Mondiale de la Santé, 1946.

[735] Notons que selon l'étude menée par le cabinet GFK, plus grand cabinet d'étude et d'audit marketing d'Allemagne, en 2016, les Français ont acheté plus d'un million d'objets connectés, soit une hausse de 28 % par rapport à l'année 2015.

[736] Commission Européenne, *Livre vert sur la santé mobile,* 10 avr. 2014, p. 9.

rapport sur la nécessité d'apporter une protection adaptée à ces dispositifs contribuant à la massification des données.

1058. Toutefois, les dispositifs juridiques développés au sein de la directive de 1995 ne permettant pas de répondre entièrement à cette problématique. Aussi, la définition de la donnée de santé au sein Règlement général sur la protection des données du RGPD a été façonnée par cet impératif afin d'apporter un « *niveau élevé et uniforme de protection des individus, [garantissant] la sécurité juridique aux entreprises et [suscitant] une confiance accrue dans les services de santé en ligne ».*[737] « *Le Règlement intègre donc à la donnée de santé « l'état physiologique (…) 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 »*[738]. Par cette disposition, le Règlement fait de toute information physiologique une donnée de santé. Cette unification nous semble, de prime abord, excessivement contraignante compte tenu du régime spécifique applicable aux données à caractère personnel relatives à la santé. Elle conduit, par ailleurs, à considérer la donnée indépendamment de la finalité du traitement. Il aurait été concevable, selon nous, de définir un régime dérogatoire. Dans ce raisonnement, selon la qualité des capteurs du dispositif, selon le fait qu'ils soient certifiés *« medical device »*[739], que leur utilisation soit réalisée sous le contrôle d'un professionnel de soins, ou qu'il s'agisse de dispositifs dont l'utilisation est destinée au grand public et exclusivement à des fins de coaching, c'est à dire sans que les données

[737] Ibid.

[738] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 2016, préc. §, 35, Préambule.

[739] De par leur nature, certains objets connectés qui peuvent être utilisés à des fins de bien-être ou pour la santé à des fins de diagnostic, de prévention, de contrôle, de traitement ou d'atténuation d'une maladie peuvent être qualifiés de dispositifs médicaux. La qualification d'un objet connecté comme dispositif médical dépend de l'usage prévu et de la volonté du fabricant. La certification d'un dispositif médical est encadréeencadré par le Règlement (UE) 2017/745 du Parlement européen et du Conseil 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.

recueillies ou produites ne soient traitées à d'autres fins, les données le composant devraient être ou non considérées comme des données de santé et faire l'objet de mesures de protection et de contrôle adaptées à leur sensibilité. *A contrario,* la donnée qualifiée de simple donnée physiologique, devrait dans ce contexte et compte tenu de la finalité des traitements relatifs au bien-être, ne devrait pas être soumis à un régime dérogatoire du droit commun sans pour autant relever de celui applicable aux données sensibles.

1059. Ainsi, les données de quantification, pour lesquelles la personne concernée par le traitement y aurait consenti, vont être collectées directement par le dispositif mobile, par la simple utilisation qui en est faite par le consommateur. Contrairement à une utilisation traditionnelle où un professionnel de santé peut être amené à intervenir [740], aucune intermédiation n'a lieu dans le processus de collecte, la donnée est captée et va être conservée dans le *« cloud computing »* [741] ou directement partagée avec d'autre utilisateurs, sur les réseaux sociaux, ou encore avec les acteurs des objets connectés et, jusque lors, avec leurs partenaires commerciaux qui ne sont pas soumis au secret professionnel. Les données vont donc transiter via « Bluetooth » vers le smartphone de l'utilisateur puis par l'internet mobile vers le fournisseur du service. Si ce dernier n'était pas soumis aux dispositions de l'article 9 du RGPD, ainsi qu'au même régime juridique que les acteurs de santé, il n'en demeure pas moins

[740] Il peut s'agir, à titre d'exemple, de l'utilisation d'un Holter, dispositif portable qui permet pendant une période donnée, généralement vingt-quatre heures, d'enregistrer, de manière continue, l'activité électrique du cœur. Le cardiologue a usuellement recours à ce dispositif afin de dépister des troubles du rythme cardiaque survenant de manière épisodique. Dans ce cadre, le cardiologue analyse, a posteriori, les données captées et conservées par ce dispositif.

[741] Habituellement, les données d'un utilisateur sont conservées sur son ordinateur ou, lorsqu'il s'agit de données produites dans le cadre d'une activité professionnelle, sur les serveurs installés en « LAN »,» c'est à dire en réseau local au sein d'une entreprise. Le « cloud computing »,» encore appelé « données dans les nuages »,, désigne la technologie qui permet de conserver des données et d'y accéder à partir de serveurs localisés à distance.

que le traitement de ces données présente les mêmes dangers pour les personnes concernées par leur traitement.

1060. Retenir une approche unitaire et simplifiée de la donnée à caractère personnel relative à la santé étant favorable à la protection des droits et libertés de la personne, le rattachement de la donnée physiologique aux données de santé traditionnellement recueillie ou produite par les acteurs du système de santé nous apparaît *in fine*, opportune.

1062. Section 2. Le consentement pour seule condition

1063. **La santé personnalisée terreau de l'autodétermination informationnelle.** L'autodétermination informationnelle qui permet à la personne de librement décider de l'utilisation de ses données à caractère personnel trouve pleinement vocation à s'appliquer dans le cadre de la santé personnalisée. Rappelons que le traitement de données de bien-être, dès lors qu'il comporte des données à caractère personnel physiologiques ou qu'il est susceptible de *« fournir des informations sur l'état de santé de cette personne »*[742], passé, présent ou futur doit être considéré comme un traitement de données à caractère personnel relatives à la santé[743]. A moins qu'il ne soit possible de distinguer différentes finalités et fichiers, l'ensemble des données traitées se trouvent, en application du *principe specialia generalibus derogant* réglementées par les dispositions spécifiques de l'article 8 de la loi de 1978 et 9 du Règlement de 2016.

1064. A l'image de la télémédecine, le m-santé constitue une pratique médicale, ainsi le traitement est réalisé au titre de l'article 8 II, 6° de la loi de 1978 et 9-2, h) du Règlement. Il s'agit des *« Traitements mis aux fins de la médecine préventive […] de diagnostics médicaux, de la prise en charge sanitaire ou sociale, […] »*

1065. *A contrario,* le traitement mis en œuvre dans le cadre d'une activité de santé personnalisé dès lors qu'il ne s'agit pas d'une pratique médicale personnalisé mais d'un service de bien-être, celui-ci est réalisé exclusivement au titre l'article 8-1 de la loi de 1978 et 9-2, h) du Règlement relatif aux données sensibles c'est-à-dire sur le consentement préalable de la personne.

[742] Règl. (UE). PE et Cons. UE préc. art. 4 § 15.

[743] Règl. (UE). PE et Cons. UE préc. considérant 35.

1066. En l’absence de dispositions nationales contraires le consentement de la personne est déterminant puisqu’il permet la circulation de la donnée et fait de la personne un acteur de sa protection. (Paragraphe 1). Il existe toutefois des circonstances particulières où la volonté de la personne doit être encadrée afin de tenir compte de risques particuliers (Paragraphe 2).

1068. § 1. La prééminence de la volonté

1069. Avec les progrès de la technique se sont développées de plus en plus des application et technologies permettant, la collecte, au quotidien, de données relatives à la santé et, de manière générale, à l'ensemble de nos habitudes de vie et de consommation. Certaines de ces applications et dispositifs sont de purs gadgets mais d'autres contribuent sérieusement à la prévention et au suivi en permettant, à titre d'exemple, de surveiller le niveau d'activité, la tension artérielle et le rythme cardiaque, etc.

1070. Ces technologies reposant, le plus souvent, sur l'utilisation combinée du smartphone et, présentant un coût acceptable, se sont démocratisées devenant ainsi aisément accessibles au grand public. Par effet d'échelle, ce phénomène a provoqué une massification des données produites, suscitant les convoitises et ainsi leur commercialisation et, le détournement de finalités quant à leur traitement. A titre d'exemple, des données collectées par une application à des fins de coaching sportif peuvent ainsi se retrouver utiliser dans le but de connaitre les habitudes alimentaires ou le niveau d'activité des utilisateurs et, permettre d'en déduire l'état de santé d'une personne. Ces données peuvent également être réutilisées afin de leur proposer de la publicité ciblée pour de l'alimentation, des équipements sportifs, etc. ou des polices d'assurance adaptées en raison du fait qu'un groupe d'utilisateurs représentent un moindre risque. En ce qui concerne les prévisions les plus alarmantes, ces traitements pourraient permettre d'identifier un groupe de population constituant un gros risque assurantiel ou de sélectionner des cocontractants refusant d'utiliser ces dispositifs, afin de les exclure de toute garantie.

1071. Notons également que ces services et applications sont, le plus souvent librement accessibles en ligne et qu'il existe désormais des dispositifs de collecte de données à bas prix disponibles sur internet mais

aussi, en grande surface. Par ailleurs, les fournisseurs de ces services ne sont pas nécessairement de grandes entreprises, il peut également s'agir d'entrepreneurs individuels ou de petites et moyennes entreprises (PME) ne disposant pas des connaissances et des moyens permettant d'assurer un niveau de conformité et de sécurité des traitements approprié. De plus, le plus souvent, ces entreprises sont situées en dehors de l'Union européenne. Il s'agit essentiellement d'entreprises américaines ou encore asiatiques, etc. qui initialement n'étaient pas systématiquement soumises à la règlementation européenne en matière de protection de données à caractère personnel. C'est dans le but de règlementer le traitement de ces données, que le Parlement a adopté la proposition de la Commission, consistant à intégrer les données physiologiques, dans la définition des données à caractère personnel relatives à la santé.

1072. S'agissant de données à caractère personnel relatives à la santé, le principe demeure l'interdiction de tout traitement.

> *« Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. »*[744]

1073. Rappelons que la violation de ce principe est sanctionnée au titre de l'article 226-19 du code pénal par une peine de cinq ans d'emprisonnement et de 300. 000 euros d'amende. Cependant, celui-ci

[744] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 2016, pré, art. 9.

souffre de plusieurs exceptions qui existaient déjà au sein de l'article 8 de la Directive de 1995[745]. De ce fait, la mise en œuvre de traitement de données physiologiques doit également relever de l'une des exceptions listées à l'article 9 du Règlement. Ainsi, en dehors de toute prise en charge traditionnelle nécessitant la supervision d'un acteur de santé et, la mise en œuvre d'un traitement à des fins de médecine préventive, de diagnostics et de services de soins de santé ou de protection sociale[746], le consentement de la personne concernée est déterminant[747]. Il fait de celle-ci un acteur de sa santé et de la protection de sa vie privée.

1074. À ce titre, le point a) du 2) de l'article 9 du Règlement admet que la personne concernée par le traitement puisse consentir explicitement au traitement des données à caractère personnel la concernant pour une ou plusieurs finalités spécifiques. Elle prévoit toutefois que le droit de l'Union ou le droit d'un État membre peut aménager des exceptions à cette exception au moyen de dispositions législatives expresse, privant de tout effet la levée de l'interdiction de principe, par le simple accord de volonté de la personne concernée.

1075. Nous l'avons auparavant explicité, en faisant notamment part de son caractère « éclairé et univoque »[748], le Parlement et le Conseil, ont pris le soin de renforcer au sein des articles 4 et 7 du RGPD, les garanties entourant le recueil de ce consentement, de conditions de

[745] Dir. (UE). PE et Cons. UE 1995/46, 24 oct. 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, art. 2. JOUE L 281, 23 nov. 1995.

[746] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, art. 9, 2), h. JOUE n° L 119, 4 mai 2016.

[747] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, art. 9, 2), a. JOUE n° L 119, 4 mai 2016.

[748] Protection des données personnelles – Bénédicte Fauvarque-Cosson – Winston Maxwell – D. 2018. 1033

validités que l'on ne retrouve pas en droit commun des contrats[749]. Ils disposent en outre, que le consentement ne peut être présumé comme ayant été exprimé *« librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce »*[750].

1076. La charge de la preuve incombant explicitement au responsable de traitement, le Règlement oblige également celui-ci à concevoir et, à mettre en œuvre, des mécanismes de recueil et de conservation du consentement opposables, permettant à la personne concernée par un traitement de données, de se rétracter à tout moment, article 7, 3) et 4) du Règlement.

1077. En matière de protection des données à caractère personnel relatives à la santé, il n'existe pas, à ce jour, au sein du droit de l'Union européenne et de notre droit national de disposition interdisant expressément le traitement de données à des fins de bien-être.

1078. Le droit est confronté à l'essor des dispositifs connectés et de services en ligne de bien-être et de santé. Cette situation engendre plusieurs interrogations, notamment en ce qui concerne la forme ainsi que de la validité du consentement donné lorsque celui-ci conditionne également l'utilisation du dispositif. Il en est de même concernant un service de santé en ligne, librement accessible aux internautes ou dont l'utilisation est subordonnée au consentement au traitement de données du futur utilisateur.

1079. Habituellement, les données physiologiques collectées par la plupart de ces instruments, ne sont pas indispensables pour l'utilisation

[749] B. FAUVARQUE-COSSON, W. MAXWELL, « Protection des données personnelles », *D.* 2018, chron. p. 1033.

[750] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, considérant 43. JOUE n° L 119, 4 mai 2016.

du service ou de certaines de ces fonctionnalités. Toutefois, le consentement au traitement de ces données, est réalisé au moment de l'initialisation de l'application. Ainsi, pour pouvoir bénéficier du service, il est indispensable pour l'utilisateur, de consentir aux conditions générales d'utilisations ainsi qu'au traitement de l'ensemble de ces données y compris celles dont la collecte n'ait pas toujours indispensable.

1080. Jusqu'à présent, aucune disposition spécifique de la Directive de 1995 ou de la loi de 1978 ne venait régir ce cas de figure et, le droit commun, ne permettait pas non plus d'y répondre. Les vices du consentement reposaient, en effet, uniquement sur la violence, l'erreur ou le dol. Il apparait désormais, compte tenu des nouvelles dispositions relatives au consentement figurant au 4) de l'article 7 du Règlement, que dans ces circonstances, le consentement ne peut être donné librement.

> *« Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat. »*[751]

1081. Concernant la forme du consentement, nous rappellerons ici, que s'agissant d'objet connecté, leur utilisation ne s'aurait suffire à matérialiser ipso facto l'adhésion de la personne concernée au traitement de ses données à caractère personnel relatives à sa santé. Un tel raccourci

[751] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, article (art.) 7, 4). JOUE n° L 119, 4 mai 2016.

serait contraire aux dispositions de l'article 9 du Règlement notamment en ce qui concerne le caractère spécial et explicite du consentement.

1082. Peut-on considérer, lorsque l'utilisation du dispositif ou de l'application est réalisée dans un cadre privé et non dans le cadre d'une prise en charge traditionnelle nécessitant l'intervention ou le contrôle d'un professionnel, qu'une simple case à cocher préalablement à l'utilisation d'une application suffise à matérialiser la réalité du consentement exprimé ?

1083. Bien évidemment, s'agissant de données de santé, antérieurement au RGPD, la pratique de l'opt-in passif, consistant à décocher une case ou un menu déroulant proposant, par défaut, une acceptation du traitement, n'était déjà pas considérée comme l'expression d'un consentement explicite. *A contrario,* le système de l'opt-in actif consistant, par exemple, en une case à cocher est et demeure acceptable. L'originalité du Règlement repose, en ce qui concerne les données physiologiques, à leur rattachement aux données de santé, y compris lorsque celles-ci sont collectées ou produites au moyen de dispositifs de bien-être. Ce faisant, le consentement explicite de l'utilisateur, au traitement de ses données de santé à caractère personnel, est également exigible dans ce cas de figure.

1084. Ainsi, à titre d'exemple, en matière d'application de santé et fitness, le dispositif, fictif, de recueil de consentement relatif au traitement de données de santé physiologiques, représenté ci-dessous, lorsqu'il est précédé des informations visées par les articles 13 et 14 du Règlement et que celles-ci sont exprimées de manière « concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples », remplis les exigences du Règlement.

1086.

