Léo Guittet

La transparence des données de santé issues des bases médico-administratives

Pour une ouverture des bases de données respectueuse de la vie privée

---

GUITTET Léo. *La transparence des données de santé issues des bases médico-administratives. Pour une ouverture des bases de données respectueuse de la vie privée,* sous la direction de Guillaume Rousset. - Lyon : Université Jean Moulin (Lyon 3), 2019.
Disponible sur : http://www.theses.fr/2019LYSE3028

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 3.0 France (CC BY-NC-ND 3.0 FR)

Document diffusé sous le contrat *Creative Commons* « **Attribution – Pas d'utilisation commerciale - Pas de modification** »
Vous êtes libre de le reproduire, de le distribuer et de le communiquer au public à condition d'en mentionner le nom de l'auteur et de ne pas le modifier, le transformer, l'adapter ni l'utiliser à des fins commerciales.

N° d'ordre NNT : 2019LYSE3028

THÈSE de DOCTORAT DE L'UNIVERSITÉ DE LYON
opérée au sein de
L'Université Lyon 3 - Jean Moulin

Ecole Doctorale N° ED-492
(Ecole doctorale de droit)

Discipline de doctorat : Droit

Soutenue publiquement le 04/07/2019, par :
Léo GUITTET

LA TRANSPARENCE DES DONNÉES DE SANTÉ ISSUES DES BASES MÉDICO-ADMINISTRATIVES

Pour une ouverture des bases de données respectueuse de la vie privée

---

Devant le jury composé de :

M. George FAURÉ, Professeur des Universités, Université de Picardie Jules Vernes, Rapporteur

Mme Marion GIRER, Maître de conférence habilité à diriger des recherches, Université Lyon 3-Jean Moulin, Examinatrice

M. Guillaume ROUSSET, Maître de conférence habilité à diriger des recherches, Université Lyon 3- Jean Moulin, Directeur

M. François VIALLA, Professeur des Universités, Université de Montpellier, Rapporteur

L'Université Jean Moulin n'entend accorder aucune approbation ni improbation aux opinions émises dans les thèses ; ces opinions doivent être considérées comme propres à leur auteur.

REMERCIEMENTS

Je tiens à remercier Monsieur Guillaume ROUSSET pour son implication, sa disponibilité, ses nombreux conseils et ses encouragements à chacun de nos rendez-vous. La régularité et la qualité de nos échanges m'ont permis de conserver la dynamique nécessaire pendant toute la durée des travaux.

Je remercie également Madame Marion GIRER pour ses conseils réguliers, ses nombreuses relectures avisées et son exigence. Ses interventions précieuses dans la rédaction ont permis de conserver le cœur du sujet, qui est la protection de la vie privée, tout au long de mon travail.

Merci à Messieurs les Professeurs George FAURÉ et François VIALLA qui me font l'honneur de juger le fruit de mon travail.

Je remercie aussi Monsieur Eric VERHAEGHE ainsi que l'entreprise Tripalio qui sont à l'origine de ce travail et qui m'ont permis d'amorcer mes recherches et de les mener à leur terme.

Merci à tous les intervenants qui ont accepté de consacrer une partie de leur temps précieux à nos échanges enrichissants. Je remercie particulièrement Monsieur Frédéric BIZARD, Professeur d'économie à l'ESCP Europe ; Madame Catherine COMMAILLE-CHAPUS, Directrice de la stratégie de la société Openhealth ; Madame Mylène GIRARD, alors Cheffe de la mission accès aux données de santé à la DREES ; Monsieur Hervé NABARETTE, alors Conseiller technique à la Direction évaluation économique, médicale et de santé à la Haute Autorité de Santé ; Monsieur Mohammed Adnène TROJETTE, Responsable de la mission auprès du Premier Ministre sur la réutilisation des données publiques. La pluralité des points de vue recueillis, la qualité et la profondeur de nos réflexions ont été autant d'atouts inestimables dans l'élaboration des différents développements de cette thèse.

Merci à Floriane pour sa patience, son soutien et sa bonne humeur pendant ces années de travail.

Merci enfin à tous les membres de ma famille, tout le soutien reçu en toutes circonstances m'a permis d'être là aujourd'hui.

SOMMAIRE

Principales abréviations p. 9
Introduction p. 17

PARTIE I : LA TRANSPARENCE PERMANENTE DES DONNÉES DE SANTÉ RÉSERVÉE À DES ACTEURS PUBLICS PRIVILÉGIÉS p. 61
TITRE I : L'ACCÈS PERMANENT AUX DONNÉES DE SANTÉ JUSTIFIÉ PAR LE MEILLEUR FONCTIONNEMENT DU SERVICE PUBLIC p. 67
Chapitre 1 : L'accès permanent ouvert uniquement à des acteurs privilégiés du service public p. 71
Chapitre 2 : L'accès permanent prudemment ouvert au nom de la sécurité des données p. 93
TITRE II : L'ACCÈS PERMANENT AUX DONNÉES DE SANTÉ LIMITÉ PAR LA PROTECTION DE LA VIE PRIVÉE p. 119
Chapitre 1 : L'identification des limites vacillantes de l'accès permanent p. 123
Chapitre 2 : Le dépassement bienvenu des limites à l'accès permanent p. 143

PARTIE II : LA TRANSPARENCE SÉLECTIVE DES DONNÉES DE SANTÉ AU BÉNÉFICE DES ACTEURS PUBLICS ORDINAIRES ET PRIVÉS À BUT NON LUCRATIF p. 169
TITRE I : L'ACCÈS SÉLECTIF AUX DONNÉES DE SANTÉ JUSTIFIÉ PAR LA PROTECTION DE LA VIE PRIVÉE p. 175
Chapitre 1 : L'accès sélectif ouvert à des acteurs strictement contrôlés p. 179
Chapitre 2 : L'accès sélectif soumis à une procédure protectrice de la vie privée p. 213
TITRE II : L'ACCÈS SÉLECTIF AUX DONNÉES DE SANTÉ EFFECTIF SOUS CONDITIONS p. 245
Chapitre 1 : L'accès sélectif entravé par ses dysfonctionnements p. 249
Chapitre 2 : L'accès sélectif réformé sous de nouvelles conditions p. 271

PARTIE III : LA TRANSPARENCE TARDIVE DES DONNÉES DE SANTÉ POUR LES ACTEURS PRIVÉS À BUT LUCRATIF p. 315
TITRE I : L'INTERDICTION INITIALE D'ACCÈS AUX DONNÉES DE SANTÉ POUR LES ACTEURS PRIVÉS À BUT LUCRATIF p. 317
Chapitre 1 : La fermeture de l'accès aux données de santé pour le respect de la vie privée p. 321
Chapitre 2 : L'ouverture attendue de l'accès aux données de santé dans le respect de la vie privée p. 343
TITRE II : L'AUTORISATION PROGRESSIVE D'ACCÈS AUX DONNÉES DE SANTÉ POUR LES ACTEURS PRIVÉS À BUT LUCRATIF p. 367
Chapitre 1 : L'accès aux données de santé refusé sans motif concret p. 369
Chapitre 2 : L'accès aux données de santé autorisé dans un contexte favorable p. 391

Conclusion p. 423
Bibliographie p. 429
Index p. 465
Annexes p. 471
Table des matières p. 499