1087. Finalité du traitement

1088. Dénomination du responsable de traitement collecte traite et conserve vos informations personnelles pour vous fournir les informations ou les services auxquels vous avez souscrit et qui concernent votre coaching santé et fitness personnalisé.

1089. Durée de conservation

1090. Vos informations personnelles sont conservées par Identité du responsable de traitement (ID) et ses sous-traitants (listés ci-dessous) uniquement pour le temps correspondant à la souscription du service. Elles seront immédiatement effacées lors de la suppression de votre compte.

1091. Identité des sous-traitants

1092. ID sous-traitant n°1

1093. Vos droits

1094. (…)

1095. ☐ Je consens à la collecte et au traitement de mes données personnelles dans les conditions définies ci-dessus.

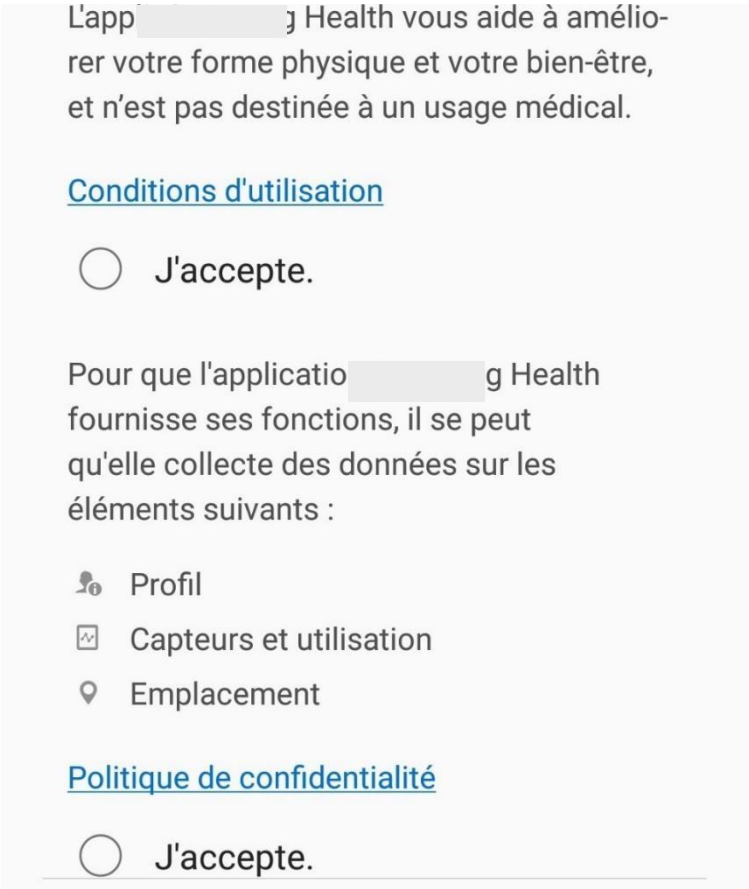
1096. ☐ Je reconnais avoir pris connaissance des conditions générales d'utilisation et les accepter sans réserve.

1097. Un autre exemple concernant, cette fois-ci, une application existante et destinée au grand public. Celle-ci se présentant comme étant conçue principalement à des fins de conservation de suivi mais aussi de conseil et d'amélioration des performances sportives des personnes. La page de téléchargement de l'application concernée comporte à plusieurs reprises la mention « santé » exprimée en français mais aussi en anglais « health ».

1098. Toutefois, lorsqu'on a procédé au téléchargement de l'application et, qu'on analyse attentivement la page d'information et de consentement, celle-ci ne comporte nullement les mentions exigées par le Règlement. Elle renvoie par ailleurs aux conditions d'utilisation et à la politique de confidentialité, comprenant ces mentions. Toutefois, la prise de connaissance préalable des conditions générales d'utilisation et de la

politique de confidentialité n'est pas indispensable pour pouvoir cocher la case « J'accepte ». Pire encore, cette application comporte expressément la mention selon laquelle elle n'est pas destinée à un usage médical mais à l'amélioration de la forme physique et du bien-être de l'utilisateur alors même qu'elle permet le suivi régulier de son activité et qu'elle peut collecter des données au moyen d'un cardio-fréquence-mètre, recueillir les données de géolocalisation de l'utilisateur ainsi que l'indication de son identité sexuelle, de sa date de naissance, de sa taille, de son poids et de son niveau d'activité. Aussi, cette mention peut induire en erreur l'utilisateur, non pas sur la finalité du traitement mais sur la nature des données collectées et traitées. Son téléchargement nécessite, par ailleurs, une identification, préalable, à partir d'un compte mail nominatif et une authentification forte au moyen d'un dispositif « one time password » (OTP) ou mot de passe à usage unique. Son utilisation laisse enfin peu de doute sur l'identité de l'utilisateur puisqu'elle nécessite également la création d'un compte personnel.

1099.



1100. Ce cas concret, ne respecte pas, selon nous, les dispositions des articles (art.) 7, 12 et 13 ainsi que les recommandations du 32 du Règlement qui précisent que « si le consentement de la personne concernée est donné à la suite d'une demande introduite par voie électronique, cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé ».

1101. La portabilité des données. L'utilisation des applications de bien-être, et le recours aux services de santé en ligne, génèrent des données des données qui sont ou ne sont pas à caractère personnel en plus des données relatives à la santé. Ces données sont, le plus souvent, nécessaires au fournisseur pour l'utilisation du service et la gestion du compte utilisateur. Il peut arriver qu'elles soient exploitées à d'autres fins.

1102. Antérieurement à l'entrée en vigueur du RGPD, la loi pour une République numérique a consacrée à l'article 48[752] un droit à la récupération et à la portabilité des données.

1103. Ce droit a été codifié au sein du Code de la consommation aux articles L. 224-42-1 à L. 224-42-4. Il prévoyait que les données qui peuvent résulter de l'alimentation de fichiers mis en ligne par l'utilisateur ou de l'utilisation du compte de l'utilisateur et qui sont consultables en ligne ainsi que toutes les données qui facilitent le changement de fournisseur de service ou qui permettent d'accéder à d'autres services puissent être récupérées, par le consommateur, par une requête unique.

1104. Une distinction était toutefois opérée entre les données présentant un caractère personnel et les données anonymes. En effet, en ce qui concerne les données à caractère personnel, la demande devait être réalisée dans les conditions définies à l'article 20 du Règlement 2016/679, alors que pour les données anonymes elle devait être réalisée dans les conditions définies à la sous-section 4 de la section 3 « Contrats de services de communications électroniques » du Code de la consommation.

1105. Ces dispositions ont été abrogées à la suite de l'entrée en vigueur de la loi de 2018 modifiant les dispositions de la loi de 1978 et précisant les modalités d'application du RGPD.

1106. Nous sommes favorables à la suppression des articles du Çode de la consommation car ces dispositions n'étaient de nature à contribuer à la qualité de la loi. En effet la dilution des conditions de mises en œuvre de ce droit à la portabilité au sein des différents codes et lois ne contribue pas à la bonne compréhension ainsi qu'à la clarté du régime juridique applicable. Par ailleurs, les données mentionnées à l'article L. 224-42-1 du code de la consommation à partir du moment où elles sont rattachées à un compte utilisateur nominatif et qu'elles ne font pas l'objet

[752] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, article (art.) 48.

de mesures d’anonymisation, présentent un caractère personnel et entrent dans le champ d’application matériel du Règlement et par conséquent, ne relèvent pas des articles précités.

1107. Il en résulte que l’article 20 du Règlement est applicable à l’ensemble des données à caractère personnel y compris relatives à la santé, dès lors que leur traitement est mis en œuvre sur le fondement du consentement de la personne concernée et, est effectué de manière automatisée. Ce droit peut conduire le responsable du traitement à transmettre, à la demande de l’utilisateur du dispositif, les données à un autre responsable de traitement dans un format structuré, couramment utilisé et lisible par machine. Ces dispositions sont favorables à la circulation des données à caractère personnel relatives à la santé, puisque le responsable de traitement ne peut s’opposer à cette demande, sauf à invoquer un motif lié à l’exercice d’une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont il serait investi.

1108. Le droit à la portabilité des données est ainsi révélateur de la prééminence de la volonté de la personne et de la maitrise des données le concernant lorsque les traitements sont fondés sur son consentement.

1109.

1110. § 2. La prise en compte de situations spécifiques

1111. Les dispositifs connectés sont accessibles au public. Leur utilisation est fondée sur le consentement de la personne concernée. A ce titre, des mineurs peuvent accéder aux dispositifs et les utiliser (A) Depuis quelques années l'utilisation de ces dispositifs n'a pu uniquement lieu dans un cadre privé ce qui peut entrainer des dérives vis-à-vis d'un droit ou d'une prestation y compris en matière de couverture assurantielle (B)

A. La prise en compte de l'enfance

1112. Il n'existe pas, à notre connaissance, d'étude menée sur l'utilisation des objets et applications connectées par les mineurs. Toutefois, ils commencent à avoir recours à ces applications et à s'équiper de ces dispositifs. Les titulaires de l'autorité parentale ne sont pas toujours conscients des dangers qui peuvent résulter de l'utilisation de leurs données et n'ont pas les connaissances appropriées pour les paramétrer efficacement[753]. L'institut de sondage Ipsos, a réalisé pour le compte de l'association e-Enfance, une étude quantitative sur l'utilisation d'Internet, du smartphone et des jeux vidéo, par les enfants. Cette étude publiée en juin 2009, ne porte pas sur les objets connectés, à proprement dit, mais donne quelques informations et chiffres sur le comportement des mineurs et des « jeunes adultes ». Il ressort de cette étude que « la très grande majorité des enfants de 9 à 17 ans bénéficient d'équipement variés qui peuvent être des moyens de connexion à internet ». Ainsi soixante-cinq pourcent d'entre eux possèdent un smartphone, « *seulement 15% des*

[753] Il ressort au contraire de l'étude *« EU kids online »* menée par *The London school of economics and political science*, que 56%des enfants savent comparer des sites pour en évaluer la qualité et ainsi adapter leur comportement en modifiant les données à caractères personnel qu'ils sont susceptibles de renseigner sur les réseaux sociaux.

enfants de 9 à 10 ans en ont un contre 56% des 11-12 ans, 74% des 13-14 ans et 98% des 15-17 ans (…) 95% ont pour consigne de ne jamais dévoiler des informations les concernant (photos intimes, nom, adresse…) »[754]

1113. Enfin, notons qu'il ressort de cette étude, que « plus d'un enfants sur deux a le sentiment de pouvoir faire ce qu'il veut sur internet sans que ses parents le sachent. 7% le font même déjà ». Il en résulte que les « jeunes adultes » et mineurs ont effectivement accès à internet ainsi qu'à un smartphone et qu'ils sont à même de télécharger et d'utiliser les applications ainsi que les services de bien-être et de santé ou de publier des données à caractère personnel relatives à leur santé.

1114. En ce qui concerne le consentement au traitement de leurs données de santé aux moyens de ces outils. La plupart des applications et services à disposition du grand public ne prévoient pas de contrepartie financière et, par conséquent, échappent à la qualification de service de la société de consommation au sens de l'article 2, 25) de la Directive de 2015[755].

1115. Il existe toutefois des applications proposant des services prestés moyennant une contrepartie financière. Les concernant, le Règlement organise, dans le cadre de l'offre de « services de la société de l'information » [756], le consentement des enfants. Les dispositions concernées, renvoient à l'article 6, a) du Règlement relatif au traitement

[754] *Op. cit.*

[755] Art. 1, b) défini la notion de «service», comme *« tout service de la société de l'information, c'està-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services. »* Dir. (UE). PE et Cons. UE 2015/1535, 9 sept. prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, art. 1. b).

[756] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, article (art.) 8, 1). JOUE n° L 119, 4 mai 2016.

de données à caractère personnel communes mis en œuvre sur le fondement du consentement de la personne concernée et non à celles de l'article 9, a) applicables aux données sensibles.

1116. Il convient de s'interroger sur les dispositions applicables compte tenu de la sensibilité des données. Ainsi, si l'on considère que ces traitements relèvent, en raison de leur caractère onéreux, des dispositions de l'article 8, 1) les enfants, lorsqu'il s'agit de mineurs âgés de treize[757] à quinze ans[758], ne peuvent consentir valablement seuls. Le consentement du ou des titulaires de l'autorité parentale vis-à-vis de ce mineur doit nécessairement être donné conjointement. Ainsi, dans la limite des moyens technologiques disponibles, notamment en ce qui concerne l'authentification, tout traitement qui serait réalisé sans respecter cette condition serait illicite. Après quinze ans, les enfants peuvent consentir seuls à un traitement de données à caractère personnel collectées et traitées dans le cadre de services de la société de l'information.

1117. *A contrario,* si le traitement tombe sous le coup des dispositions de l'article (art.) 9, a). Il n'existe pas de dispositions, laissant supposer de l'application d'un régime spécial, par conséquent, l'appréciation de la validité du consentement, ainsi que la licéité du traitement, relèveraient des conditions de droit commun, *« se pose la question de la validité de la collecte auprès des mineurs, qu'il s'agisse ou non de leurs données personnelles. En principe, le consentement du mineur n'a de valeur que s'il est corroboré par celui d'un parent ou du moins d'un majeur responsable »*[759].

---

[757] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, article (art.) 8, 1) alinéa (al.) 2. JOUE n° L 119, 4 mai 2016

[758] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, article (art.) 7-1 alinéa (al.) 2.

[759] C. Nlend. La protection du mineur dans le cyber espace, Thèse, Picardie, 2007, p. 50.

1118. Ainsi, si nous partons du principe que les dispositions de ces deux articles avaient vocation à s'appliquer alternativement en fonction du caractère onéreux ou gratuit du service souscrit, les traitements ne relevant pas des dispositions de l'article 6, c'est-à-dire, les traitements mis en œuvre dans le cadre de services fournis à titre gratuit, qu'ils relèvent ou non des dispositions de l'article 9, nécessiterait, par conséquent, *de jure*, l'autorisation du titulaire de l'autorité parentale jusqu'aux dix-huitième anniversaire de l'enfant. En effet, la majorité civile étant de dix-huit ans en droit français, le mineur ne peut consentir valablement au traitement de ses données au cours de sa minorité.

1119. Pour les traitements relevant des dispositions de l'article 6, autrement dit, pour les services à titre onéreux, qui nécessiteraient la mise en œuvre de traitements de données à caractère personnel relatives à la santé, le ou les titulaires de l'autorité parentale devraient consentir au traitement concernant les données des mineurs de moins de treize ans dont-ils ont la responsabilité pour que celui-ci soit licite. Entre treize et quinze ans, le consentement du ou des titulaires de l'autorité parental ainsi que du mineur seraient indispensables pour la licéité d'un tel traitement. *In fine* le consentement d'un enfant de plus de quinze ans pourrait consentir seul au traitement de ses données. *In abstracto,* cela aboutirait à mieux protéger les traitements réalisés dans le cadre de services fournis à titre gratuit.

1120. Nous ne souscrivons pas à cette dernière thèse mais constatons toutefois, que les nouvelles dispositions relatives aux données sensibles ne figurent plus, dans le RGPD, au sein d'une section portant sur des « catégories particulières de données »[760] mais dans le cadre d'un chapitre II relatif aux « principes ». Ce chapitre fait coexister différentes dispositions, qu'ils s'agissent de principes relevant du droit commun des traitements ou de dispositions spécifiques. Ce découpage de la norme,

[760] Au sein de la Directive 95/46/CE les dispositions relatives aux données à caractère personnel relatives à la santé relevaient d'une section III intitulée « catégories particulières de données » mettant en évidence, le caractère spécifique des dispositions réglementant leur traitement.

entretient le doute quant à l'articulation entre les articles 8 et 9. Cependant, la distinction opérée au sein de la loi de 1978 entre l'article 7-1 qui figure au sein de la section 1 « Dispositions générales » du Chapitre II relatif aux *« Conditions de licéité des traitements de données à caractère personnel »* et, les dispositions relatives aux données de santé qui, elles, sont situées dans la section 2 du même chapitre qui est dédiée aux *« Dispositions propres à certaines catégories de données »* semble confirmer l'application des dispositions de l'article 9.

1121. Notons cependant que les services, gratuitement accessibles sur Internet, ainsi que les applications, disponibles à partir des plateformes de téléchargement ou « magasins d'applications » ne comportent pas, le plus souvent de dispositifs de gestion du consentement ou d'authentification. Ils sont, de ce fait, librement accessibles aux mineurs. Enfin, le paramétrage du contrôle parental à partir des comptes de ces « magasins d'applications » ne permet pas, le plus souvent, de filtrer les applications de bien-être.

1122. *« Dans ce contexte, seuls la mise en œuvre d'outils de contrôle accessibles à tous sur tous les supports, d'une part, et le développement d'une réelle politique d'éducation (…), d'autre part, semblent à même de pallier, voire de combler [ce vide]. »*[761]

[761] Conseil supérieur de l'audiovisuel (CSA). *« La protection des mineurs à l'heure de la convergence des médias audiovisuels et d'internet »*, mars 2012. p. 7.

1123. B. Le domaine particulier de l'assurance

1124. Ces dernières années, les assureurs ont cherché à innover et à tirer parti des objets connectés afin de personnaliser leurs polices d'assurance en fonction des habitudes comportementales des candidats et de leur proposer conditions tarifaires adaptées à leur hygiène de vie. Au cours de l'année 2015, ce sont développés des offres assurantielles s'appuyant sur les données collectées et communiquées à partir de bracelets connectés, podomètres, cardio-fréquence-mètres, etc. Comme dans de nombreux domaines, ce phénomène a émergé aux États-Unis[762] où des compagnies d'assurance telles que John Hancock, se sont appuyés sur les données produites par leurs assurés afin de surveiller leur hygiène de vie et de faire varier les primes en fonction de leur activité par exemple. Il s'est progressivement développé en Europe et notamment, en France. Toutefois à la différence des polices d'assurance américaines, le droit français ne permet pas aux organismes d'assurance d'augmenter ultérieurement *« le tarif d'un assuré ou d'un adhérent en se fondant sur l'évolution de l'état de santé de celui-ci »*[763]. Cependant, une hausse de tarif peur *« être appliquée de manière uniforme pour l'ensemble des assurés ou adhérents »*[764]. Par conséquent, dans le modèles français, les comportements des souscripteurs n'influençant pas les tarifs, l'assuré consent uniquement à l'utilisation d'objets connectés afin de bénéficier d'avantages en nature, bons d'achats dans des commerces de loisirs, de bien-être, ou de voyages.

[762] Elisa Chelle. *« La complémentaire santé comportementale : un nouveau logiciel assurantiel ? »*. RDSS 2018. p. 674.

[763] Loi n° 89-1009 du 31 décembre 1989 renforçant les garanties offertes aux personnes assurées contre certains risques, article (art.) 6, alinéa (al.) 1.

[764] Loi n°89-1009 du 31 décembre 1989 renforçant les garanties offertes aux personnes assurées contre certains risques, article (art.) 6, alinéa (al.) 2.

1125. Pour les compagnies d'assurance, les données produites et transmises par les dispositifs connectés peuvent permettre de procéder à une analyse plus fine du risque et permettent de compléter les informations collectées lors des éventuels questionnaires médicaux réalisés préalablement à la souscription de la police d'assurance. Ainsi, plusieurs compagnies d'assurance, ont vu l'opportunité que pouvaient représenter les objets connectés auprès d'un échantillon d'assurés et ont offert des dispositifs à leurs clients. C'est notamment le cas de la compagnie Axa qui, sous couvert d'encourager les assurés à devenir acteur de leur propre santé, a offert un dispositif connecté[765] auprès d'un échantillon d'assurés volontaires. Dans le cadre de cette expérimentation, les plus grands marcheurs se sont vu remettre des bons de réduction pour des séances de médecine douce. Notons que cette incitation à des fins de préventions n'est pas l'apanage des assureurs. Ainsi, les agglomérations de Nantes, Bordeaux, Toulouse mais aussi, le Grand Nancy[766] ont également mis en œuvre des dispositifs équivalents au moyen d'une application dont l'utilisation consiste essentiellement à collecter des données de géolocalisation. Pour préserver la vie privée, l'application permet cependant aux utilisateurs d'entrer leurs trajets manuellement. Celle-ci est par conséquent moins intrusive et perd également de son intérêt. Il semble s'agir, en l'espèce, exclusivement de données de bien-être plutôt que de véritables données relative à la santé.

1126. Sans aller jusqu'à dire qu'il est dangereux de laisser volontairement à la disposition de son assureur, des données à caractère personnel relatives à sa santé, cette forme d'utilisation pose de nombreuses interrogations quant à la sécurité des flux de données, quant aux catégories

---

[765] Le vocable dispositif connecté est ici entendu, au sens commun. Il comprant l'objet connecté ainsi que l'application nécessaire à son utilisation, c'est-à-dire à son paramétrage, à l'affichage des constantes et aux renseignements d'informations à caractère personnel. N'entre pas dans cette définition, les dispositifs médicaux connectés qui font l'objet d'un régime juridique spécifique et qui sont définies à art. L. 5211-1 C. santé publ.

[766] G. UTARD. *« Grand Nancy - Déplacements Et si marcher vous rapportait ? »* L'Est Républicain, 27.09.2018.

de données réellement collectées mais aussi vis-à-vis de l'utilisation qui est faite de ces données.

1127. Cet usage constitue une intrusion dans la vie privée de l'assuré concerné par le traitement de ses données. Il ne devrait pas, par conséquent, admettre si facilement les potentielles intrusions de l'assureur, dans sa vie privée, au moyen du dispositif connecté. Nous l'avons précédemment exposé, le droit français exclue la modification tarifaire d'un adhérent en se fondant sur l'évolution de son état de santé ou sur les conjectures de son évolution en raison de ses habitudes comportementales.

1128. Toutefois, d'autres pratiques peuvent naître de la collecte et de l'exploitation de ces données et entrainer des effets recherchés ou induits à l'égard des droits de la personne. Dans ce contexte, il convient de s'interroger sur le fait que le consentement de la personne constitue ou ne constitue pas, une brèche dans le rempart de la protection des droits de la personne.

1129. Au-delà des dispositions législatives précitées et, en l'absence de contrôle, a priori, opéré par la CNIL, l'information de la personne constitue un moyen de protection supplémentaire face aux dangers que peut représenter l'absence de réglementation spécifique de ces catégories de traitements.

1130. En ce qui concerne le responsable de traitement, c'est-à-dire, l'assureur ou le fournisseur du service, nous avons précédemment évoqué ces obligations d'information. Il ne s'agit pas ici d'en détailler, à nouveau, dans le domaine particulier de l'assurance ou dans le cadre plus général du contrat aléatoire ou à exécution successive, le contenu mais le moment auquel intervient la délivrance de l'information.

1131. Remarquons cependant, à titre liminaire que la collecte de données à caractère personnel étant réalisée directement auprès de la personne concernée, les modalités d'exécution de l'obligation d'information sont décrites à l'article 13. Parmi les conditions énoncées

figure l'obligation de reposer le contexte dans lequel vont être collectées les données. Autrement dit, il s'agit de préciser si le traitement a pour fondement la bonne application de dispositions réglementaires ou s'il résulte simplement de dispositions contractuelles. Dans ce cadre, le comportement du souscripteur ne sera pas nécessairement le même en fonction de la nature de l'obligation. Il pourra se montrer plus prudent sur l'utilisation qui est faite de ses données. Autre élément important, s'agissant de contrat pouvant reposer sur l'utilisation d'objets connectés et l'exploitation de données, le caractère obligatoire de l'acceptation du traitement dans la conclusion du contrat ou le caractère subsidiaire de l'acceptation de la transmission des données ainsi que les conséquences éventuelles de la non-fourniture de ces données.

1132. Notons qu'en matière d'assurance, « l'assureur doit obligatoirement fournir une fiche d'information sur le prix et les garanties avant la conclusion du contrat. », ainsi qu'un exemplaire du projet de contrat, *« de ses pièces annexes ou une notice d'information sur le contrat qui décrit précisément les garanties assorties des exclusions, ainsi que les obligations de l'assuré »*[767].

1133. En ce qui concerne le moment de la délivrance de l'information, lorsque le traitement repose sur l'utilisation d'un objet connecté, en fonction des modalités d'utilisation du dispositif et de l'utilisation qui est faite des données, l'information peut, ne pas être délivrée dans une même unité de temps ou selon une même forme. Habituellement, il est de coutume, que le cocontractant soit informé concomitamment à la souscription du contrat. Pour que le cocontractant consente valablement à l'utilisation de ses données dans le cadre d'une action de promotion de l'activité physique, cela suppose qu'il soit parfaitement informé de la nature des données collectées, des opérations de traitements qui sont réalisées ainsi que de l'usage qui en est fait par le fournisseur. Notons que nous n'envisageons pas exclusivement ce sujet

[767] Code des assurances (C. ass.) article (art.) L. 112-2.

vis-à-vis de l'assuré et de l'assureur, la problématique peut également concerner tout fournisseur proposant des services reposant sur l'utilisation d'objets connectés.

1134. Les informations peuvent être complétées lors de la collecte des données. Dans ce cadre il n'est pas inenvisageable de recourir aux technologies pour proposer, le cas échéant, des modifications du contrat initial aux souscripteurs ou compléter l'information préalablement à la collecte de la donnée comme le permet l'article 13 Cette faculté démontre l'intérêt des nouvelles technologies dans le secteur du droit et l'aspect innovant des *blockchain* dans le cadre de smart contrats.

1135. Il en résulte que l'information peut, du fait de l'usage des nouvelles technologies, être délivrée en deux temps, lors de la souscription d'un contrat, quel qu'il soit, qu'il s'agisse de couverture assurantielle ou de prestation de toute autre forme de service et à distance, préalablement à la collecte de données mais aussi, au moment où les informations sont obtenues, article 13, 2) du Règlement.

1136. On peut ainsi imaginer dans le cadre de contrat aléatoire ou à exécution successive de proposer la fourniture de services à distance ou, le cas échéant, des évolutions du contrat souscrit en ayant recours à une condition suspensive permettant par exemple, de déclencher à distance la collecte de données ou l'information en temps réel en fonction de l'utilisation qui est faite, par l'utilisateur, du dispositif.

1137. Ainsi, une information générale peut-être réalisé sur l'utilisation du dispositif, les mesures de sécurité mises en œuvre, le cas échéant la durée de conservation et une information spécifique à chaque utilisation d'une nouvelle fonctionnalité. Cela peut également représenter un avantage en ce qui concerne des services dont le modèle économique repose sur une facturation à l'utilisation du service ou dans le cadre de programmes de préventions, y compris en santé publique, de la fourniture d'avantages en fonction de l'activité.

1138. En ce qui concerne l'obligation d'information de l'assuré, vis-à-vis de l'assureur, de nos jours, l'assuré est tenu, sur le fondement de l'article L. 113-2 du code des assurances de « répondre exactement aux questions posées par l'assureur dans le formulaire de déclaration du risque par lequel l'assureur l'interroge lors de la conclusion du contrat, sur les circonstances qui sont de nature à faire apprécier par l'assureur les risques qu'il prend en charge ». Il est également tenu de déclarer, en cours de contrat, « les circonstances nouvelles qui ont pour conséquence soit d'aggraver les risques, soit d'en créer de nouveaux et rendent de ce fait inexactes ou caduques les réponses faites à l'assureur ». Bien que la conclusion des contrats d'assurance ne soit pas conditionner, à ce jour, à l'utilisation de dispositifs connectés, en raison de son caractère facultatif, on peut légitimement s'interroger sur l'utilisation de tels objets dans l'appréciation du risque et surtout dans son évolution. Qu'elle pourrait être, dès à présent, dans notre droit positif, les conséquences de l'exploitation de données transmises par le dispositif connecté lorsque celles-ci démontrent une évolution du risque couvert par l'assureur et quelles en seraient les conséquences, pour l'assuré ?

1139. Devrait-on considérer que l'assureur est informé par l'utilisation du dispositif malgré que celui-ci soit actuellement exclusivement utilisé à des fins de prévention ? L'assuré devrait-il démontrer que l'assureur a détourné le traitement afin d'en obtenir des informations quant à l'évolution du risque couvert ?

1140. Répondre à ces questions n'est pas l'objet de nos travaux mais ces interrogations démontrent les défis que peut représenter aujourd'hui mais aussi dans un avenir proche, la circulation des données pour les droits et libertés de la personne.

1141. Il en résulte qu'il est important d'adopter une démarche prospective et de réglementer de tels traitements afin de ne pas les confier à la seule volonté des parties. Rappelons à cette fin la célèbre citation de Monsieur Henri Lacordaire « entre le fort et le faible, entre le riche et le

pauvre, entre le maître et le serviteur, c'est la liberté qui opprime et la loi qui affranchit ».

CONCLUSION DU CHAPITRE 1

1143. Si les dispositifs médicaux ainsi que l'utilisation de dispositif m-santé dans un cadre défini avec la participation d'un professionnel du soin, ne semble pas concrètement représenté de risque, il n'en est pas de même en ce qui concerne les autres situations.

1144. La santé personnalisée repose sur la licéité des traitements mis en œuvre par les fournisseurs d'application de bien être ou de m-santé. Lorsque les données traitées peuvent être qualifiées de données de santé, le traitement fait l'objet d'une interdiction de principe. Celle-ci ne peut être levée que si la personne y consent à moins qu'il n'existe une disposition contraire interdisant expressément la mise en œuvre d'un tel traitement uniquement sur le consentement de la personne.

1145. Les mineurs font l'objet de mesures de protection particulière en fonction de leur âge, afin de les préserver de toute atteinte à leur vie privée.

1146. Cependant, hormis les services payants, l'application accessible au grand public ne comporte pas nécessairement les moyens techniques permettant de contrôler l'âge de l'utilisateur.

1147. Le recours à ces dispositifs en matière assurantiel ne fait l'objet d'une interdiction exprès. Celle-ci résulte indirectement de l'interdiction d'adapter individuellement le montant de la cotisation de l'assuré. Cette causalité indirecte ne nous semble pas satisfaisante compte tenu du risque qui peut résulter de l'utilisation de ces données par une compagnie d'assurance

1148. Il conviendrait que le recours à de tels dispositifs dans le secteur de l'assurance fasse l'objet de dispositions spécifiques de natures

à définir où se place le curseur entre la disponibilité de la donnée de santé et la protection des droits de la personne.

CHAPITRE 2. UN REGIME DE PROTECTION A CONSOLIDER

1150. **De la fiction à la réalité.** CNIL décrie dans son cahier innovation et prospective de 2013,[768] la journée de Léa une adepte du *quantified self* qui évolue dans une compagnie prônant la transparence et le bien-être. Le personnage devient rapidement esclave de ses propres données physiologiques. Celles-ci étant partagées avec l'ensemble de ses collaborateurs Léa se trouve privée de tout libre arbitre. Cette fiction s'inspire du roman dystopique de Dave Eggers « The Circle ». Cette œuvre y décrit la disparition de l'intimité de la vie privée et de l'individualité au profit de la transparence et du conformisme.

1151. Pour autant, cette fiction est déjà une réalité, notamment pour les clients américains de la compagnie d'assurance John Hancock Financial qui leur propose de faire baisser leurs cotisations si ceux-ci s'engagent à faire régulièrement de l'exercice physique et à enregistrer leurs activités avec leurs bracelets[769]. Elle l'est également pour quelques assurés Français qui bénéficient d'avantages en nature en fonction de leur niveau d'activité. Cette fiction est également le quotidien de N. Felton, ancien salarie de la société Facebook qui pendant dix ans a de son plein gré entièrement quantifier sa vie afin d'accumulées et modélisées des informations sur son sommeil, son poids, ses performances sportives, etc. et analyser des séquences de sa vie afin de mieux les comprendre.

1152. **Des écarts entre le soin et le bien-être.** Si ces utilisations sont volontaires et pour le moment bénéfiques, ont entrevois aisément les

[768] CNIL, *Le corps, nouvel objet connecté, du quantified self à la m-santé : les nouveaux territoires de la mise en données du monde,* Cahier IP n°2, 13 octobre 2013.