LISTE DES PRINCIPALES ABRÉVIATIONS

ADELF	Association des épidémiologistes de langue française
AFSSAPS	Agence française de sécurité sanitaire des produits de santé
AIPD	Analyse d'impact relative à la protection des données
AJ	Actualité juridique
AJDA	Actualité juridique droit administratif
Al.	Alinéa
ALD	Affection de longue durée
AMELI	Assurance maladie en ligne
AMM	Autorisation de mise sur le marché
AMOS	Assurance maladie offre de soins
AMP	Assistance médicale à la procréation
ANSM	Agence nationale de sécurité du médicament et des produits de santé
Ar. ou Art.	Article
ARH	Agence régionale de l'hospitalisation
ARS	Agence régionale de santé
ATIH	Agence technique de l'information sur l'hospitalisation
BCMD	Base de causes médicales de décès
BO	Bulletin officiel
CADA	Commission d'accès aux documents administratifs
CASD	Centre d'accès sécurisé aux données à distance
CCDSHS	Comité de concertation pour les données en sciences humaines et sociales
CCMSA	Caisse centrale de la mutualité sociale agricole

CCNE	Comité consultatif national d'éthique
CCTIRS	Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé
CE	- Conseil d'Etat - Communauté européenne
CEPD	Comité européen de la protection des données
CépiDc	Centre d'épidémiologie sur les causes médicales de décès
CEREES	Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé
CESREES	Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé
CETAF	Centre technique d'appui et de formation des centres d'examens de santé
Chap.	Chapitre
CHU	Centre hospitalier universitaire
CIL	Correspondant informatique et libertés
CLCC	Centre de lutte contre le cancer
CMS	*Centers for medicare & medicaid services*
CMU	Couverture maladie universelle
CNAM	- Caisse nationale d'assurance maladie - Conservatoire national des arts et métiers
CNAMTS	Caisse nationale d'assurance maladie des travailleurs salariés
CNIL	Commission nationale de l'informatique et des libertés
CNRS	Centre national de la recherche scientifique
CNSA	Caisse nationale de solidarité pour l'autonomie
Concl.	Conclusion
COPIIR	Comité d'orientation et de pilotage d'information inter-régimes
CPAM	Caisse primaire d'assurance maladie

CPP	Comité de protection des personnes
CPRD	*Clinical practice research datalink*
CRO	Organisation de recherche clinique par contrat
CSF	Comité stratégique de filière des industries et technologies de santé
CTIP	Centre technique des institutions de prévoyance
D.	Recueil Dalloz
DAMIR	Dépenses d'assurance maladie inter-régimes
DARES	Direction de l'animation de la recherche, des études et des statistiques
DC	Contrôle de constitutionnalité des lois ordinaires, lois organiques, des traités, des règlements des Assemblées
DCIR	Datamart de consommation inter-régimes
DGCS	Direction générale de la cohésion sociale
DGOS	Direction générale de l'offre de soins
DGS	Direction générale de la santé
DPD	Délégué à la protection des données
DPO	*Data protection officer* (version anglaise du DPD)
DREES	Direction de la recherche, des études, de l'évaluation et des statistiques
DRSM	Direction régionale de service médical
Dr. Soc.	Droit social
DSS	Direction de la sécurité sociale
EGB	Echantillon généraliste des bénéficiaires
EHESP	Ecole des hautes études en santé publique
EPST	Etablissement public à caractère scientifique et technologique
FFA	Fédération française de l'assurance
FIV	Fécondation *in vitro*
FNIM	Fédération nationale indépendantes des mutuelles

FNMF	Fédération nationale de la mutualité française
FOIN	Fonction d'occultation des identifiants nominatifs
GIE	Groupement d'intérêt économique
GIP	Groupement d'intérêt public
HAS	Haute autorité de santé
HCAAM	Haut conseil pour l'avenir de l'assurance maladie
Ibid. *Ibidem*	Au même endroit
IDS	Institut des données de santé
INDS	Institut national des données de santé
Infra	Voir ci-dessous
INRIA	Institut national de la recherche en informatique et en automatique
INSEE	Institut national de la statistique et des études économiques
INSERM	Institut national de la santé et de la recherche médicale
InVS	Institut de veille sanitaire
IRDES	Institut de recherche et de documentation en économie de la santé
JCP A	La semaine juridique, édition administrations et collectivités territoriales
JCP E	La semaine juridique, édition entreprise
JCP G	La semaine juridique, édition générale
JCP S	La semaine juridique, édition sociale
JDSAM	Journal du droit de la santé et de l'assurance maladie
JORF	Journal officiel de la République française
LEGICOM	Revue thématique de droit de la communication
MDPH	Maisons départementales de personnes handicapées
MED	Mise en demeure

MONACO	Méthodes, outils, normes, pour la mise en commun de données entre les assureurs maladie complémentaires et obligatoires
MR	Méthodologie de référence
MSA	Mutualité sociale agricole
NIR	Numéro d'inscription au répertoire national d'identification des personnes physiques
OCT	Organismes concentrateurs techniques
OFDT	Observatoire français des drogues et de la toxicomanie
Op. cit.	Dans l'ouvrage précité
P.	Page
PAERPA	Personnes âgées en risque de perte d'autonomie
PDS	Plateforme des données de santé
PIA	*Privacy impact assessment* (version anglaise de l'AIPD)
PMSI	Programme médicalisé des systèmes d'information
PUF	Presses universitaires de France
RA	La Revue administrative
RDP	Revue de droit public
RDS	Revue droit et santé
RDSS	Revue de droit sanitaire et social
RGDM	Revue générale de droit médical
RGPD	Règlement général sur la protection des données. Nom complet : 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, et abrogeant la directive 95/46/CE
RNIPP	Répertoire national d'identification des personnes physiques
RPDA	Revue pratique de droit administratif
RPU	Résumés de passage aux urgences
RSI	Régime social des indépendants

RTD Eur.	Revue trimestrielle de droit européen
S.	Recueil Sirey
SAFARI	Système automatisé pour les fichiers administratifs et le répertoire des individus
SCA	Syndromes coronariens aigus
SIG	Service d'intérêt général
SIEG	Service d'intérêt économique général
SESAM	Système électronique de saisie de l'Assurance maladie
SNDS	Système national des données de santé
SNIIRAM	Système national inter-régimes de l'Assurance maladie
Supra	Voir ci-dessus
TFUE	Traité sur le fonctionnement de l'Union européenne
UE	Union européenne
UNCAM	Union nationale des caisses d'assurance maladie
UNOCAM	Union des organismes d'assurance maladie complémentaire
URPS	Union régionale des professionnels de santé
V.	Voir
Vol.	Volume

INTRODUCTION

1. Les données de santé à caractère personnel « *ne sont pas des données comme les autres. C'est pourquoi le Conseil constitutionnel a considéré*[1] *qu'il appartenait au législateur d'instituer une procédure propre à sauvegarder la vie privée des personnes, lorsqu'est demandée la communication de données susceptibles de permettre leur identification, et a érigé en principe de valeur constitutionnelle le respect de la vie privée* »[2]. C'est en respectant ce principe inamovible que l'accès aux données de santé contenues dans les bases de données médico-administratives s'est développé progressivement en France.