[769] Elisa Chelle. « La complémentaire santé comportementale : un nouveau logiciel assurantiel ? ». RDSS 2018. p. 674.

dérives d'une démocratisation de la quantification dans une société où le recours à ces pratiques serait devenu la norme.

1153. Les données de santé traitées au moyen d'objets connectés en dehors du système de soin semblent être propices à générer l'objet d'un régime de protection incomplet qu'il convient d'analyser (Section 1) qui peut être amélioré en s'inspirant du droit de la santé (Section 2).

Section 1. Un régime de protection incomplet

1155. **Une protection contextuelle.** La qualification de donnée à caractère personnel relative à la santé emporte l'application de dispositions qui sont propres à certaines catégories de données qualifiées de sensibles. Ces dispositions figurent au sein du RGPD ainsi qu'au sein de la loi relative à l'informatique, aux fichiers et aux libertés, modifiées par la loi 2018-493 et sont communes à tout traitement de données de santé (Paragraphe 1). Toutefois, selon la situation dans laquelle la donnée a été collectée, d'autres dispositions, de droit national, qui sont plus protectrices, peuvent être inopérantes (Paragraphe 2).

1156. § 1. Une protection équivalente

1157. En ce qui concerne les dispositifs médicaux connectés au sens de l'article L. 5211-1 du Code de la santé publique, leur utilisation s'inscrivant dans un parcours de soins, les données captées ou collectées au moyen de ces dispositifs ne font pas l'objet de dispositions particulières. Elles font partie intégrantes des données à caractère personnel relatives à la santé produites par le système de santé. Par conséquent, elles sont alternativement traitées sur le fondement des dispositions de l'article 9 paragraphe 2, c), h) et i) du Règlement n°2016/679. Leur traitement est strictement réglementé par le RGPD ainsi que le droit national français qui, à l'exception des dispositions de la loi de 1978 modifiée[770], se retrouve principalement codifiées au sein du Code de la santé publique, du Code de l'action sociale et des familles mais aussi du Code de la sécurité sociale.

[770] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles.

1158. À titre d'exemple, l'hébergement des données de santé, *« recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social »*. Lorsque ces données sont hébergées, « pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même », elles doivent être confiées à un hébergeur certifié dans les conditions définies l'article L. 1111-8 du Code de la santé publique, ainsi qu'aux articles R. 1111-9 à R. 1111-11 du même code. À titre principal, il s'agit pour l'hébergeur (en dehors des services d'archivage électronique) de l'obligation d'être agréé[771] ou certifié dans les conditions définies par l'ordonnance n°2017-27 et de l'article L. 1111-8 précité. Rappelons que la certification remplace l'agrément aujourd'hui délivré par le ministère de la Santé dans les conditions définies par le décret n°2006-6 du 4 janvier 2006.

1159. **La santé mobile ou m-santé**. Les traitements mis en œuvre, lors de l'utilisation d'application de santé mobile, dès lors qu'elle capte et conserve ces données et propose des fonctionnalités permettant d'assurer un service, à distance, à son utilisateur qui peut être suivi par un professionnel ou sous surveillance médicale ou qu'elle comporte une connexion extérieure notamment afin de sauvegarder les données dans le cloud[772] est soumis au RGPD ainsi que la loi de 1978 modifiée[773]. Lorsque les données relatives à la santé, sont captées et/ou collectées au moyen des applications et objets connectés dans le cadre d'une activité sanitaire, elles sont soumises aux dispositions applicables aux données à caractère

[771] Les agréments pour l'hébergement de données de santé sur support électronique pris sur le fondement de l'article L. 1111-8 avant l'entrée en vigueur de l'ordonnance n°2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel continuent à produire leurs effets jusqu'à leur terme.

[772] « Applications mobiles en santé et protection des données personnelles : Les questions à se poser », 17 aout 2018, www.cnil.fr , consulté le 05.10.2018.

[773] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles.

personnel relatives à la santé qui sont traitée sur le fondement de l'article 9 paragraphe 2, c), h), i) du Règlement n°2016/679. Ainsi, lorsqu'elles sont collectées *« à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social »*[774], ces données sont également hébergées de manière externalisée selon les dispositions protectrices de l'hébergement de données de santé.

1160. Toutefois, dans la pratique, les applications de m-santé constituent des applications sans mesures particulières et les données peuvent être en plus d'être partagées entre le professionnel et le patient auprès de tiers. Dans ce cadre, lorsque les données sont conservées au sein du système d'information de l'établissement ou du cabinet, externalisée elles le sont généralement dans le cadre d'un environnement hébergeur de données de santé. *A contrario,* lorsque le traitement est réalisé dans un cadre privé le recours à hébergeur de données de santé n'est pas obligatoire si les données ne sont pas traitées dans les conditions définies à l'article L. 1110-8 du Code de la santé publique.

1161. Le consentement du patient au traitement des données de santé le concernant n'est qu'une dérogation parmi d'autres au principe d'interdiction de traitement de ces données sensibles. Il est discutable de considérer, d'une manière théorique, que les données traitées à des fins de soins, dans le cadre d'une activité sanitaire, sont mieux protégées que les données traitées à des fins de bien-être puisque, le traitement de données par les acteurs de santé, ne nécessite pas inévitablement le consentement du patient. Par ailleurs, en ce qui concerne les données recueillies ou produites lors d'activités de soins, le patient ne décide pas véritablement du traitement des données de santé le concernant. Il dispose toutefois d'un droit d'accès aux données de santé le concernant ainsi que le droit d'en obtenir une copie.[775]

---

[774] C. santé publ, art. L. 1111-8.

[775] C. santé publ. art. L. 1111-7.

1162. *A contrario,* lorsque les données sont traitées à des fins de bien être, le consentement de l'utilisateur, lui confère le droit *« de décider et de contrôler les usages qui sont faits des données à caractère personnel [le] concernant »*[776]. Par ailleurs, il existe des applications qui permettent aux utilisateurs de gérer finement l'utilisation qui est faite de leur donnée à caractère personnel.

1163. Aussi, la CNIL a identifié trois facteurs susceptibles de conditionner le caractère sensible de ces données : *« le contexte de production d'abord (médical ou non) ; ensuite les informations objectives véhiculées par la donnée brute ; enfin la destination de ces données »*. Or, selon la CNIL, « ces contours flous constituent une véritable difficulté dans l'appréhension du *quantified self* au regard des exigences de la protection des données personnelles », puisque « les contraintes attachées en France et dans l'Union européenne à la qualification de donnée de santé peuvent créer un risque de "sur-régulation" ou de "régulation excessive" pour certains outils dont les finalités et les traitements demeurent pour l'heure bénins ou à l'inverse générer une trop faible régulation à l'égard d'outils susceptibles, dans certaines conditions, de se révéler dangereux pour leurs utilisateurs compte tenu des données collectées ou de l'usage qui en sera fait » (CNIL, Cahiers IP Innovation & Prospective, no 2, mai 2014).

[776] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. Article (art.) 54.

1164.

§ 2. Une protection insuffisante

1165. **L'inapplicabilité d'un pan du droit**. Les données à caractère personnel relatives à la santé qui sont traitées en dehors du système de santé et sous la condition préalable d'obtenir le consentement de la personne ne font pas l'objet d'une réglementation aussi protectrice que les données produites par le système de santé. En conséquence, elles ne relèvent pas des dispositions du Code de la santé publique qui protègent la personne tout au long de son parcours de santé mais des obligations découlant du Règlement 2016/67. Ainsi, tout un champ du droit à la protection des données mais aussi des personnes est inopérant. S'agissant de données sensibles, directement ou indirectement identifiantes, elles sont cependant régies par les dispositions du Règlement 2016/67. Nous l'avons précédemment évoqué, selon le contexte, ces traitements vont pouvoir constituer à l'égard de l'utilisateur, des traitements de données à caractère personnel mis en œuvre par une personne physique dans le cadre d'une activité strictement personnelle ou domestique. Par conséquent, ils ne vont pas relever du champ d'application *ratione materiae* du Règlement.

1166. *A contrario,* toute externalisation des données ou toute intervention extérieure sur les fichiers fait entrer le traitement dans le champ d'application *ratione materiae* du Règlement. Par conséquent, le fournisseur du dispositif connecté, n'est pas dispenser de ses obligations en matière de sécurité, rappelons que ces obligations comprennent les exigences de sécurité issues du Règlement mais excluent les dispositions issues du Code de la santé publique. À titre d'exemple, le fournisseur échappera aux éléments de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), il se trouvera toutefois dans l'obligation de respecter les exigences de sécurité issues du Règlement qui constituent, par ailleurs l'état de l'art. Il sera également dans l'obligation de prévoir dès la conception du traitement la mise en œuvre de mesures

juridiques, logiques et organisationnelles permettant aux utilisateurs d'exercer leurs droits dans les conditions définies au Règlement[777].

1167. *A contrario*, « les professionnels de santé, 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 Code de la santé publique» se trouvent dans l'obligation en raison des dispositions de l'article L. 1110-4-1 du Code de la santé publique, d'utiliser des systèmes d'information conformes aux éléments de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)[778].

1168. Le responsable de traitement mettant en œuvre, en dehors des conditions susmentionnées, des traitements de données à caractère personnel poursuivant une finalité ayant un lien avec la santé ou le bien-être[779], ne sont pas concerné par ses dispositions mais se trouvent toutefois dans l'obligation de respecter les exigences de sécurité issues du Règlement qui constituent, par ailleurs l'état de l'art.

1169. De la sorte, ils *« devraient […] garantir une sécurité et une confidentialité appropriées, y compris pour prévenir l'accès non*

[777] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 2016, préc. §, 35, Préambule.

[778] Afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, les professionnels de santé, 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 par le groupement d'intérêt public mentionné à l'article L. 1111-24. Ces référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés.

[779] Il s'agit uniquement des traitements de données directement ou indirectement identifiantes, poursuivant une finalité de bien être, qui sont susceptibles d'apporter une information sur l'état de santé de la personne.

autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement. »[780]

1170. De la même manière, ces responsables de traitements proposent des services composés de fonctionnalités qui sont, dans une certaine mesure, librement accessibles et d'autres qui sont susceptibles d'être activées après le paiement d'un droit d'usage. Ainsi, tout citoyen d'un état membre de l'Union européenne, pouvant télécharger ces applications ces traitements, sont *de facto* réalisés à grande échelle et concernent des données sensibles qui exigent un suivi régulier et systématique des personnes concernées[781]. Par conséquent, ceux-ci requièrent la désignation d'un délégué à la protection des données qui constituent une garantie supplémentaire vis-à-vis de la protection de ces données et de l'effectivité des droits de la personne.

1171. Enfin, les dispositions de l'article 83 du Règlement 2016/679 ainsi que celles du Code pénal, relatives aux atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques ainsi que les atteintes aux systèmes de traitement automatisé de données ont également vocation à s'appliquer. En ce qui concerne, le secret professionnel, la situation est différente, le responsable de traitement ainsi que les membres de son personnel, n'étant pas dépositaire, par état ou par profession ou encore en raison d'une fonction ou d'une mission temporaire, d'une information à caractère secret, toute révélation qui serait réalisée à partir d'une ou de plusieurs informations dont ils auraient eu connaissance dans l'exercice de leur fonction, ne pourrait être sanctionnée sur le fondement de l'article 226-13 du Code pénal.

1172. Cependant, l'intimité de la vie privée, n'est pas pour autant dépourvue de toute protection, la confidentialité entendu dans son acceptation technique doit, concernant ces traitements, être assurée a priori

[780] Règl. (UE). PE et Cons. 2016/679, 27 avr. 2016, préc. art. 25.

[781] Règl. (UE). PE et Cons. 2016/679, 27 avr. 2016, préc. art. 37 §1, b), c).

par la mise en œuvre de mesures de sécurité, organisationnelles, physiques, logiques et juridiques appropriées[782]. Par ailleurs, la divulgation non consentie, des données recueillies lors de la mise en œuvre de ces traitements, n'échappe pas à toute sanction pénale, dès lors qu'elle a pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée. Le responsable de traitement ainsi que toute personne ayant concouru à la mise en œuvre de ces traitements, peut se voir condamné à une peine délictuelle y compris lorsque l'infraction a été commise par imprudence ou négligence[783]. Enfin le préjudice résultant de l 'atteinte à l'intimité de la personne en raison de la divulgation d'une l'information ou d'une donnée sensible peut également faire l'objet d'une réparation, soit, en raison d'une responsabilité délictuelle ou quasi-délictuelle[784], lorsqu'il s'agit d'un tiers, soit par la mise en œuvre du tryptique classique : fait dommageable, dommage, lien de causalité en raison de l'inexécution ou de la mauvaise exécution, par le responsable de traitement, d'une obligation contractuelle[785] de confidentialité.

1173. Bien que les données physiologiques collectées dans une démarche de quantification constituent désormais expressément des données de santé, leur hébergement ne doit pas nécessairement être réalisé auprès d'un hébergeur de donnée de santé certifié. Le critère déterminant pour l'application des dispositions relatives à l'hébergement de données à caractère personnel relatives à la santé est le contexte dans lequel ont été recueillies les données confiées. Par conséquent, les données produites par un dispositif connecté, dans le cadre d'une activité de prévention, de diagnostic ou de suivi social et médico-social, vont nécessairement être

[782] v. supra n° 356 et svt.

[783] C. pén., art. 226-22.

[784] C. civ. art. 1241 – ancien art. 1241, anc. art. 1383.

[785] Bien qu'il s'agisse, le plus souvent de contrat d'adhésion, le responsable de traitement peut, au sein des conditions générales ou, le cas échéant, au sein des confitions particulières d'utilisation d'un dispositif connecté, d'une application ou d'un service, stipuler une obligation de confidentialité en faveur des deux parties.

conservées par l'établissement le professionnel de santé producteur ou le patient ou être confiées à un hébergeur certifié.

1174. *A contrario*, les mêmes données, lorsqu'elles sont renseignées par l'individu lui-même ou qu'elles sont captée et transmises par un objet connecté puis recueillies au moyen de l'application qui lui est associée sans que cette activité soit réalisée dans le cadre de l'une des activités décrite à l'article précité et/ou s'inscrivant dans une prise en charge traditionnelle par les acteurs du système de santé, l'hébergement peut être réalisé dans des conditions ordinaires [786]. L'hébergeur des données devra toutefois respecter les exigences imposées par le Règlement à l'égard des données à caractère personnel relatives à la santé particulièrement en ce qui concerne, le niveau de sécurité des données et l'exercice des droits de la personne.

1175. Il en résulte que ces données ne sont pas protégées dans des conditions équivalentes. Pour autant, la qualité technique des applications et objets connectés de bien-être est propre à chaque fabricant et fournisseur de services. Par conséquent, les données captées par ces dispositifs peuvent s'avérer aussi précises que les données produites traditionnellement par le système de soin en raison des progrès réalisés dans la sensibilité des capteurs ainsi que dans la précision des algorithmes d'interprétation. Par ailleurs, ces données peuvent être plus sensibles que les données traitées dans le cadre d'une activité sanitaire. En effet, elles sont captées ou collectées de manière continue auprès ou à partir de la personne concernée et portent sur de multiples paramètres.

1176. Il peut s'agir, pour les fonctions de base, de l'alimentation détaillée, de la qualité du sommeil, de la fréquence cardiaque, du nombre de calories consommées, du nombre de kilomètres parcourus ou de pas réalisés voir également, de la concentration en oxygène dans le sang.

[786] Ces informations sont disponibles sur le site de la Cnil, accessible à l'adresse suivante : www.cnil.fr

Notons que désormais avec le développement des applications de domotique et la multiplication des capteurs au sein de l'habitat, ces informations peuvent être complétées par des données relatives à l'environnement de la personne, à titre d'exemple, en ce qui concerne la qualité de l'air. Ainsi, ces fichiers constituent des sources d'informations riches et extraordinairement précises sur les personnes concernées, leur l'interconnexion ou le croisement des données qui les composes peut conduire à la production d'un soi numérique, c'est-à-dire à une véritable emprunte du corps à l'image d'une trace ADN. Par conséquent, leur mauvaise utilisation est susceptible de porter atteintes aux droits et libertés des personnes.

1177. Notons qu'en matière d'hébergement, ces données peuvent être conservées en dehors de l'Union Européenne, c'est également le cas en ce qui concerne les données de santé entrant dans le champ des dispositions de l'article L. 1111-8 du Code de la santé publique. Toutefois bien que l'hébergeur soit en qualité de responsable de traitement, cotraitant ou de sous-traitant, tenu de respecter les dispositions applicables aux données à caractère personnel y compris celles relatives aux données de santé[787], la protection apportée par les dispositions du Code de la santé publique en matière d'hébergement de données de santé, s'avèrent présenter des garanties que nous estimons supérieures[788].

1178. **Des données susceptibles de faire l'objet d'une exploitation commerciale.** La problématique de la commercialisation des

[787] Figure parmi ces obligations, *« la mise en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque »*, art. 30 à 32 du RGPD, la désignation d'un délégué à la protection des données, art. 37 du RGPD, ainsi que le respect des règles relatives au transfert de données dans un Etat situé hors de l'Union européenne (UE), art. 44 du RGPD.

[788] v. supra n°429 et svt.

données conduit inévitablement à remettre en question *« l'opposition prétendue des droits de la personnalité au droit de propriété »*[789].

> *« Les activités humaines s'emploient de plus en plus à tirer un profit commercial de tout recueil d'informations, […] Non seulement les données médicales personnelles n'échappent pas à cette valorisation économique mais elles sont au contraire l'objet d'une "marchandisation" spécialement attractive sous couvert de l'intérêt du patient, du médecin et de la collectivité. »*[790]

1179. D'un côté, le bien est défini comme *« toute entité identifiable et isolable, pourvue d'utilités et objet d'un rapport d'exclusivité »*. Or, *« la personnalité désigne les éléments originaux de la personne humaine qui, par ce qu'ils sont utiles et rares, appellent l'établissement d'une relation exclusive »*. La personnalité, et ses attributs, apparaissent donc, à raison de leur originalité, comme des biens[791].

1180. Ainsi, à l'aune du droit à l'image qui a également trait à la notion d'identification et qui admet une valeur commerciale[792] à l'image sans toutefois se départir d'une approche personnaliste, nous ne considérons pas que la qualification de données à caractère personnel relative à la santé, élude toute approche fondé sur la valeur monétaire de la donnée.

---

[789] F. Zenati-Castaing, T. Revet. "Manuel de droit des personnes", Puf Droit, oct. 2006. p. 215.

[790] Pr L. Dusserre. *« La commercialisation des informations médicales est-elle « déontologiquement correcte » ? »*, Cnom. 29 juin 2000.

[791] F. Zenati-Castaing, T. Revet, *Les biens*, PUF, coll. « Droit fondamental », 3e éd. 2008 ;F. Zenati Castaing, T. Revet, *Manuel de droit des personnes*, PUF, coll. *« Droit fondamental »*, 2006, -Adde. JC. Saint Pau (sous la dir.) *« Droit de la personnalité »*. LexisNexis. 2013, p. 713.

[792] *« Il est en effet pleinement admis, en jurisprudence, qu'une personne puisse autoriser, contre de l'argent, l'usage de son image, de sa voix, de ses informations personnelles. Il est encore constant qu'elle peut obtenir en justice des dommages-intérêts quand une atteinte est portée aux mêmes attributs »*. F. Zenati-Castaing, T. Revet, *Manuel de droit des personnes*, PUF, coll. *« Droit fondamental »*, 2006, p. 216.

1181. *« L'opposition prétendue des droits de la personnalité au droit de la propriété est artificielle, car les droits de la personnalité consistent réserver à leur titulaire les attributs de la personnalité et, contrairement à une idée reçue, la propriété n'est pas un droit plus patrimonial que ne le sont es droits de la personnalité. L'utilisation par une partie de a doctrine et de la pratique des notions de biens et de propriété n'est donc pas techniquement incorrecte. Elle gagnerait à être intégrée dans la théorie des droits de la personnalité plutôt que de lui être opposée. »*

1182. En ce sens, les données de santé n'échappent pas toute valorisation et peuvent se trouver dans le cadre d'activités illicites, commercialisées sur le dark web[793] et représente par ailleurs une valeur attractive. Ainsi, des bases de données de quelques dizaines de milliers à quelques millions de patients se sont vues proposées à la vente[794] à des prix substantiels.

1183. Au-delà de l'analyse de la nature du régime de protection, cette question n'est pas dépourvue d'intérêt en ce qui concerne la circulation de la donnée puisque dénier toute valeur mercantile et conséquemment toute coloration patrimoniale à la donnée peut constituer selon la situation un vecteur ou un frein à son utilisation.

1184. Concernant les données produites, par le système de santé, celles-ci sont protégées expressément par les dispositions des articles L. 1110-4 du Code de la santé publique paragraphe 1 alinéa 1 et 2 et 226-13 du code pénal ainsi que au titre du droit au respect de la vie privée et du

---

[793] *« Le dark web (« web sombre ») est une portion de la Toile à laquelle on accède par un logiciel. Une fois arrivé là, sites et autres services sont consultables à l'aide d'un navigateur, comme pour le web officiel. »* The conversation *« Le dark web, qu'est-ce que c'est ? »,* 28 sept. 2015, disponible sur le site www.theconversation.com, dernière consultation le 06. Oct. 2018.

[794] Bfm, *« Les données de millions d'assurés médicaux en vente sur le Dark Web »*, 28 juin 2016, disponible sur le site www. hightech.bfmtv.com, dernière consultation le 06 oct. 2018.

secret qui empêchent toute commercialisation des données à l'initiative des professionnels et institutions du soin. La loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie introduit, quant à elle, au paragraphe VII de l'article L. 1111-8 du Code de la santé publique, l'interdiction de céder, à titre onéreux, les données de santé directement ou indirectement identifiantes, y compris avec l'accord de la personne concernée sous peine des sanctions prévues à l'article 226-21 du Code pénal. Rappelons qu'en matière de protection des données à caractère personnel relatives à la santé, le RGPD, *« s'inscrit dans le cadre de la théorie des droits de la personnalité qu'elle contribue à faire progresser »*[795]. Ainsi, il serait raisonnable de penser que cette interdiction, qui figure au sein de la section relative aux principes généraux du livre premier, sur la protection des personnes en matière de santé, soit de portée générale. Cette interdiction a été inopportunément intégrée au sein des dispositions relatives à l'hébergement de données à caractère personnel relatives à la santé. Elle n'a, par conséquent, pas vocation à interdire de manière générale, l'aliénation onéreuse des données de santé directement ou indirectement identifiantes. Celles-ci concernent uniquement les hébergeurs de données de santé qui se trouvent dans l'obligation de restituer, à la fin de l'hébergement, les données aux personnes qui les leur ont confiées, sans en garder de copie.

1185. Qu'en est-il des données à caractère personnel relatives à la santé qui sont collectées sur le consentement de la personne concernée par le traitement ?

1186. La Directive de 1995 prévoyait initialement, que la CNIL se livre à un contrôle préalable des traitements de données à caractère personnel. À ce titre, la Commission analysait la finalité des traitements mis en œuvre sur le fondement du consentement de la personne. Elle se montrait peu encline à autoriser un traitement consistant en l'exploitation

[795] A. LUCAS, Le droit de l'informatique, Puf, coll. « Thémis Droit », Paris, 1987, n°304

à des fins commerciales de données de santé. Le RGPD, substitut au dispositif de contrôle préalable, le principe d'accountability. Il s'agit de l'obligation, pour les responsables de traitement, de mettre en œuvre des mécanismes et des procédures internes permettant d'en démontrer le respect. Il en résulte que la CNIL n'a plus compétence pour apprécier et contrôler, a priori, de la finalité du traitement et d'en autoriser ou non la mise en œuvre.

1187. De ce fait, en l'absence de contrôle préalable, il ne paraît plus inconcevable que des données physiologiques qui ont été originellement traitées à partir du consentement de la personne à des fins de bien-être ou de quantification[796], se trouvent désormais exploitées, pour des finalités mercantiles. La condition nécessaire est déterminante consistant en l'information préalable de la personne concernée, et son assentiment à l'égard de la réutilisation escomptée.

1188. Nous l'avons précédemment précisé, les données physiologiques, faisant l'objet d'un traitement à des fins de bien-être ou de quantification de soi, constituent des données à caractère personnel relatives à la santé dont le traitement a pour condition de licéité le consentement de la personne. Ce consentement est donné dans le cadre d'une finalité déterminée. La Directive de 1995 exigeait déjà que les finalités du traitement soient explicites, légitimes et déterminées lors de la collecte des données. De cette manière, les finalités des traitements ultérieurs à la collecte ne pouvaient être incompatibles avec les finalités spécifiées à l'origine »[797]. Le Règlement général exige désormais du responsable du traitement que « la personne concernée [ait] consenti au traitement de ses données à caractère personnel pour une ou plusieurs

[796] Les nouvelles frontières de la vie privée. Droits de la personnalité. Protection des données personnelles, Forum Legipresse, 25 sept. 2008, Legicom, n° 43, 2009/2. Voir également, *« Etude 110 Droit des « nouveaux médias » : enjeux et limites »*, Le Lamy droit des médias et de la communication, déc. 2012.

[797] Directive 95/46/CE 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, considérant (cons.) 28.

finalités spécifiques »[798]. L'article 6 paragraphe 4 du Règlement permet toutefois au responsable de traitement, de traiter des données à caractère personnel pour d'autres finalités que celles pour lesquelles elles ont été initialement collectée, mais uniquement si le nouveau traitement est compatible avec la finalité initiale. Cependant, lorsque le traitement repose sur le consentement de la personne, que celle-ci est ou non, expressément consenti à l'utilisation ultérieure de ses données à caractère personnel, y compris sur le fondement de l'article 9 paragraphe 2, a), du Règlement, elle doit être informée de toute utilisation ultérieure de ses données.

1189. Il deviendrait donc envisageable que l'utilisation d'une application ou d'un service en ligne puisse prévoir ultérieurement la cession des données de ses utilisateurs en contrepartie d'une compensation financière. Pour autant, nous l'avons précisé, le Règlement 2016/679 semble tourner le dos à une protection par le prisme de la patrimonialité et incliné en faveur d'une conception personnaliste. Ainsi, sont attachés à l'autorisation consentie, les droits reconnus à la personne concernée par le traitement au titre du chapitre III du Règlement. Cette inclinaison n'exclue pas l'application des dispositions spécifiques à la protection des bases de données figurant aux articles L. 341-1 à L. 343-7 du Code de propriété intellectuelle. *« Cette protection qui organise une forme de monopole au profit du producteur conduit donc à une appropriation indirecte des données composant la base de données. Les données composant la base sont donc indirectement privatisées et protégées par le biais du droit sui generis des bases de données ou par le contrat qui permet leur commercialisation. »*[799].

[798] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, article (art.) 6, paragraphe (§1), a). JOUE n° L 119, 4 mai 2016.

[799] A. Mendoza-Caminade « Big data et données de santé : quelles régulations juridiques ? », Revue Lamy Droit de l'Immatériel, Nº 127, 1er juin 2016.

1190. Le propriétaire de la base ne peut toutefois s'opposer à l'exercice des droits et libertés de la personne définies au chapitre III du Règlement 2016/679. Par ailleurs, l'exercice de ce droit par la personne concernée par le traitement, ne saurait être analysé comme constituant une extraction qualitativement ou quantitativement substantielle du contenu de la base puisque celles-ci sont, usuellement, constituées par les données de milliers de patients. Nous pouvons considérer que sans être absolument hors du commerce ces données sont consubstantielles de la personne. La personne pouvant, à titre d'exemple, demander d'accéder à ses données[800] ou à ce que celles-ci soient rectifiées[801], il est par conséquent difficile d'envisager leur exploitation commerciale comme opérant un transfert de la pleine et entière propriété au profit du responsable du traitement ou de tiers acquéreurs. Cet acte pourrait toutefois s'apparenter à la reconnaissance d'un droit d'usage, à une forme d'usufruit, ou s'agissant, le plus souvent *« de données en réseau afférentes à plusieurs individus, devrait plutôt être regardées comme un "bien commun" »*[802] au sens ou l'entend, D. Bourcier ou encore J. Cohen[823].

1191. Le traitement reposant sur le consentement, les acceptations successives de procéder à une exploitation commerciale des données interroge sur la capacité des responsables de traitement à démontrer que la personne à bien été informée de l'identité des acquéreurs successifs ainsi que des diverses exploitations commerciales projetée et y a consentie [803] . Eu égard aux technologies contemporaines, il est

[800] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, article (art.) 15.

[801] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, article (art.) 16.

[802] D. Bourcier, P. de Filippi. « Vers un droit collectif sur les données de santé ». RDSS 2018. p. 444. 823 J. E. Cohen, Turning Privacy Inside Out. Theoretical Inquiries in Law 20.1 (2019 Forthcoming).

[803] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, article (art.) 7, paragraphe (§1).

concevable de parvenir à cette démonstration en ayant recours au *blockchain*. Pour mémoire, le *blockchain* ou chaine de blocs *« permet de stocker et de transmettre des informations de manière transparente et sécurisée en ayant recours à la cryptographie asymétrique et sans l'intervention d'un tiers de confiance »*[804]. Ce dispositif s'apparente à une écriture comptable d'opérations numériques ou à un registre public distribué et anonyme. Il permet de conserver de manière intègre et opposable, l'historique des opérations réalisées auprès des parties au contrat et rend par conséquent vraisemblable la commercialisation des données de santé produites en dehors du système de soin.

[804] C. Jay, *le risque sante et la souscription d'assurance du crédit*. Thèse. Nancy. 2017, p. 157. -Adde. JDN, *« Blockchain : définition et application de la techno derrière le bitcoin »*, 14 sept. 2018, disponible sur le site www.journaldunet.com

Section 2. Un régime de de protection à améliorer

§ 1. Des détournements identifiés

1193. **Le détournement illicite de finalité.** Avant de procéder à la collecte de données à caractère personnel, le responsable de traitement, doit définir précisément la finalité du traitement et à partir de celle-ci, les données qui vont être collectées pour parvenir à la réalisation de cette finalité. Dans le cas des applications nécessitant ou non l'utilisation d'un objet connecté, le consentement constitue le principal fondement juridique à la licéité du traitement. Les données à caractère personnel relatives à la santé vont être collectées dans le respect du principe de spécificité et de proportionnalité et traitées au moyen de dispositifs connectés, sur la base du consentement de la personne concernée. Elles sont conservées au sein de bases de données. Il ressort de l'avis du G29 du 27 février 2013[805], que les données collectées au moyen des applications ne respectent pas, pour la plupart, le principe de proportionnalité.

1194. Cette finalité devant être respectée pendant toute la durée du traitement, elles ne peuvent faire l'objet d'aucun traitement ultérieur dépassant le périmètre de la finalité initiale pour laquelle la personne a consentie[806]. Tout traitement réalisé à d'autre fin que celle portée à la connaissance de la personne concernée antérieurement à la collecte, constitue un détournement de finalité et peut être sanctionnée.

1195. **Le traitement ultérieur autorisé.** L'article 6 paragraphe du Règlement permet au responsable de traitement, de traiter des données à caractère personnel pour d'autres finalités que celles pour lesquelles elles

---

[805] GROUPE DE TRAVAIL DE L'ARTICLE 29 (G29) SUR LA PROTECTION DES DONNÉES,

« Risque en matière de protection des données des applications mobiles », 27 février 2013.

[806] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, article (art.) 5, paragraphe (§1), b). JOUE n° L 119, 4 mai 2016.

ont été initialement collectée, mais uniquement si le nouveau traitement est compatible avec la finalité initiale. Cependant, lorsque le traitement repose sur le consentement de la personne, que celle-ci est ou non, expressément consenti à l'utilisation ultérieure de ses données à caractère personnel, y compris sur le fondement de l'article 9 paragraphe 2, a), du Règlement, elle doit être informée de toute utilisation ultérieure de ses données.