2. Au cœur des préoccupations des acteurs du système de santé et de ses usagers, notamment depuis la création du Système national d'information interrégimes de l'Assurance Maladie (SNIIRAM) en 1999[3], les données de santé ont fait couler beaucoup d'encre que cela soit en raison de leur nature juridique[4], que des grandes affaires relatives à la santé publique, dont la plus emblématique est celle du Mediator[5], qui ont vu le jour en raison du manque de maîtrise de ces données. La volonté de récolte massive des données de santé par l'administration française dès la veille du XXIe siècle semblait indiquer une volonté de faire évoluer les mécanismes organisationnels du système de santé pour l'adapter aux nouvelles technologies de

---

[1] Conseil constitutionnel, 23 juillet 1999, n° 99-416 DC *relative à la loi portant création d'une couverture maladie universelle.*

[2] Rapport d'information déposé par la Commission des affaires sociales à l'Assemblée nationale 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, 21 février 2017.

[3] Loi n° 98-1194 du 23 décembre 1998 *de financement de la sécurité sociale pour 1999*, *JORF*, n° 300, 27/12/1998, article 21.

[4] V. notamment CLEMENT J.-M., MEMETEAU G., *Le droit des données de santé*, RGDM, 2004, n° 4 ; HERVE C., STANTON-JEAN M. et MARTINENT E., *Les systèmes informatisés complexes en santé. Banque de données, télémédecine : normes et enjeux éthiques*, Dalloz, 2013, 282 p. ; GROSJEAN A. (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Larcier, 2015, 465 p. ; CASTETS-RENARD C. (dir.), *Quelle protection des données personnelles en Europe ? : actes du colloque tenu le 14 Mars 2014 à la Faculté de droit de l'Université Toulouse 1 Capitole*, Larcier, 2015, 187 p.

[5] V. notamment ARBBOUSSET H., « Mediator et indemnisation des victimes : retour sur une affaire d'Etat », *JCP A*, 12/12/2011, n° 50 ; ROTOULLIE J. C., « Responsabilité de la puissance publique – Mediator : responsabilité de l'Etat à partir de 1999 et faute des laboratoires Servier – Veille », *JCP G*, 21/11/2016, n° 47 ; Conseil d'Etat, « Affaire du médiator : portée de la responsabilité de l'Etat », *Recueil Dalloz*, 24/11/2016, n° 40.

Si l'affaire du Mediator relève avant tout de la pharmacovigilance, il a beaucoup été affirmé que l'accès plus ouvert aux données de santé, notamment de prescription et d'utilisation des produits pharmaceutiques concernés, aurait permis, par la multiplication facilitée des études sur le sujet, de détecter plus rapidement les conséquences d'une consommation du médicament en dehors du cadre de son autorisation de mise sur le marché. C'est notamment ce qui est démontré à la page 17 du document de POLTON D. et RICORDEAU P., « Le SNIIRAM et les bases de données de l'Assurance maladie en 2011 », CNAMTS, 30/03/2011.

l'information. Or, avant la réforme portée par la loi du 26 janvier 2016[6], l'accès aux bases de données en santé s'est très rapidement limité à quelques rares privilégiés : les accès permanents sont restés trop rares et les modalités d'autorisation d'accès ont pêché par leur grande imprécision, leur lenteur et leur manque d'ergonomie[7]. La création d'un système de récolte de données de santé, en apparence potentiellement accessible mais plutôt difficile d'accès en pratique, a donné lieu à de nombreuses critiques. Ce d'autant plus qu'il est apparu que si certaines données de santé avaient été accessibles plus facilement, le scandale du Mediator aurait pu être, sinon évité, au moins en partie limité.

3. Si les responsables des bases de données de santé ont semblé si réticents à proposer un accès plus large à leur contenu, c'est précisément pour protéger ce contenu. En effet, les données de santé sont bien souvent associées à des individus et à ce qui relève de leur sphère privée : ce sont alors des données personnelles. En voulant s'adapter aux nouvelles technologies, les créateurs de l'une des plus grandes bases de données de santé au monde[8] n'ont pas souhaité proposer de nouveau cadre d'utilisation des données qui respecte la vie privée des individus. Il est vrai que les innovations en matière d'informatique et de traitement automatique des informations ont été très nombreuses dans les années 2000 : le temps de l'innovation technologique était alors bien plus rapide que le temps de l'innovation législative et réglementaire. La réforme proposée par la loi du 26 janvier 2016 a pour objectif de rattraper le retard pris depuis plusieurs années en fixant un cadre d'autorisation d'accès aux données de santé sans que cela ne contrevienne au droit des individus au respect de leur vie privée.

4. La protection de la vie privée est un élément fondamental de l'émergence des données personnelles. Ce principe de protection des individus à travers l'utilisation informatique qui peut être faite de leurs informations a été consacré par le droit français dans la loi relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés, du 6 janvier 1978[9]. Cette loi n'a pas été pensée ni votée en un jour et trouve ses origines dans un projet de loi initié

[6] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, JORF n° 0022, 27/01/2016.

[7] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *Communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale*, 03/2016, p.50 – 64.

[8] Cour des comptes, *Ibid.* p.25.

[9] Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés, JORF*, 07/01/1978.

par le ministère de l'Intérieur en 1973[10]. Dénommé projet SAFARI, pour système automatisé pour les fichiers administratifs et le répertoire des individus, l'objectif était alors de créer une base de données entièrement informatisée permettant de centraliser toutes les informations relatives à la population en utilisant un seul et unique identifiant pour l'ensemble des fichiers. L'intention première était ainsi de favoriser l'interconnexion entre les fichiers. Révélé par le journal Le Monde en 1974, qui titrait alors « *SAFARI ou la chasse aux Français* »[11], le projet de loi a rapidement été perçu comme une menace sur la vie privée et la liberté individuelle.

5. C'est dans ce contexte de défiance vis-à-vis du traitement informatique des informations que la commission Informatique et liberté fut créée, devenant la première autorité administrative indépendante[12], afin de travailler sur la mise en œuvre d'une réglementation sur l'utilisation des moyens informatiques. De ce travail découle directement le projet de loi relatif à l'informatique et aux libertés qui est la loi que nous connaissons bien aujourd'hui. Cette loi étant une réponse aux craintes ressenties face à une utilisation des données personnelles des individus, elle pose immédiatement les principes de son application. Ainsi, son article 1 précisait dès 1978 que « *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* »[13]. Jusqu'à l'entrée en vigueur de la loi pour une République numérique du 7 octobre 2016[14], soit une période de plus de 30 ans, cet article 1 n'a fait l'objet d'aucune modification. Dans sa version modifiée le 9 octobre 2016, l'article 1 ajoute que « *toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* »[15]. Puis, cette formule a été une nouvelle fois modifiée pour entrer en résonance directe avec le Règlement général relatif à la protection des données[16] (aussi appelé RGPD). L'article 1 précise effectivement que « *les droits des personnes de décider et de contrôler les usages qui sont faits des données à caractère*

[10] Site internet du CNRS, Origine de la loi Informatique et Libertés.

[11] BOUCHER P., « Safari ou la chasse aux Français », *Le Monde*, édition du 21/03/1974, page 9.

[12] MAISL H., « Informatique et libertés : de 1978 à 2004 », *Communication Commerce électronique*, 01/2005, n° 1.

[13] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, article 1.

[14] Loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique*, *JORF*, n° 0235, 08/10/2016.

[15] Loi n° 78-17 du 6 janvier 1978, *op*. cit., article 1 modifié par l'article 54 de la loi pour une République numérique.