1196. Dans la pratique, l'information n'est pas nécessairement délivrée à la personne et, lorsqu'elle l'est, elle ne respecte pas, le plus souvent, les conditions exigées par le Règlement[807]. L'approche consistant à inviter l'utilisateur à accepter une liste de conditions générales d'utilisation et/ou une politique de confidentialité, ne peut s'apparenter à un consentement spécifique. Les données collectées peuvent ainsi contribuer à la constitution de véritables *Big data* licites ou illicites, utilisées pour la revente de données pour la réalisation d'opérations de « profilage »[808] ou encore de marketing direct, ou toute autre pratique illicite ainsi qu'à la revente des données collectées.

> *« La sensibilité des données de santé tient aussi à ce que leur collecte et leur traitement sont susceptibles d'être conçus ou détournés à des fins commerciales ou d'élaboration de profils par et au service d'entreprises privées, notamment celles qui fournissent des services de banque ou d'assurance. »*[809]

1197. Le profilage a été défini au sein du Règlement afin de réglementer une pratique que ne l'était pas auparavant. Cette pratique

---

[807] Groupe de travail de l'article 29 sur la protection des données (G29), *« Risque en matière de protection des données des applications mobiles »*, 27 février 2013.

[808] Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 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, article (art) 4, 4). JOUE n° L 119, 4 mai 2016.

[809] Sauvé J-M. (2017) Santé et protection des données : Septièmes entretiens du Conseil d'Etat en droit social : Santé et protection des données. Conseil d'Etat, le 1er décembre 2017.

consistant en un traitement ayant pour objectif d'évaluer les aspects personnels relatifs à une personne physique pour analyser ou prédire, par exemple, l'état de santé de cette personne et notamment permettre de prendre des décisions la concernant. L'utilisation des données produites par les dispositifs connectés peut ainsi permettre ce type de pratique. Notons que si le profilage est licite son association à une prise de décision automatisée est prohibée.

1198. L'utilisation de données de santé à des fins de profilage constitue lorsqu'elle n'est pas réalisée dans les conditions précédemment décrites constitue dun détournement de finalité visée à l'article 226-21 du Code pénal puni d'une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende.

1199. *« 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, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende. »*

§ 2. Un risque de perte de la donnée

1200. **Des dispositions initialement insuffisantes**. L'objectif initial de la loi n°78-17 du 6 janvier 1978 était de rétablir, suite à l'échec du projet SAFARI, la confiance des citoyens français en l'informatique. Il s'agissait également, par ce moyen, de réglementer l'utilisation des outils informatiques et que leur généralisation au sein des administrations nationales afin que celui-ci se fasse dans le respect de l'identité humaine, des droits de l'homme, de la vie privée et des libertés individuelles ou

publiques[810]. De la sorte, il n'y avait aucune raison que la rédaction initiale de la loi relative à l'informatique, aux fichiers et aux libertés ne comporte quelconques dispositions relatives au champ d'application territorial.

1201. Suite à l'accord de Schengen[811] l'intégration économique et sociale résultant de l'établissement et du fonctionnement[812] du marché intérieur a entrainée « *une augmentation sensible des flux transfrontaliers de données à caractère personnel entre tous les acteurs de la vie économique et sociale des États membres* » [834]. Les progrès des technologies de l'information ont facilité considérablement le traitement et l'échange des données entre les entreprises établies dans les différents Etats membre de l'Union européenne ainsi qu'avec les entreprises situées en dehors du territoire des Etats membres de l'Union européenne. Toutefois, concomitamment au développement de la naissance et du développement des outils numériques, des règlementations nationales ont fleuries dans toute l'Europe. Ces dispositions nationales, législatives réglementaires et administratives, ont institués des niveaux de protection différents des droits et libertés des personnes, notamment du droit à la vie privée, à l'égard des traitements de données à caractère personnel. Ces disparités ont constituées un obstacle pouvant empêcher la transmission de ces données d'un territoire d'un Etat membre à celui d'un autre Etat membre[813]

[810] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 1.

[811] Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française

[812] Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes 834 Dir. (UE). PE et Cons. UE 1995/46, préc. considérant 5.

[813] CJUE, 1er oct. 2015, aff. C-230/14, Weltimmo c/ Autorité nationale de la vie privée et de la liberté,, RLDI 2015/120, no 386, obs. Costes. L., Comm. com. électr., no 12, déc. 2015, n°101, note Debet A 836 Traité instituant la Communauté économique européenne, Rome, le 25 mars 1957.

et ainsi rendu difficile voire impossible l'exercice d'une série d'activités économiques à l'échelle communautaire.

1202. **La libre circulation des marchandises, des personnes**[836], des services et des capitaux nécessite non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés[814]. Partant de ce principe, pour éliminer les obstacles à la circulation des données à caractère personnel, il est apparu évident que le niveau de protection des droits et libertés des personnes à l'égard du traitement de ces données devait être équivalent dans tous les États membres. Compte tenu en particulier de l'ampleur des divergences qui existaient entre les législations nationales applicables en la matière, cet objectif, fondamental pour le marché intérieur, ne pouvait être atteint par la seule action des États membres. La Commission européenne a, par conséquent, proposée aux membres des autres institutions législatives européennes de constituer un socle commun en coordonnant, au sein d'une Directive, la règlementation des Etats membres de l'Union européenne pour que les flux transfrontaliers de données à caractère personnel soient réglementés d'une manière cohérente et conforme à l'objectif du marché intérieur.

1203. La circulation des données à caractère personnel s'est développée non plus à l'échelle nationale mais à l'échelle de la Communauté Européenne, puis de l'Union Européenne et corrélativement à l'échelle du monde. Ont été institué, au moyen de la Directive de 1995, en plus des conditions relatives au champ d'application *ratione materiae*, des critères, alternatifs, relatifs à son champ d'application territorial. Cependant, *« en raison d'un accroissement toujours plus exponentiel de*

[814] Dir. (UE). PE et Cons. UE 1995/46, préc. considérant 3.

partage d'informations à l'international »[815] ces critères se sont vites révélés insuffisants menant la Cour de justice de l'Union européenne à se livrer à des interprétations plus précises[816].

1204. Les sociétés qui conçoivent, développent, commercialisent des moniteurs d'activité physique et autres objets et dispositifs connectés, opèrent à l'échelle internationale et transfèrent, en règle générale, les informations collectées sur le territoire de l'Union, vers des pays tiers. Ces pays dans lesquels les traitements sont opérés, peuvent bénéficier de règlementation moins protectrices des droits et libertés des personnes et, par conséquent, des données à caractère personnel et, de la confidentialité des informations. Prenant acte de ces circonstances et, afin de mieux appréhender la protection des données à caractère personnel au sein, comme à l'extérieur de l'Union européenne, lorsque des services et, par conséquent, des traitements sont mis en œuvre par des firmes multinationales sur le territoire d'un ou plusieurs des Etats membres à partir d'un Etat tiers ou en ayant recours à des sous-traitants situés sur le territoire d'un état tiers, les instances européennes ont profitées de la réforme relative à la protection des données personnelles pour faire évoluer les critères de son champ d'application territorial.

1205. Le champ d'application de la règlementation relative à la protection des données à caractère personnel a été étendu par les dispositions du Règlement 2016/679[817]. Il contient désormais un nouveau

---

[815] *« Quel est le champ d'application territorial de la réglementation relative à la protection des données personnelles ? »* Le Lamy droit immobilier 2015, étude 2932.

[816] CJUE, 13 mai 2014, aff. C-131/12, Google Spain SL, Google Inc. c/ Agence Espagnole de Protection des Données (AEPD) et Mario Costeja González

[817] Le Règlement conserve le critère de l'établissement mais sa portée est élargie puisqu'il ne concerne plus exclusivement le traitement de données à caractère personnel *« effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union »* lorsque le traitement considéré a lieu dans l'Union européenne. Il comprend dorénavant les traitements de données à caractère personnel réalisé dans le cadre des activités réalisées dans les mêmes conditions mais en dehors de l'Union européenne.

critère d'application extraterritorial consistant au ciblage de personnes concernées se trouvant sur le territoire de l'Union européenne. C'est ainsi que le RGPD, conserve la compétence de l'établissement et substitut au critère des moyens le critère de ciblage qui semble s'apparenter à la notion d'activité dirigée qui est employée en droit de la consommation par le Règlement (CE) n°593/2008[818]. Selon ce principe, les activités doivent être dirigées vers l'État membre du domicile du consommateur. C'est-à-dire que le fournisseur de service doit avoir manifesté sa volonté d'établir des relations commerciales avec les consommateurs d'un ou de plusieurs autres États membres, au nombre desquels figure celui sur le territoire duquel le consommateur a son domicile[819].

1206. Cette notion y est employée afin de renforcer la protection du consommateur dans un environnement électronique qui complexifie la détermination du lieu de conclusion du contrat. La Cour de justice de l'Union européenne dans le cadre de l'arrêt de 2010 adopte la méthode du faisceau d'indice pour déterminer si l'activité du commerçant est dirigée vers l'État membre du domicile du consommateur. Elle définit une liste non exhaustive d'indices comprenant *« la nature internationale de l'activité, […], l'utilisation d'une langue ou d'une monnaie autres que la langue ou la monnaie habituellement utilisées dans l'État membre dans lequel est établi le commerçant avec la possibilité de réserver et de confirmer la réservation dans cette autre langue, la mention de coordonnées téléphoniques avec l'indication d'un préfixe international, l'engagement de dépenses dans un service de référencement sur Internet afin de faciliter aux consommateurs domiciliés dans d'autres États membres l'accès au site du commerçant ou à celui de son intermédiaire,*

[818] Règl. (UE). PE et Cons. UE 593/2008, 17 juin 2008, sur la loi applicable aux obligations contractuelles (Rome I). Voir également, Règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale. Journal officiel n° L 012 du 16/01/2001 p. 0001 – 0023.

[819] CJUE, 7 déc. 2010, Peter Pammer contre Reederei Karl Schlüter GmbH & Co. KG et Hotel Alpenhof GesmbH contre Oliver Heller, Aff. jointes C-585/08 et C-144/09.

l'utilisation d'un nom de domaine de premier niveau autre que celui de l'État membre où le commerçant est établi et la mention d'une clientèle internationale composée de clients domiciliés dans différents États membres. »[820]

1207. Elle précise toutefois que *« la simple accessibilité du site Internet du commerçant ou de celui de l'intermédiaire dans l'État membre sur le territoire duquel le consommateur est domicilié est insuffisante. Il en va de même de la mention d'une adresse électronique ainsi que d'autres coordonnées ou de l'emploi d'une langue ou d'une monnaie qui sont la langue et/ou la monnaie habituellement utilisées dans l'État membre dans lequel le commerçant est établi. »*[821].

1208. Le Règlement n'emploie pas expressément cette notion mais il semble cependant en décrire l'application. De la sorte, lorsque le responsable du traitement ou un sous-traitant n'est pas établi d'ans l'Union européenne, le Règlement 2016/679 devra être appliqué si le traitement de données à caractère personnel est lié soit à l'offre de biens ou de services à des personnes se trouvant sur le territoire de l'Union, (qu'un paiement soit exigé ou non) ; soit le traitement a pour finalité le suivi du comportement de ces personnes au sein de l'Union européenne[822].

1209. La loi de n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel n'a pas modifié l'article 5 de la loi de 1978[823] relatif au champ d'application territorial. Bien que le Règlement puisse être invoqué directement par les particuliers, en raison du principe d'effet

[820] CJUE, 7 déc. 2010, C-585/08 et C-144/09. préc. considérant 93.

[821] CJUE, 7 déc. 2010, C-585/08 et C-144/09. préc. considérant 94.

[822] Règl. (UE). PE et Cons. 2016/679, 27 avr. 2016, préc. art. 3.

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

direct[824] il aurait été judicieux, pour des considérations de compréhension et de qualité de profiter de l'opportunité de la révision de 2018 pour reprendre les dispositions de son article 3. Il ne reste qu'à espérer que la future ordonnance opère cette modification[825].

1210. Il en résulte, que si le traitement est réalisé par une entreprise située en dehors du territoire de l'Union européenne, les dispositions du Règlement général sur la protection des données devront tout de même être appliquées. Pour autant, ce ne sont pas toutes les dispositions du Règlement qui auront vocation à s'appliquer.

1211. L'Etat concerné pourra, par ailleurs, disposer d'une règlementation moins protectrice des droits et libertés et plus particulièrement de la vie privée.

1212. La difficulté repose sur la situation particulière du transfert de données vers des entreprises situées sur le territoire d'états étrangers dont les règles de protection ne seraient pas jugées équivalentes.

1213. La Directive de 1995, pose un principe d'interdiction de transfert des données à caractère personnel, hors de l'Union européenne. Elle aménage cependant cinq dérogations. Ces modalités de transfert vers les pays tiers demeurent relativement complexes mobilisant, hormis dans

[824] CJCE, 5 février 1963, NV Algemene Transport- en Expeditie Onderneming van Gend & Loos contre Administration fiscale néerlandaise.

[825] La Loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, a modifié la loi Informatique et Libertés du 6 janvier 1978 afin d'exercer certaines des « marges de manœuvre nationales » autorisées par le Règlement général sur la protection des données. Certaines de ses dispositions demeurent formellement inchangées, et ne sont plus applicables. Les dispositions du Règlement 2016/679 se substituent à ces dispositions et devraient être retranscrites dans la loi de 1978 au moyen d'une ordonnance de réécriture afin de répondre à ce besoin de lisibilité du cadre juridique de la protection des données à caractère personne. Conseil d'Etat, avis sur le projet de loi d'adaptation au droit de l'Union européenne de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 7 déc. 2017.

de rares exceptions la Commission nationale de l'informatique et des libertés.

1214. Le Règlement général sur la protection des données, maintient la plupart de ces dérogations tout en les simplifiant. Il met fin au principe de l'interdiction, son article 44 est en effet rédigé en des termes positifs permettant le transfert à la condition que le niveau de protection des personnes physiques qu'il garantit ne soit pas compromis. Ces dispositions sont, par ailleurs, favorables à la circulation des données puisque celui-ci précise expressément que « les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale » peuvent être réalisés. Par ce moyen, des données à caractère personnel relatives à la santé, traitées dans le cadre de traitements poursuivant une finalité de bien-être ou pour toute autre finalité légitimée par le consentement de la personne peuvent être collectées sur le territoire de l'Union européenne et être transférées par les responsables de traitement auprès de sous-traitants ou d'autres de leurs établissements situés dans des Etats non membres de l'Union européenne. Le Règlement simplifie en la matière les dispositions relatives au transfert de données hors de l'Union européenne en supprimant drastiquement, les hypothèses dans lesquelles une autorisation préalable est obligatoire. Ce faisant, il réduit considérablement les délais de mise en œuvre des traitements de données à caractère personnel constitués sur des flux de données entre les Etats membres de l'Union européenne et les Etats tiers.

1215. **Le maintien des décisions d'adéquation par le Règlement.** Bien que la Directive de 1995 accorde un niveau de protection des données et des droits et libertés d'une valeur inférieur au Règlement, celui-ci maintient en son article 45 paragraphe 9, les décisions adoptées par la Commission prises en application de l'article 25, paragraphe 6 de la Directive 95/46/CE.

1216. Ces autorisations de transfert demeurent valables jusqu'à leur modification, remplacement ou abrogation par la Commission européenne. C'est-à-dire sur à un examen périodique, réalisé au moins tous les quatre ans[826] et/ou « *lorsque les informations disponibles révèlent, […] qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale n'assure plus un niveau de protection adéquat »*[827].

1217. Il en résulte que les transferts ou flux de données vers la Suisse, le

1218. Canada, l'Argentine, l'Uruguay, la Nouvelle-Zélande ou Israël demeurent valable[828.] Toutefois si dans ces quatre années, aucune mesure n'étaient prises, par ces Etats, pour procéder à la modification de leur législation afin d'y intégrer les évolutions apportées par le Règlement, la Commission européenne reviendrait sur ces décisions d'adéquation. Notons, en ce qui concerne le Royaume-Uni, malgré le *Brexit, l'Information Commissionner's Office* (ICO)[829] a précisé qu'un niveau de protection élevé des données à caractère personnel serait maintenu[830].