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

personnel les concernant et les obligations incombant aux personnes qui traitent ces données s'exercent dans le cadre du [RGPD] […] *de la présente loi* »[17]. La loi est, par conséquent, d'abord un moyen de rassurer les individus sur la protection de leurs données personnelles face aux traitements informatiques dont elles peuvent faire l'objet. Mais son existence et son effectivité n'ont pas empêché de vives réactions à la fin de l'année 2016 lorsqu'un décret[18] a annoncé la mise en œuvre d'un fichier unique contenant toutes les informations relatives à l'identité des individus. Les questionnements sur ce fichier[19], mis en place par décret, sans consultation du Parlement, ont ravivé des questionnements déjà émis avec l'affaire SAFARI. J. THYRAUD[20] disait alors s'interroger « *sur le devenir des libertés individuelles et publiques dans la quête permanente à l'information* ».

6. Dans cette atmosphère peu sereine, la loi de modernisation de notre système de santé[21] est entrée en application pour proposer une nouvelle rédaction des dispositions de la loi Informatique et libertés relatives à l'accès aux données de santé. Si le nouveau mécanisme de mise à disposition des informations est présenté comme une amélioration nécessaire de l'ancien système[22], cette réforme soulève d'autant plus d'interrogations et de doutes[23] sur la sécurité de données que les technologies permettant d'exploiter les données gagnent en performances[24].

---

[17] Loi n° 78-17 du 6 janvier 1978, *op. cit*., article 1 modifié par l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 *relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel*, *JORF*, n° 0288, 13/12/2018.

[18] Décret n° 2016-1460 du 28 octobre 2016 *autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité*, *JORF*, n° 0254, 30/10/2016.

[19] KOUBI G., « *Le « méga-fichier » des titres électroniques sécurisés* », Etude, *JCP A*, 28/11/2016, n° 47.

[20] Jacques THYRAUD était sénateur de Loir-et-Cher de 1974 à 1992, il est l'auteur de plusieurs rapports rédigé au nom de la Commission des Lois sur le Projet de loi relatif à l'informatique et aux libertés : Rapport n° 72 (1977-1978) de M. Jacques THYRAUD, fait au nom de la commission des lois, déposé le 10 novembre 1977, Rapport n° 199 (1977-1978) de M. Jacques THYRAUD, fait au nom de la commission des lois, déposé le 19 décembre 1977, Rapport n° 232 (1977-1978) de MM. Jacques THYRAUD, sénateur et Jean FOYER, député, fait au nom de la commission mixte paritaire, déposé le 21 décembre 1977.

[21] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*, article 193.

[22] Le titre du chapitre V de la loi Santé « Créer les conditions d'un accès ouvert aux données de santé » induit qu'auparavant, l'accès était fermé.

[23] PECHILLON E., « L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ? », *L'information psychiatrique*, 8/2015, volume 91, p. 645-649.

[24] MENDOZA-CAMINADE A., « Big data et données de santé : quelles régulations juridiques ? », *Revue Lamy Droit de l'immatériel*, 01/06/2016, n° 127.

7. La définition précise de la notion même de donnée de santé et de chacune de ses composantes est un préalable essentiel (§1) à la compréhension de l'étude. Les enjeux qui entourent l'accès aux données de santé doivent également être abordés au travers des thèmes majeurs qui traversent l'étude (§2). Puis la question essentielle de la compatibilité entre la sécurisation des données de santé et le développement d'un accès plus ouvert à ces données sera finalement traitée (§3).

Paragraphe 1 : La donnée de santé, une notion aux visages multiples

8. Préalablement à une réflexion portant sur le sujet des données de santé, il est primordial de discerner les contours élémentaires des termes utilisés (A), avant d'aborder les caractéristiques des différentes formes sous lesquelles peut se présenter la donnée de santé (B).

A) La donnée de santé, l'association de deux termes distincts

9. Pour comprendre ce qu'est une donnée de santé, il faut étudier dans un premier temps la notion de donnée (1), puis il convient d'analyser dans un deuxième temps la signification du terme « santé » (2) qui caractérise le type de donnée qui nous intéresse. Une fois ces notions définies, la donnée de santé peut faire l'objet d'un décryptage complet (3). Enfin, il est important de s'intéresser aux grandes bases médico-administratives susceptibles de contenir des données de santé (4).

1) La donnée, une information transformée

10. Le terme « donnée » dispose à lui-seul de plusieurs définitions dans le dictionnaire. Celle qui nous intéresse n'est pas la première à être proposée. En effet, la notion de donnée, au sens informatique, ne s'est greffée aux définitions existantes qu'avec le développement des technologies informatiques au cours du XXe siècle. La donnée est alors définie comme une « *Représentation conventionnelle d'une information en vue de son traitement informatique* »[25]. Une donnée serait donc une information qui a subi une transformation. Ce n'est qu'en vue de l'usage informatique qui sera fait de l'information que cette dernière est traitée pour devenir

[25] Dictionnaire Petit Larousse, édition 2017.

une donnée. Certains juristes, comme I. de LAMBERTERIE ont défini la donnée comme « *une information valorisée qui possède une valeur ajoutée d'ordre technologique* »[26]. La distinction opérée entre l'information et la donnée est primordiale : l'information initiale, par un traitement spécifique, cesse d'être une information pour devenir une donnée nouvelle qui sera utilisée par le truchement d'une technologie informatique.

11. Ces définitions restent doctrinales et, même si la doctrine est claire dans son propos, tout cela reste insuffisant et fort éloigné d'une définition juridique appropriée. Un arrêté en date du 22 décembre 1981 relatif à l'enrichissement du vocabulaire informatique est tout de même venu proposer une définition juridique qui n'en demeure pas moins une simple recommandation. La donnée est, d'après cet arrêté « *la représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement* »[27]. Le Conseil de l'Europe[28] s'est également emparé de la question en 2001 en définissant la donnée comme « *toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction* ». La donnée reçoit ici une définition plus étendue : elle devient une représentation immatérielle destinée à un traitement informatique de faits, d'informations ou de concepts.

12. Au travers de ces différentes approches, juridiques ou non, de la donnée, plusieurs enseignements peuvent être tirés. Le premier enseignement est que cette notion, si elle n'a pas encore été clairement définie en droit français, parvient à agréger autour d'elle des définitions qui procèdent d'un résultat similaire : la donnée est le produit d'une information transformée. Le deuxième enseignement est celui de l'usage qui sera fait de la donnée : l'information devient donnée à des fins de traitement par une technologie informatique. Il est finalement plutôt regrettable, que le législateur n'ait pas saisi l'opportunité de définir la donnée au cours des débats sur la loi pour une République numérique[29] ou sur la loi relative à la modernisation de notre système de santé[30].

[26] de LAMBERTERIE I., « Qu'est-ce qu'une donnée de santé ? », *RGDM*, 30/09/2004, n° 4, p. 13.

[27] Arrêté du 22 décembre 1981 *relatif à l'enrichissement du vocabulaire informatique*, *JORF*, 17/01/1982.

[28] Conseil de l'Europe, Convention sur la cybercriminalité signée à Budapest, Chapitre I, Article 1, 23/11/2001.

[29] Loi n° 2016-1321 du 7 octobre 2016, *op. cit*.

[30] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

2) La santé, une thématique vaste

13. Pour définir la notion de santé, il convient de se rapporter à la définition précise qu'en donne l'Organisation mondiale de la Santé (OMS) : « *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* »[31]. L'OMS lie *de facto* la santé aux individus et à leur état, qu'il soit bon ou mauvais. Il est important de retenir que les informations d'ordre social entrent dans la sphère sanitaire. Cette approche qui n'a pas changé depuis 1948 se limite à l'information relative à l'individu. Cela reste malgré tout une définition plutôt restrictive car cantonnée à la santé de l'individu. L'OMS semble aussi avoir une approche uniquement positive de la santé en évoquant le « *complet bien-être* ». Il aurait été intéressant de retrouver une définition, non pas exhaustive, mais plus élaborée du terme, notamment avec l'inclusion de la distinction entre bonne ou mauvaise santé.

14. Le dictionnaire français propose, lui, une définition comprenant deux approches distinctes. D'abord la santé relative aux êtres vivants qui est définie en premier lieu comme un « *bon état physiologique d'un être vivant* »[32] puis comme le « *fonctionnement plus ou moins harmonieux de l'organisme* »[33]. Une deuxième définition est donnée, celle de la santé dans le cadre d'une collectivité qui permet de connaître d'une part l'« *état physiologique et psychique des membres d'un groupe social* »[34], d'autre part l'« *état plus ou moins satisfaisant (dans le domaine économique)* »[35]. La définition de la santé est ici plus vaste que celle, bien trop sujette à interprétations, donnée par l'OMS. La santé peut porter sur une information positive ou négative relative à la physiologie d'un individu. Tandis que le terme peut aussi renvoyer à la santé physiologique ou psychique d'un groupe d'individus, par exemple, la santé publique.

15. La définition de la santé reste finalement assez ouverte pour l'associer à de nouvelles thématiques ou interprétations. Il est étonnant qu'aucune définition juridique n'ait vu le jour

---

[31] Préambule à la Constitution de l'Organisation mondiale de la Santé, tel qu'adopté par la Conférence internationale sur la Santé, New York, 19 juin -22 juillet 1946 ; signé le 22 juillet 1946 par les représentants de 61 Etats. (Actes officiels de l'Organisation mondiale de la Santé, n° . 2, p. 100) et entré en vigueur le 7 avril 1948.

[32] Dictionnaire Petit Larousse, édition 2017.

[33] *Ibid.*

[34] *Ibid.*

[35] *Ibid.*

depuis celle donnée par l'OMS. Cette absence de définition n'a toutefois pas empêché la donnée de santé de recevoir une définition juridique dans les règles de l'art.

3) La donnée de santé, une notion récemment définie

16. La donnée de santé a longtemps été mentionnée et utilisée tant au niveau national qu'au niveau européen, sans jamais être définie. Ainsi, la loi relative à l'Informatique aux fichiers et aux libertés du 6 janvier 1978[36] ou encore la directive européenne 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[37] de 1995 restent silencieuses à ce propos. La notion même de donnée de santé n'a été intégrée à la loi relative à l'informatique et aux libertés[38] qu'avec l'entrée en vigueur de la loi relative au traitement de données nominatives[39] ayant pour fin la recherche dans le domaine de la santé[40]. Bien que, d'après le titre de ce texte, la santé soit une caractéristique propre au domaine de la recherche envisagée et non aux données nominatives potentiellement traitées, nous pouvons déduire sans grand risque que ces données pouvaient être qualifiées de données de santé, cela alors même que cette notion difficile à cerner n'a été concrètement définie que récemment par le Règlement général pour la protection des données[41].

17. Une distinction essentielle doit s'opérer entre la donnée de santé au sens large et la donnée de santé à caractère personnel[42] qui est plus restrictive. La donnée de santé ne peut être limitée à la seule information concernant la santé d'un individu. Comme le soulignent les auteurs du rapport de la Commission Open data en santé[43], les données de santé sont nombreuses et vont bien au-delà de la personne. Elles visent aussi bien l'offre de soins (infrastructures,

---

[36] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[37] Directive 95/46/CE du 24 octobre 1995 modifiée par le règlement n° 1882/2003 du 20 novembre 2003 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.

[38] V. le chapitre V bis contenant les articles 40-1 à 40-10 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version modifiée par la loi n° 94-548 du 1er juillet 1994, *relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé*, JORF n° 152, 02/07/1994.

[39] V. *infra* n° 273 notre réflexion sur l'utilisation des termes « données nominatives ».

[40] Loi n° 94-548 du 1er juillet 1994, *op. cit.*

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

[42] *Infra* n° 27 à 39.

[43] BURNEL P. et VON LENNEP F., Rapport de la Commission open data en santé, 9 juillet 2014, 122 p., p. 33.

professionnels, tarifs), que la finance (dépenses de soins, de prévention, de gestion), ou que la santé publique et épidémiologique (données relatives aux patients, données sur l'environnement). Cette cartographie officielle des données de santé est proposée par la mission Etalab[44] sous l'autorité du Premier ministre.

18. Ce n'est qu'en 2007 qu'une première proposition de définition de la donnée de santé a vu le jour. Elle est alors abordée sous l'angle de la donnée personnelle. C'est le G29, qui regroupe les instances nationales européennes chargées de la protection des données et de la vie privée, a proposé une première approche[45] de la donnée personnelle de santé qui serait alors « *une donnée en relation étroite avec l'état de santé de la personne, telle qu'une information sur la consommation d'alcool, de drogues ou de médicaments doit être considérée comme une donnée de santé au sens de la directive* »[46]. Le G29 tente ici d'élargir le spectre de la donnée personnelle de santé qui doit englober des informations donnant des indices sur l'état de santé de l'individu.

Lors de la conférence nationale de santé de 2010, l'avis sur les données de santé informatisées[47] proposait la définition suivante : « *les données de santé sont des informations sur l'état de santé et les maladies d'un individu ou d'une population donnée mais aussi sur des éléments qui peuvent déterminer l'état de santé et les maladies (facteurs de risques médicaux, biologiques ou génétiques ; comportements de santé ; consommation de soins ; positions sociales ; conditions de travail ; conditions de vie ; environnement physique de l'habitat…)* ». Cette définition est intéressante à plus d'un titre. D'abord, il en ressort que les données de santé peuvent concerner un individu mais aussi une population donnée, ce qui n'était pas le cas dans la définition du G29. Ensuite, elle va plus loin que le G29 en donnant une liste non exhaustive des éléments qui permettent de déterminer l'état de santé et les maladies : se retrouvent notamment dans cette liste des éléments sur les positions sociales, en référence à la définition de la santé donnée par l'OMS, mais aussi des éléments sur les conditions de vie ou les conditions de travail.

[44] Etalab, Cartographie des bases de données publiques en santé, www.data.gouv.fr.

[45] BURNEL P. et VON LENNEP F., *op. cit*., p. 18.

[46] G29, "Working Document on the processing of personal data relating to health in electronic health records (EHR)", février 2007.

[47] Conférence Nationale de Santé, Avis sur les données de santé informatisées, 19 octobre 2010, p. 3.

Une autre définition de la donnée de santé a été proposée en 2013 par le rapporteur Pierre-Louis Bras. Cette définition vise particulièrement la donnée de santé à caractère personnel[48], l'auteur indique, en l'absence de définition légale, qu'une donnée de santé à caractère personnel est « *une donnée susceptible de révéler une maladie de la personne* »[49]. Cette nouvelle tentative d'explication de ce qu'est une donnée personnelle de santé démontre l'instabilité juridique qui entoure ce sujet. En effet, la définition suggérée en 2010 se voulait précise et extensive tandis que les critères retenus par M. Bras semblent signifier une régression en abandonnant le caractère ouvert de la notion pour se concentrer sur la maladie éventuelle de l'individu.