1219. **Le cas particulier du Privacy shield.** Les sociétés dont l'activité porte sur le « *quantified self* » ont, pour une partie d'entre elles, leur principal établissement à l'étranger et y traitent ou y font traiter les données collectées auprès des résidents Européens situés sur le territoire de l'Union européenne. C'est notamment le cas de la société d'origine

---

[826] Règl. (UE). PE et Cons. UE préc. art. 45 §3.

[827] Règl. (UE). PE et Cons. UE préc. art. 45 §5.

[828] La liste des pays proposant un niveau de protection adéquat est disponible à l'adresse suivante : https://linc.cnil.fr/fr/la-protection-des-donnees-dans-le-monde.

[829] L'ICO est un organisme public indépendant britannique, créé par le *« Data Protection Act 1998 »* transposant la Directive de 1995 pour protéger les données à caractère personnel et en promouvoir l'accès.

[830] ICO, *« The Information Commissioner's response to the House of Commons Justice Committee consultation on the implications of Brexit for the justice system », 10 nov. 2016.*

américaine, Fitbit qui commercialise des objets connectés (balances, bracelets et montres, etc.) sur le territoire de l'Union européenne. Depuis le 1er août 2016, le « ¨Privacy shield » est venu remplacer Depuis 1er août 2016, le « *Privacy shield* » ou bouclier de protection des données, remplace l'ancien dispositif de *« Safe Harbor »*. Il permet aux responsables de traitements et aux sous-traitants établis aux Etats-Unis soumis de transférer des données à caractère personnel, vers les Etats Unis, sans autorisation préalable de la CNIL. Il leur suffit de s'auto-certifier en s'enregistrent auprès de l'Administration du commerce international (ACI) de la Commission Fédérale du Commerce (FTC).

1220. Il est désormais possible de s'y référer pour transférer des données personnelles vers les USA, à condition que les entreprises destinataires des données se soient préalablement inscrites sur le registre tenu par l'administration américaine. Au-delà de cette obligation formelle, les entreprises américaines devront respecter les obligations et les garanties de fond prévues par le « *Privacy shield* ».

CONCLUSION DU CHAPITRE 2

1221. **Une protection juridique inégale.** Nous partageons, l'analyse réalisée par A. Mendoza-Caminade.[831] Les données recueillies dans le cadre du *quantified self* constituent des données pouvant relever de l'intime et aller jusqu'au champ du sensible. Toutefois ces données sont soumises à une protection juridique allégée. Ainsi, une brèche pourrait s'ouvrir au sein du droit de la protection des données à caractère personnel et *« de créer une voie médiane entre l'absence de régulation et la [régulation] actuellement issue de notre dispositif légal »* Cette faille résulte du contexte innovant dans lequel ces données sont traitées, de l'absence de réglementation spécifique en résultant et du fait que ces traitements aient pour fondement l'adhésion de la personne concernée qui va volontairement mettre ses données à disposition et consentir à leur captation[832]. Notons que les applications mobiles sont généralement peu transparentes sur le traitement qui est fait des données collectées et elles se révèlent très indiscrètes. En ce sens *« une enquête[833] du Financial Times a révélé que 9 des 20 applis de santé les plus utilisées transmettent des données à l'unes principales sociétés recueillant des informations sur l'utilisation que les gens font des téléphones portables[834] ». De la même manière, le Conseil national de l'Ordre des médecins (Cnom), dans le cadre de son livre blanc de janvier 2015 mentionnait que « la CNIL et 26 de ses homologues dans le monde l'ont mesuré, en mai 2014, lors d'une*

[831] 1. A. MENDOZA-CAMINADE, « Big data et données de santé : quelles régulations juridiques ? », Revue Lamy Droit de l'Immatériel, nº 127, 1er juin 2016.

[832] A. Mendoza-Caminade *« Big data et données de santé : quelles régulations juridiques ? »*, Revue Lamy Droit de l'Immatériel, Nº 127, 1er juin 2016.

[833] Financial Times, Health apps run into privacy snags, 1 sept. 2013

[834] Commission Européenne. *« Livre vert sur la santé mobile »*, 10 avril 2014.

opération commune d'audit en ligne simultané de plus de 1200 application mobiles, (…) Pour ce qui concerne la France, où 121 applications parmi les plus populaires ont été examinées, 15% d'entre elles ne fournissent aucune information sur le traitement des données collectées ; et lorsque l'information existe, la CNIL observe qu'elle est difficilement accessible, voire incompréhensible. (…) Aux États-Unis, lorsque la Fédéral Trade Commission a étudié, au printemps 2014, 12 applications de santé et de fitness mobiles, elle a constaté qu'elles diffusaient des données à pas moins de 76 entreprises tierces. (…) Or, les risques qui pèsent sur la confidentialité et la protection des données de santé des utilisateurs s'avèrent supérieures en situation de mobilité comparés à l'usage d'un ordinateur. (…) Or les développeurs ignorent le plus souvent l'existence d'obligations en matière de confidentialité et ont tendance à maximiser la collecte d'informations sans pertinence avec la finalité du service et en l'absence de consentement explicite de la part de l'utilisateur »[835].

1222. Compte tenu de ce qui précédent, il parait indispensable de mettre en œuvre une labélisation et un contrôle des dispositifs connectés utilisés à des fins de santé. La sécurité des données de santé nécessite également de sensibiliser les professionnels sur les risques qui pèsent sur la vie privée des personnes quant à l'utilisation de ces applications à des fins de soins.

1223. Il serait également souhaitable de confier à la CNIL, avec l'appui de l'ANSM et de la HAS, le contrôle des dispositifs connectés et leur labélisation.

1224. Enfin, il nous semble prioritaire, de sortir les dispositions du paragraphe VII de l'article L. 1111-8 afin de les intégrer dans un article spécifique au sein de la section 1 du Code de la santé publique sur les

[835] Cnom, *« Santé connectée : De la e-santé à la santé connectée »*, janvier 2015.

principes généraux afin d'exclure toute commercialisation des données produites par le système de santé.

1225. Ces dispositions devraient également être transcrites au sein de la loi relative à l'informatique, aux fichiers et aux libertés pour éviter que des données de santé collectées lors de traitement de bien-être ou de m-santé se trouvent ultérieurement commercialisées.

CONCLUSION DU TITRE II

1227. **L'activité de bien-être insuffisamment réglementée.** Au regard de nos développements précédents, nous constatons en ce qui concerne le traitement de données de santé au moyens de dispositifs connectés en dehors de toute prise en charge par le système de santé que les conditions de mises en œuvre des traitements ne sont pas de nature à garantir la protection des droits de la personne.

1228. L'utilisation des dispositifs connectés à des fins de bien – être pourrait s'analyser comme une activité de prévention. Cependant, il semble que cette analyse n'ait pas été retenue par le législateur. Ainsi, les données susceptibles de fournir des informations sur l'état de santé d'une personne se trouvent, le plus souvent, conservées dans le cloud sans que le responsable de traitement soit assujetti aux dispositions de l'article L. 1111-8 du Code de la santé publique. Il appert compte tenu des rapports et enquêtes précitées que les fournisseurs de ses applications ne respectent pas leur obligation d'information, de consentement, de sécurité.

1229. Ces données peuvent se retrouver traitées dans un pays tiers ne respectant pas les dispositions du Règlement et rendant de ce fait toute protection ineffective. Enfin, l'on voit poindre par les nouvelles incitations des compagnies d'assurance ou sociétés d'achat de données à caractère personnel, des pratiques qui si elles se banalisent vont amener une situation propice au refus de droits ou de prestations.

1230. Concernant les traitements fondés sur le consentement de la personne, le paragraphe II, a) de l'article 9 du règlement 2016/679 laisse toute latitude aux États-membres pour introduire les garde-fous nécessaires afin d'empêcher que des atteintes disproportionnées aux droits et libertés soient consenties par la personne, que celle-ci soit mal avisée ou

confrontée vis-à-vis du responsable du traitement à un rapport déséquilibré. Le recours à ces dispositions nous semble donc recommandé afin de réglementer et de contrôler concernant l'utilisation de ces dispositifs

CONCLUSION GENERALE

« Le cœur de l'informatique, ce sont des informations qui font l'objet de traitements automatiques et puissants et de diffusions potentiellement infinies.
Parmi ces informations, les données à caractère personnel sont devenues la matière première de l'économie numérique »[836]

1232. Ces informations, lorsqu'elles se rapportent à la santé d'une personne, sont au cœur de la relation de soin. Elles relèvent toutefois de l'intime. Le droit accorde à la personne, des droits sur les données la concernant et aux informations relatives à sa santé, une protection qui tient compte de leur spécificité. Ces dispositions protectrices ont été récemment revues par le droit de l'Union européenne ainsi que le droit national français afin d'assurer une conciliation plus adaptée entre le respect des droits de la personne, dont le droit à la vie privée et, la poursuite d'objectifs légitimes auxquels appartient la santé publique. Il résulte de ces réformes une réglementation propice à la circulation maitrisée de l'information au sein du système de santé qui admet l'échange, le partage, l'accès et le traitement de l'information indispensables à l'efficacité du système de santé et à sa pérennité[837].

1233. Ce nouveau cadre participe également, au moyen de l'autodétermination informationnelle, au développement du bien-être et de la santé personnalisée, contribuant à la prévention santé. En raison de la définition de la donnée de santé, le développement de ces usages, est désormais réalisé dans

[836] Sauvé J-M. (2017) Santé et protection des données : Septièmes entretiens du Conseil d'Etat en droit social : Santé et protection des données. Conseil d'Etat, le 1er décembre 2017.

[837] Etude annuelle du Conseil d'Etat, Numérique et droits fondamentaux, Annexe 3, La Documentation française, 2014, p. 367.

des conditions plus respectueuses des droits de la personne. Toutefois, en l'absence de dispositions nationales protectrices, un écart significatif subsiste entre la protection de l'information confiée au système de santé et la protection de la donnée captée par les acteurs économiques. Il appert qu'une modification de la réglementation est nécessaire afin d'encadrer ces nouveaux usages qui sont susceptibles d'engendrer de sérieuses atteintes aux droits de la personne.

Table des matières

Bibliographie

Ouvrages généraux : Traités manuels

1. G. ADREANI, R. BISMUTH, *Méthodologie de la recherche documentaire juridique*, Larcier, coll. Paradigme, 2014.

2. S. HENNION, *La responsabilité des travailleurs sociaux,* éd. ASH, 2e éd., 2012, p. 129.

3. A. LUCAS, *Le droit de l'informatique,* PUF, coll. Thémis, 1987.

4. F. RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles-Paris, Bruylant-LGDJ, 1990.

5. J.-P. ROSENCZVEIG, P. VERDIER, C. DAADOUCH, *Le secret professionnel en travail social et médico-social*, Santé Social, Dunod, 6e éd., 2016.

6. F. ROUVILLOIS, Libertés fondamentales, Flammarion, coll. *« Champs Université »*, 2e éd., 2016.

7. J.-C. SAINT PAU (dir.), *Droits de la personnalité,* LexisNexis, coll. Traités, 2013.

8. F. ZENATI-CASTAING, T. REVET, *Manuel de droit des personnes*, PUF, coll. Droit fondamental, 2006.

Ouvrages spéciaux : Thèses et monographies

1. A. NIETO**,** *La vie privée à l'épreuve de la relation de soin*. Thèse, Montpellier, 2017.

2. B. LAVERGNE, *Recherche sur la soft law en droit public français*, Thèse, Toulouse, 2011.

3. B. PY, *Le secret professionnel*, L'Harmattan, coll. « La justice au quotidien », Paris, 2005.

4. C. BRETON-RAHALI, *Le secret professionnel et l'action médico-sociale*, Thèse, Nancy, 2014.

5. C. JAY, le risque sante et la souscription d'assurance du crédit, Thèse, Nancy, 11 déc. 2017

6. M. CHAWKI, *Essai sur la notion de cybercriminalité*, IEHEI, 2006.

7. C. NLEND**.** La protection du mineur dans le cyber espace, Thèse, Picardie, 2007.

8. C. ZORN**,** *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé*, avant-propos B. Py, préf. I. de Lamberterie, PUN, 2010.

9. F. KUSZ, *Secret professionnel du médecin généraliste et maltraitance à enfants*, Thèse, Nancy, 2004.

10. G. RIPERT, *Le déclin du droit*, LGDJ, 1949.

11. I. COULIBALY, *La protection des données à caractère personnel dans le domaine de la recherche scientifique*, Thèse, Grenoble, 2011.

12. J. BRISSAUD, *Secret médical, Responsabilité pénale et civile du médecin*, Thèse, Bordeaux, 1912.

13. J. LE CLAINCHE, *L'adaptation du droit des données à caractère personnel aux communications électroniques*, Thèse, Montpellier, 2008.

14. J. LEONHARD, *Etude sur la pornographie pénalement prohibée*, Thèse, Nancy, 2011.

15. J. SAVATIER, *La profession libérale – Etude juridique et pratique*, LGDJ, 1947.

16. K. RENAUDIN, *Le spamming et le droit. Analyse critique et prospective de la protection juridique des « spammés »*, Thèse, Nancy, 2011.

17. L. ROUSVOAL*, L'infraction composite, essaie sur la complexité en droit pénal*, thèse Rennes I, 2011.

18. M. CAVALIER, *La propriété des données de santé*, Thèse, Lyon, 2016.

19. M. COUTURIER, *Pour une analyse du secret fonctionnel*, Thèse Lille, 2004.

20. M. GAY, F. CROTTA, *Les dessous des affaires judiciaires*, Max Milo éditions, coll. Essais-documents, 2014.

21. M. LAILA, *La télémédecine et les technologies d'assistance pour la prise en charge des personnes âgées fragiles à domicile et en institution : modélisation du besoin, de la prescription et du suivi*, Thèse, Grenoble, 2009.

22. N. ETIEN-GNOAN, *L'encadrement juridique de la gestion électronique des données médicales*, Thèse, Lille, 2014.

23. P. A. SAMUELSON, *L'Economique*, t. II, Armand Colin, Paris, 1973.

24. P-G. FONTOLLIET, *Systèmes de télécommunications*. Nouvelle édition, revue et augmentée, Vol. XVIII, Presses Polytechniques et Universitaires Romandes, 1996.

25. R. REZSOHAZY, *Sociologie des valeurs*, Armand Colin, 2006.

26. S. LANGARD, *Approche juridique de la télémédecine – Entre Droit commun et règles spécifiques*, Thèse, Nancy, 2012.

Articles, contributions, communications

1. R. BADINTER, *« Le droit au respect de la vie privée », JCP G* 1968, I, 2136.

2. R. BADINTER, *« Le droit et l'écoute électronique en droit français », Publications de la Faculté de droit et de sciences politiques et économiques d'Amiens*, n° 1, 1971-1972, p. 21.

3. B. BEIGNIER, *« Vie privée et vie publique », Arch. Phil. Droit*, n° 41, 1997, p. 163.

4. M. BENEJAT-GUERLIN, *« Que reste-t-il de la protection pénale du secret médical ? », AJ Pénal* 2017, p. 368.

5. X. BIOY, *« Le libre développement de la personnalité en droit constitutionnel : essai de comparaison (Allemagne, Espagne, France, Italie, Suisse) », RIDC*, janvier-mars 2003, p. 123.

6. 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* A. LECA (dir.), *Le secret médical*, CDSH , n° 15, LEH, 2012, pp. 51-66.

7. E. BROSSET, *« Consentement, santé et droit européen » in* A. LAUDE (dir.), *Consentement et santé*, Dalloz, coll. Thèmes et commentaires, 2014, p. 165.

8. J. CABANNES, *« Le droit au respect de la vie privée : fondement et quantum de la responsabilité du journaliste indiscret »,* conclusions sous CA Paris, 15 mai 1970, *D.* 1970, p. 466.

9. C. CASTETS-RENARD, *« Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data », Revue Lamy Droit de l'immatériel*, nº 108, 1er oct. 2004.

10. E. DROUARD, C. MAROLLA, « Anonymisation et internet des objets : une « première » du Conseil d'État qui fera date », *Lamy Droit du numérique*, n° 135, 1er mars.

11. L. DE ROQUEFEUIL, A. STUDER, E. NEUMANN, Y. MERLIERE, *« L'échantillon généraliste de bénéficiaires : représentativité, portée et limites », Pratiques et organisation des soins* 2009/3, p. 96.