19. Finalement, après des années d'incertitude, le Parlement européen est intervenu en 2016 en proposant, dans le RGPD[50] une définition complète de la donnée de santé à caractère personnel. Cette définition est composée d'une part du contenu du considérant numéro 35 du Règlement, d'autre part du contenu du point numéro 15 de l'article 4 du Règlement.

Ainsi, le considérant numéro 35 indique que « *les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil (1) au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source,*

[48] Pour la définition de la donnée à caractère personnel, voir *infra* n° 28 à 31.

[49] BRAS P.-L., Rapport sur la gouvernance et l'utilisation des données de santé, septembre 2013, p. 29.

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

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 »[51].

Quant au point numéro 15 de l'article 4 du Règlement, il précise que les données de santé à caractère personnel sont « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* »[52].

20. Cette définition, prise en ses deux composantes, appelle plusieurs commentaires. Le considérant 35 interpelle d'abord par l'utilisation du conditionnel. Cela sous-entend que les auteurs de la définition sont conscients que leur proposition a vocation à servir d'ancrage juridique tout en laissant la possibilité à de nouveaux critères de venir se greffer au champ recouvert par la donnée personnelle de santé. Si le considérant 35 est remarquable par sa longueur, le point numéro 15 de l'article 4 est tout aussi remarquable de par sa brièveté. Et c'est à cet endroit qu'une ambiguïté s'installe car les informations susceptibles de révéler une information sur l'état de santé de la personne sont totalement absentes de la définition de la donnée personnelle de santé par le Règlement européen. D'après la rédaction du texte, seules les données qui révèlent directement une information sur la santé de la personne entrent dans le champ de la donnée de santé. L'usage du conditionnel au considérant numéro 35 prend alors toute son importance et il semble essentiel, d'adopter une approche extensive de la définition de donnée personnelle de santé.

4) La donnée de santé au cœur des bases médico-administratives

21. Avant de parler de l'accessibilité des données de santé, il convient de savoir dans quelles bases elles sont contenues, et depuis combien de temps. Dans le cadre de cette étude, ce sont les deux grandes bases de données historiques qui sont à l'honneur, le SNIIRAM et le PMSI (Programme de médicalisation des systèmes d'information), sans oublier le nouveau SNDS (Système national des données de santé) créé pour les rassembler.

[51] Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016, *op. cit.*, à lire à la lumière du considérant 53.

[52] *Ibid.*

22. La base médico-administrative la plus importante en France est le SNIIRAM. Créé à la fin de l'année 1998 par la loi de financement de la sécurité sociale pour 1999[53], il n'a été véritablement mis en œuvre qu'à partir de la parution de l'arrêté de 2002 relatif à son fonctionnement[54]. Cette base de données de santé a été conçue pour contenir les informations liées aux soins de ville provenant des organismes gérant un régime de base d'assurance maladie : elle est rapidement devenue l'une des plus grandes bases de données de santé au monde[55]. Les trois finalités alors prévues étaient l'amélioration de la qualité des soins, la meilleure gestion de l'assurance maladie, la transmission aux prestataires de soins des données relatives à leur activité. Mais le SNIIRAM a aussi été pensé, dès l'origine, pour contenir les données hospitalières. En effet, l'arrêté paru en 2002[56] a décidé du déversement des données issues du PMSI au sein du SNIIRAM, mais ce n'est qu'en 2006 que le premier chaînage a véritablement eu lieu, puis c'est en 2010 que ce processus a été industrialisé : le SNIIRAM est alors devenu le SNIIRAM élargi[57]. Nous verrons plus en détails à travers la présente étude l'étendue des données de santé qui, petit-à-petit, ont intégré le champ du SNIIRAM. L'accès aux données de santé à caractère personnel contenues dans cette base, bien que traitées pour ne pas être directement identifiantes, est très étroitement contrôlé par un processus législatif et réglementaire qui n'a cessé d'évoluer depuis sa création. Le terme SNIIRAM utilisé à travers l'étude renverra de façon générale à sa structure élargie.

23. Chronologiquement, le PMSI, dédié à la récolte des données hospitalières, est né avant le SNIIRAM. Il a émergé progressivement entre le début des années 1980 et le milieu des années 1990. En effet, dès 1982 ce programme encore appelé « *Projet de médicalisation du système d'information* »[58] est en pleine préparation pour devenir l'équivalent français d'un système déjà existant sur le sol américain : les « Diagnosis Related Groups » ou DRG. L'objectif du PMSI est de récolter les données produites par les hôpitaux afin de leur donner une visibilité sur leur

[53] Loi n° 98-1194 du 23 décembre 1998 *de financement de la sécurité sociale pour 1999*, JORF, n° 300, 27/12/1998, article 21.

[54] Arrêté du 11 avril 2002 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, JORF n° 89 du 16/04/2002.

[55] BRAS, P.-L., Rapport sur la gouvernance et l'utilisation des données de santé, *op. cit.*, p. 21.

[56] *Ibid.*

[57] BRAS P.-L., Rapport sur la gouvernance et l'utilisation des données de santé, *op. cit.*, p. 12.

[58] RODRIGUES J.-M., « Le Projet de médicalisation du Système d'Information-PMSI- : Méthode définition organisation », *Gestions Hospitalières*, 03/1983, n° 224, p. 205-209.

activité et de mieux maîtriser leur financement[59]. Pendant quelques années, la mise en œuvre du PMSI est expérimentée dans certains hôpitaux publics jusqu'en 1989 où son utilisation est généralisée à tous les établissements publics par circulaire[60]. Puis, en 1991, l'obligation d'évaluer l'activité hospitalière (sans utiliser le PMSI) a été étendue à tous les établissements, qu'ils soient publics ou privés, par la loi[61]. Ce n'est qu'avec la parution d'un arrêté en 1994[62] et d'une circulaire parue l'année d'après[63] que l'obligation de transmettre les données hospitalières à destination du PMSI a été décidée pour les établissements de santé publics et privés à but non lucratif. L'obligation a finalement été étendue aux établissements de santé privés à but lucratif avec un arrêté paru en 1996[64]. Le respect de la vie privée des individus dont les données de santé à caractère personnel sont traitées est au centre des textes qui portent sur la mise en œuvre des traitements liés au PMSI. Les hôpitaux ont ainsi l'obligation de demander l'avis préalable de la CNIL ou de procéder à une déclaration auprès d'elle. Les arrêtés précités précisent également que toutes les mesures doivent être prises pour garantir aux patients la possibilité d'exercer leurs droits d'accès et de rectification à leurs données à caractère personnel, comme le prévoit la loi relative à l'informatique et aux libertés[65]. Autre mesure hautement importante : toutes les données destinées au PMSI doivent faire l'objet d'un processus d'anonymisation. Cette base est gérée indépendamment du SNIIRAM par l'Agence technique de l'information hospitalière[66] (ATIH). La particularité du PMSI tient au contrôle de

[59] HOLCMAN R., « Le programme de médicalisation du système d'information (PMSI) », *Management hospitalier*, 2015, p. 553-568.

[60] Circulaire DH/PMSI relative à la généralisation du programme de médicalisation des systèmes d'information (PMSI) et à l'organisation de l'information médicale dans les hôpitaux publics, n° 303, 24/07/1989.

[61] Loi n° 91-748 du 31 juillet 1991 portant réforme hospitalière, JORF n° 179 du 02/08/1991.

[62] Arrêté du 20 septembre 1994 relatif au recueil et au traitement des données d'activité médicale et de coût, visées à l'article L. 710-5 du code de la santé publique, par les établissements de santé publics et privés visés aux articles L. 714-1, L. 715-5 du code de la santé publique et aux articles L. 162-23, L. 162-23-1 et L. 162-25 du code de la sécurité sociale et à la transmission aux services de l'Etat et aux organismes d'assurance maladie d'informations issues de ces traitements, JORF n° 242, 18/10/1994.

[63] Circulaire DH/DSS/95 relative à la généralisation du dispositif technique, expérimenté en région Languedoc-Roussillon, de mesure de l'activité et des coûts des établissements hospitaliers sous compétence tarifaire de l'Etat, à l'aide des informations provenant du système d'information médicalisé, n° 23, 10/05/1995.

[64] Arrêté du 22 juillet 1996 relatif au recueil et au traitement des données d'activité médicale, visées à l'article L. 710-6 du code de la santé publique, par les établissements de santé visés à l'article L. 710-16-2 du même code et à la transmission, visée à l'article L. 710-7 du code de la santé publique, aux agences régionales de l'hospitalisation, aux organismes d'assurance maladie et à l'Etat d'informations issues de ce traitement, JORF n° 173, 26/07/1996.

[65] Art. 34 de la loi n° 78-17 du 6 janvier 1978, *op. cit.,* dans sa version initiale.

[66] L'ATIH a été créée par le décret n° 2000-1282 du 26 décembre 2000 portant création de l'Agence technique de l'information sur l'hospitalisation et modifiant le code de la santé publique, JORF n° 301, 29/12/2000. Ce n'est qu'à partir de 2002 et du Décret n° 2002-1284 du 22 octobre 2002 relatif à l'organisation et au fonctionnement de l'Agence technique de l'information sur l'hospitalisation, modifiant le code de la santé publique, JORF, n° 250, 25/10/2002, que l'ATIH est véritablement entré en fonction.

l'accès direct aux données qu'il contient. Bien que ces données soient agrégées, l'accès a longtemps été plus souple[67] que ne l'était l'accès aux données du SNIIRAM élargi : ce que n'a pas manqué de soulever P.-L. BRAS dans son rapport[68] préalable à la réforme du 26 janvier 2016[69].

24. Désormais, le nouveau Système national des données de santé (SNDS) rassemble les données provenant du SNIIRAM, du PMSI, mais aussi d'autres sources[70]. Cette nouvelle base médico-administrative dispose de ses propres finalités prévues par décret[71] et sa mise en place a permis de définir un nouveau mécanisme d'accès uniformisé aux données de santé. Le fonctionnement de l'accès au SNDS est étudié en profondeur dans la présente étude afin de comprendre comment les enseignements tirés des modalités d'accès au SNIIRAM élargi ont été mis à profit pour inventer un système ouvrant (autant que faire se peut) l'accès aux données de santé en préservant le droit au respect de la vie privée.

25. Les données de santé sont désormais définies, tout comme les grandes bases de données médico-administratives dont il sera question dans notre étude. Il convient alors d'analyser les différentes catégories de données qui peuvent être des données de santé.

B) Les données de santé : des données multi-catégorielles

26. Les données de santé, nous l'avons déjà évoqué[72], peuvent traiter un large spectre d'informations. Cette particularité impose une catégorisation permettant de différencier la donnée de santé à caractère personnel (1) de la donnée de santé anonyme (2) mais aussi de la donnée publique de santé (3).

---

[67] L'accès aux données du PMSI a longtemps reposé sur le chapitre V ter de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 99-641 du 27 juillet 1999 *portant création d'une couverture maladie universelle, JORF*, n° 0172, 28/07/1999, devenu le chapitre X avec l'application de la 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.*

[68] BRAS P.-L., *op. cit.*, p. 35.

[69] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[70] *Infra* n° 160, 414 et 415.

[71] Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé », JORF n° 0301, 28/12/2016.

[72] S*upra* n° 13 à 15.

1) La donnée de santé à caractère personnel

27. La donnée de santé à caractère personnel doit être analysée sous trois aspects. Il est nécessaire d'appréhender la notion de donnée personnelle (a) avant de détailler les deux sous-catégories sous lesquelles elle peut être présentée. En effet, la donnée de santé à caractère personnel est souvent nominative (b) mais elle peut aussi être anonymisée[73] (c).

a) La donnée à caractère personnel

28. En droit français la donnée à caractère personnel, ou donnée personnelle, est identifiée depuis la loi relative à l'Informatique, aux fichiers et aux libertés (ou loi Informatiques et Libertés) du 6 janvier 1978[74].

29. Dans sa version initiale, la loi Informatique et Libertés dont l'objectif était de protéger les individus face à l'émergence de l'informatisation des informations, ne définissait pas directement la donnée personnelle. C'est la notion d'information nominative qui était mise en avant. Elle était alors définie ainsi : « *sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale* »[75]. Cette première définition de l'information nominative, devenue donnée personnelle, posait déjà des fondations solides en explorant la notion d'identification directe et indirecte des individus.

30. Aujourd'hui, après de nombreuses modifications, la loi Informatique et Libertés renvoie, dans son article 2, à la définition donnée par l'article 4 du Règlement général relatif à la protection des données : il s'agit de « *toute information se rapportant à une personne physique identifiée ou identifiable* ». Le Règlement ajoute que « *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*

[73] Seule une donnée de santé à caractère personnel peut faire l'objet d'une anonymisation. La donnée de santé anonyme, elle, ne présente pas de caractère personnel. C'est pour cette raison que la donnée de santé anonyme est évoquée dans un second temps, v. *infra* n° 40 à 43.

[74] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[75] *Ibid.*, article 4.

propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[76]. Cette définition actualisée de la donnée personnelle reprend les racines de 1978 tout en proposant des évolutions importantes. Le texte explicite en effet les composantes de l'information qui permet l'identification d'un individu. Dès lors, une donnée personnelle acquiert un double visage : elle peut être directement ou indirectement nominative.

31. Historiquement, le droit européen a mis un certain temps à s'emparer de la question de la donnée personnelle contrairement au droit français qui s'est intéressé à la question dès la fin des années 1970. Ce n'est qu'en 1995[77] qu'une directive a donné la première définition européenne de la donnée personnelle. Mais, en 1995, les géants de l'internet que sont aujourd'hui Google, Apple, Facebook, Amazon et Microsoft, aussi appelés GAFAM, n'existaient pas encore. Ces sociétés privées sont devenues spécialistes dans la captation et le traitement des données personnelles[78]. Face à ces nouvelles pratiques, les dispositions européennes sont vite apparues obsolètes[79]. Le Règlement européen de 2016 a donc été ressenti par certains comme un soulagement[80] : la nouvelle définition qui prévaut aujourd'hui embrasse un large spectre et témoigne de l'universalité des interrogations et enjeux qui entourent la donnée personnelle. Notons que, contrairement à la donnée qui est une notion plutôt délaissée par le droit, la donnée personnelle est, elle, encadrée avec beaucoup de précision.

b) Le caractère nominatif de la donnée personnelle

32. La donnée de santé à caractère personnel est par essence nominative[81]. C'est-à-dire qu'elle permet d'identifier nommément et directement l'individu auquel elle est rattachée. Historiquement, les professionnels de santé ont toujours été en contact avec les données de santé à caractère personnel de leurs patients. L'exigence du secret médical, représenté par le

[76] Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016, *op. cit.*, article 4, 1).