12. M. DUPUIS, *« La vie privée à l'épreuve des réseaux sociaux »*, *Revue Lamy de droit civil* 2013, n° 102.

13. L. DUSSERRE, « La commercialisation des informations médicales est-elle « déontologiquement correcte » ? », CNOM, 29 juin 2000.

14. B. FAUVARQUE-COSSON, W. MAXWELL, « Protection des données personnelles », *D.* 2018, chron., p. 1033.

15. J. FRAYSSINET, « La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée en bois », *Legicom*, avril 2009, n° 42, p. 33.

16. S. GAMBARDELLA, « Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé », *RDSS* 2016, p. 271.

17. V. GAUTRON, « Fichiers de police », *Répertoire de droit pénal et de procédure pénale*, Dalloz, nov. 2017.

18. M. GOLDBERG, M. COEURET-PELLICER, C. RIBET, M. ZINS, « Cohortes épidémiologiques et bases de données d'origine administrative : Un rapprochement potentiellement fructueux », *médecine/sciences*, avril 2012, vol. 28, n° 4, p. 430.

19. M. GOLDBERG, M. ZINS, « Les cohortes généralistes en population – L'exemple des cohortes Gazel et Constance », *Bull. Acad. Natle Méd.*, 2013, 197, n° 2, p. 299.

20. J.-M. JOB, « La loi « Informatique et libertés » et les données de santé », *Revue Lamy Droit de l'immatériel*, janv. 2008, n° 34, p. 87.

21. D. LAROUSSERIE, « L'anonymat, un bien fragile », *Le Monde science et techno*, 7 avril 2014.

22. I. LAURENT-MERLE, « Le secret des données médicales et la protection de la vie privée : un secret de polichinelle ? », *D.* 2000, p. 521.

23. A. LEPAGE, « 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 », *Dr. pénal* 2005, chron. 5.

24. R. LINDON, « La presse et la vie privée », *JCP G* 1965, I, 1887.

25. N. MALLET-POUJOL, « Protection de la vie privée et des données personnelles », *Legamedia*, février 2004, p. 6.

26. A. MENDOZA-CAMINADE, « Big data et données de santé : quelles régulations juridiques ? », *Revue Lamy Droit de l'Immatériel*, nº 127, 1er juin 2016.

27. N. METALLINOS, « L'évolution du droit européen en matière de protection des données à caractère personnel et sa pénétration dans les droits nationaux : principes fondateurs et instruments de régulation », *L'Observateur de Bruxelles*, juillet 2013, n° 93, p. 8.

28. R. PELLET, « La protection des personnes à l'égard des traitements informatisés des données à caractère médical depuis les ordonnances du 24 avril 1966 », *RDSS* 1996, p. 853.

29. Y. PESQUEUX, « Sécurité, fiabilité et risque », 2015. Disponible à l'adresse suivante : https://halshs.archives-ouvertes.fr/halshs-01236503

30. Y. POULLET, A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel – Une réévaluation de l'importance de la vie privée pour la démocratie », *in* K. BENYEKHLEF, P. TRUDEL (dir.), *État de droit et virtualité*, Montréal, Thémis, 2009.

31. B. PY, « Le secret professionnel et le signalement de la maltraitance sexuelle.

L'option de conscience : un choix éthique », *Archives de politique criminelle* 2012/1, n° 34, p. 75.

32. Rédaction Lextenso, « Assurer le risque cyber : quels enjeux ? », *LPA* 4 juill. 2018, n° 133, p. 2.

33. S. ROZENFELD, « La donnée au cœur de l'e-santé », *Revue Expertises des systèmes d'information*, 1er déc. 2016, p. 405.

34. S. L. STAR, J.GRIESEMER, « Institutionnal ecology, 'Translations' and Boundary objects: amateurs and professionals on Berkeley's museum of vertrebate zoology », *Social Studies of Science*, vol. 19, n° 3, 1989. p. 393

35. H. TANGHE, P. O. GIBERT, « Big data et protection sociale : L'enjeu de l'anonymisation à l'heure du big data », *Revue française des affaires sociales* 2017/4, p. 79

36. A. TESSALONIKOS, A. BENSOUSSAN, « Risque informatique et sécurité juridique », *Gaz. pal*., n° 128, 18 avril 2002, p. 12.

37. F. VIALLA, « Perspectives pour une culture commune du secret et de l'information partagée », *Juris associations* 2013, n° 474, p. 30.

38. F. VILLEVIEILLE, « La ratification par la France de la Convention européenne des Droits de l'homme », *Annuaire Français de Droit International*, 1973 p. 922.

39. M. VIVANT, « Qu'entend-on par « données à caractère personnel » ? », *Lamy Droit du numérique* 2015, étude 4276.

40. M. VIVANT, « Quelles différences entre « données à caractère personnel » et « informations nominatives » ? », *Lamy Droit du numérique* 2015, étude 4278.

41. « La CNIL appelle à la mise en œuvre du règlement sur la protection des données », *Liaisons sociales Quotidien - L'actualité*, nº 17297, 30 mars 2017.

42. « Règlement général sur la protection des données », *Liaisons sociales Quotidien – Le dossier pratique*, nº 101, 2 juin 2017.

43. *« Réflexion sur le risque informatique »*, *Revue générale de droit des assurances*, n° 4, 1er avril 2018, p. 6.

44. *« Les règlements européens »*, *Lamy Droit du numérique*, étude 373, juin 2018.

45. *« Comment la CNIL exerce-t-elle son pouvoir de sanction ? »*, *Lamy Droit du numérique*, étude 2959, juin 2018.

Rapports

1. G. BRAIBANT, *Données personnelles et société de l'information : Rapport au Premier Ministre sur la transposition en droit français de la directive (dir.) 95/46*, 3 mars 1998.

2. P. BICLET, *Premier rapport d'activité du comité d'agrément des hébergeurs,* 2006-2011.

3. C. BOUCHOUX, *Rapport d'information fait au nom de la mission commune d'information sur l'accès aux documents administratif et aux données publiques*, n° 589, Sénat, Session ordinaire 2013-2014.

4. P.-L. BRAS, A. LOTH, *Rapport sur la gouvernance et l'utilisation des données de santé,* sept. 2013.

5. CNIL, *27e rapport d'activité*, 2006.

6. CNIL *7e rapport d'activité*, 1986.

7. CNIL, *6e rapport d'activité*, 1985.

8. CNIL, *Rapport d'activité – Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*, La Documentation française, 2017.

9. Commission Européenne, *Livre vert sur la santé mobile*, 10 avr. 2014.

10. Comité d'experts de l'Administration de la Santé Publique, Premier rapport, Série de rapports techniques, OMS, Genève, septembre 1952.

11. Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE n°108, 28 janv. 1981, entrée en vigueur le 1 oct. 1985.

12. Conseil d'Etat, *Rapport public 2006 – Jurisprudence et avis de 2005 – Sécurité juridique et complexité du droit*, La Documentation française, 2006.

13. Conseil national du Numérique, *La santé, bien commun de la société numérique,* Rapport, oct. 2015.

14. Conseil national de l'Ordre des pharmaciens, Direction des technologies en santé, Rapport d'activité : *Le Dossier pharmaceutique*, 2013.

15. Cour des comptes, *Rapport sur la Sécurité sociale*, sept. 2007.

16. Cour des comptes, *Rapport 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 – Les données personnelles de santé gérées par l'assurance maladie – Une utilisation à développer, une sécurité à renforcer*, mars 2016.

17. DHOS, Rapport : *La place de la télémédecine dans l'organisation des soins*, présenté par Pierre Simon et Dominique Acker, novembre 2008.

18. F. DELATTRE, *Rapport le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, Assemblée nationale, n° 1537, 13 avril 2004.

19. Y. DETRAIGNE, A.-M. ESCOFFIER, *Rapport d'information fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques*, Sénat, n° 441, Session ordinaire 2008-2009.

20. F. GIRAUD, G. DERIOT, J.-L. LORRAIN, *Rapport fait au nom de la commission des Affaires sociales sur le projet de loi relatif aux droits des malades et à la qualité du système de santé*, Sénat, n° 174, Session ordinaire 2001-2002.

21. Ph. GOSSELIN, *Rapport fait au nom de la commission des Affaires européennes sur la proposition de règlement 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*, Assemblée nationale, n° 4325, 7 févr. 2012.

22. G. GOUZES, *Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, Assemblée nationale, n° 3526, 9 janv. 2002.

23. Haut conseil de la santé publique, *Pour une meilleure utilisation des bases de données administratives et médico-administratives nationales pour la sante publique et la recherche*, mars 2012.

24. Inspection des affaires sociales, *La biologie médicale libérale en France, bilan et perspectives*, avril 2006.

25. Institut national des données de santé, *Expertise juridique sur l'intérêt public dans le contexte des données de santé*, 29 juin 2017.

26. Institut national de veille sanitaire, *L'alerte sanitaire en France – Principes et organisation*, mai 2005.

27. J. LE MENN, A. MILON, *Rapport d'information fait au nom de la misson d'évaluation et de contrôle de la sécurité sociale et de la commission des affaires sociales sur les agences régionales de santé*, Sénat, n° 400, Session ordinaire de 2013-2014.P. MORANGE, *Rapport d'information fait au nom de la commission des affaires sociales en conclusion des travaux de la mission d'évaluation et de*

contrôle des lois de financement de la sécurité sociale, sur les données médicales personnelles inter-régimes détenues par l'assurance maladie, versées au SNIIRAM puis au Système national des données de santé (SNDS), Assemblée nationale, n° 4533, 21 févr. 2017.

28. C. PAUL, C. FERAL-SCHUHL, *Rapport d'information déposé par la*

Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, Assemblée nationale, n° 3119, oct. 2015.

29. Rapport au Président de la République relatif à l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, *JORF* n°0011 du 13 janvier 2017, texte n° 16.

30. R. REID, J. HAGGERTY, R. MCKENDRY, *Dissiper la confusion : concepts et mesures de la continuité des soins*, Fondation canadienne de la recherche sur les services de santé, Ottawa, mars 2002.

31. Secrétariat général du gouvernement, *Loi et règlements en vigueur, Approche statistique*, janvier 2011.

32. J. THYRAUD, *Rapport fait au nom de la Commission des lois sur le projet de loi relatif à l'informatique et aux libertés*, Sénat, n° 72, Session ordinaire 19771978.

33. A. TÜRK, *Rapport fait au nom de la commission des lois sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, Sénat, n° 218, Session ordinaire 2002-2003.

34. O. VERAN, B. LACLAIS, J.-L. TOURAINE, H. GEOFFROY, R. FERRAND, *Rapport fait au nom de la commission des affaires sociales sur le projet de loi relatif à la santé*, Assemblée nationale, n° 2673, 20 mars 2015.

Décisions citées

Juridictions françaises :

1. CA Paris, 13e ch. corr., 15 mai 2007, n° 06/01954.

2. CA Paris, 7ème chambre, 15 mai 1970, *D.* 1970, p. 466.

3. CA Rennes, ch. com., 28 avril 2015, n° 14/05708.

4. Cass. crim., 5 nov. 2007, n° 07-81031, Inédit.

5. Cass. crim., 19 nov. 1985, n° 83-92813, *Bull. crim.*, n° 364.

6. Cons. const., 23 juillet 1999, 99-416 DC.

7. Cons. const., 13 mars 2003, 2003-467 DC.

8. Cons. const., 12 août 2004, 2004-504 DC.

9. CE, 19 fév. 2008, Profil France, n° 311974, Inédit.

10. CE, 10ème / 9ème SSR, 19 juillet 2010 : n°334014.

11. CE, 10ème / 9ème SSR, 19 juillet 2010, 317182. Publié au recueil Lebon.

12. CE, 10ème / 9ème SSR, 28 mars 2014, 361042

13. TGI Paris, 3e ch., sect. 3, 24 juin 2009.

Juridictions européennes :

1. CJCE, 5 févr. 1963, NV Algemene Transport – en Expedite Onderneming Van Gend en Loos c/ Administration fiscale néerlandaise, aff. 26/62.

2. CJCE, 15 juillet 1964, Costa c/ E.N.E.L., aff. 6/64.

3. CJCE, 9 mars 1978, Administration des finances de l'État c/ Société anonyme Simmenthal, aff. 106/77.

4. CJCE, 5 oct. 1994, X. c/ Commission, aff. C-404/92 P, Rec. I-128

5. CJUE, 7 déc. 2010, Peter Pammer contre Reederei Karl Schlüter GmbH & Co. KG et Hotel Alpenhof GesmbH contre Oliver Heller, Aff. jointes C-585/08 et C144/09.

6. CJUE, 13 mai 2014, aff. C-131/12, Google Spain SL, Google Inc. c/ Agence Espagnole de Protection des Données (AEPD) et Mario Costeja González.

7. CJUE, 1er oct. 2015, aff. C-230/14, Weltimmo c/ Autorité nationale de la vie privée et de la liberté,, RLDI 2015/120.

8. CJUE, 19 octobre 2016, Patrick Breyer c/ Bundesrepublik Deutschland, C582/14.

9. Conseil de l'Europe, Résolution 1165 (1998), 26 juin 1998, Droit au respect de la vie privée (24ème session).

10. Cour EDH 6 septembre 1978, Klass et autres c/ Allemagne, 5029/71.

11. Cour EDH 25 février 1997, Z. c/ Finlande, 22009/93.

12. Cour EDH, 27 août 1997, M. S. c/ Suède, 20837/92.

13. Tribunal constitutionnel allemand, 15 oct. 1983 (B VerfGE 65,1 - Volkszählung Urteil des Ersten Senats vom 15 Dezember 1983 auf die Mündliche Verhandlung vom 18 und 19 oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den verfahren über die Verfassungsbeschwerden).

Autorités administratives indépendantes :

1. CNIL, délib. 20 février 2007, n° 2007-036.

2. CNIL, délib. 22 avr. 2010 n° 2010-113.

3. CNIL, délib. 2 déc. 2010, n° 2010-449.

4. CNIL, délib. 3 janv. 2014, n° 2013-420.

5. CNIL, délib. 7 août 2014, n° 2014-298.

6. CNIL, délib. 19 janv. 2017, n° 2017-014.

7. CNIL, délib. 27 avril 2017, SAN-2017-006.

8. CNIL, délib. 18 mai 2017, n° SAN-2017-008.

9. CNIL, délib. 18 juil. 2017, n° SAN-2017-010.

10. CNIL, déc. 8 févr. 2018, n° MED-2018-006.

11. CNIL, délib. 7 mai 2018, n° SAN-2018-002.

12. CNIL, délib. 7 juin 2018, n° 2018-256.

13. CNIL, délib. 21 juin 2018, n° SAN-2018-003.

14. CNIL, délib. 24 juill. 2018, n° SAN-2018-008.

15. CADA, 21 nov. 2013, avis n° 20134348.

Abstract

La e santé, la m-santé et la quantification de soi connectent le corps et bousculent le modèle traditionnel du soin. Ils le font glisser d'une médecine curative et monopolistique à une médecine préventive et adoptant une approche de la santé telle que définie par l'OMS. Par ce truchement, la personne n'est plus simplement placée au centre du dispositif de soin elle en devient l'un des acteurs y compris dans l'intimité de sa vie privée.

Par ailleurs, sans cesse à la recherche de la réalisation d'économie mais aussi de qualité, le système de santé, a muté, sous l'effet du déploiement de l'e-santé. Il en résulte qu'il est désormais substantiellement décloisonné et ne peut plus être synthétisé dans la dichotomie classique entre le sanitaire et le médico-social. Le vecteur et la résultante de ce phénomène consiste dans la circulation de l'information de santé. Désormais majoritairement numérisée elle est devenue indispensable au soin ainsi qu'au fonctionnement du système de santé. Le soin est désormais conçu autour de l'échange et du partage catégoriel et inter-catégoriel, voire même homme-machine ou machine-machine et non plus sur une médecine fondée sur le secret. L'Homme devenu *homo numericus* n'en est pas pour autant dépourvu de tout droits et de toute intimité. Le droit et la techno-droit s'inscrivent dans ce jeux savant dont la moindre réforme inconséquente pourrait en bouleverser l'équilibre précaire.