[77] Directive 95/46/CE du 24 octobre 1995, *op. cit.*, article 2 a).

[78] BEYNEIX I., « Le traitement des données personnelles par les entreprises : big data et vie privée, état des lieux », *JCP G*, 09/11/2015, n° 46-47, p. 2113-2119.

[79] KASTLER F., « Union Européenne, Protection des données de santé, une réforme attendue », « Focus », *Les tribunes de la santé*, 2013/1, n° 38, p. 11-20.

[80] MARINO L., « Le règlement européen sur la protection des données personnelles : une révolution ! » (PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 2016), *JCP G*, 30/05/2016, n° 22, p. 628.

[81] BRAS P.-L., *op. cit.*, encadré p. 29.

serment d'Hippocrate[82], permet aux individus de confier ces données sensibles sans craindre qu'elles ne soient divulguées. Ces données nominatives sont les plus aisées à catégoriser car elles tombent de fait sous le coup de l'article 2 et de l'article 8 de la loi Informatique et Libertés.

33. Une précision sémantique doit être apportée : le caractère nominatif d'une donnée personnelle n'est pas systématique. En effet, des données de santé à caractère personnel peuvent être indirectement nominatives : cela signifie que ces données permettent d'isoler un individu en faisant apparaître son nom et son prénom. Mais au-delà de la donnée à caractère personnel nominative se trouve un type voisin de donnée : la donnée à caractère personnel identifiante. Comme cela a été souligné[83], les bases de données de santé françaises regorgent de données personnelles de santé qui ne sont pas nominatives. Ces données conservent pourtant un caractère personnel car elles permettent d'identifier, directement ou indirectement, un individu sans le nommer. Ce sont des données directement ou indirectement identifiantes.

34. Une donnée à caractère personnel, si elle est principalement directement nominative, peut alors être indirectement nominative, voire directement identifiante ou indirectement identifiante. Bien que les notions de donnée nominative ou de donnée identifiante soient très proches et régulièrement confondues, il n'est pas inutile de savoir les différencier. Tout au long de l'étude, c'est la notion de donnée identifiante, qui inclut à la fois les données à caractère personnel nominatives et non nominatives, qui sera utilisée.

35. La donnée de santé à caractère personnel est donc soit nominative, soit identifiante. Mais il ressort des possibilités technologiques que ces données peuvent être traitées pour basculer dans une catégorie subsidiaire, à la marge de la donnée anonyme.

c) <u>L'anonymisation opportune de la donnée personnelle</u>

36. Une donnée anonymisée pourrait être définie comme une donnée nominative qui a fait l'objet d'un traitement la modifiant pour qu'elle devienne anonyme. Une donnée nominative,

[82] BERANGER J. et BOUADI R., « Approche éthico-juridique de l'usage des données médicales à caractère personnel », *Les Cahiers du numérique*, 2014/2, vol. 10, p. 93-123.

[83] DESMARAIS P., « Open data santé, un rapport décevant pour un retard de transposition certain ? », *JCP A*, 08/09/2014, n° 36, 716.

ou identifiante, perd ce caractère. Le terme pseudonymisation[84] est également utilisé pour désigner l'anonymisation d'une donnée. En 2007, la pseudonymisation était définie comme « *un traitement qui consiste à dissimuler l'identité* »[85]. Le règlement européen de 2016 indique, lui, que la pseudonymisation est la transformation d'une donnée à caractère personnel rendue anonyme « *de telle manière que la personne concernée ne soit pas ou plus identifiable* »[86]. Dès lors que la donnée à caractère personnel est correctement anonymisée ou pseudonymisée, le règlement européen considère qu'elle échappe aux principes relatifs à la protection des données : elle perd donc son caractère de donnée à caractère personnel.

37. Or, toute la difficulté réside dans l'évaluation du processus d'anonymisation. En effet, une donnée indirectement nominative ou identifiante[87] est une donnée à caractère personnel[88]. L'utilisation des technologies modernes peut aider à réidentifier une personne à partir de données pourtant anonymisées : la maxime « *l'anonymat est souvent imparfait et peut laisser transpirer l'identité* »[89] dévoile alors tout son sens. Le Règlement européen propose alors un faisceau d'indices[90] permettant de savoir si une donnée pseudonymisée est indirectement identifiante ou non. D'abord, pour savoir si l'individu est encore identifiable, même indirectement, « *il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique* ». Ensuite, pour déterminer si des moyens sont raisonnablement susceptibles d'être utilisés pour réidentifier un individu « *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* ».

---

[84] Le terme « pseudonymisation » a été utilisé dès l'année 2007 par le Groupe de travail « article 29 », composé de représentants des autorités nationales chargées de la protection des données, du Contrôleur Européen de la Protection des Données et de la Commission européenne, Avis 4/2007, *La protection des données sur le concept des données à caractère personnel*, 20 juin 2007, p. 19.

[85] Groupe de travail « article 29 », Avis 4/2007, *op. cit.*, p.19.

[86] Règlement 2016/679 du Parlement européen, *op. cit.*, Considérant 26 et article 4, 5).

[87] *Supra* n° 33 et 34.

[88] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, article 2 renvoyant à la définition donnée par l'article 4, 1), du Règlement 2016/679 du Parlement européen, *op. cit.*

[89] PICARD R., « La santé participative est pour demain », *Annales des Mines – Réalités industrielles*, 2010/4, p. 3.

[90] Règlement 2016/679 du Parlement européen, *op. cit.*, Considérant 26.

Cette procédure de certification de la bonne anonymisation d'une donnée personnelle témoigne de la complexité du procédé, mais aussi de la volatilité de la notion : une donnée correctement anonymisée aujourd'hui pourrait très bien, du fait des nouvelles possibilités offertes par les technologies, retomber dans la catégorie des données indirectement identifiantes demain, et donc redevenir une donnée à caractère personnel.

38. En France, les données de santé des individus sont bien souvent indirectement identifiantes et utilisent le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) devenu identifiant national de santé[91]. Leur utilisation en vue de recherches liées à la santé est donc soumise à un processus d'anonymisation strict qui peut donner lieu à la mise à disposition de jeux de données agrégées anonymes.

39. Les données anonymisées et pseudonymisées font donc l'objet d'une attention toute particulière en raison du risque de les voir devenir indirectement identifiantes ou nominatives.

2) La donnée de santé anonyme

40. Contrairement à la donnée de santé à caractère personnel qui est directement, ou indirectement identifiante, la donnée anonyme est, elle, totalement déconnectée de l'individu qui est potentiellement à l'origine de sa production. De la même manière, alors que la donnée personnelle est appréhendée par le droit et fait l'objet de nombreuses discussions quant à ses limites, notamment à travers la donnée anonymisée ou pseudonymisée, la donnée anonyme, elle, n'est définie par aucun texte juridique.

41. Une chose anonyme est une chose dont on ignore le nom, ou dont le propriétaire n'est pas connu[92]. Une donnée anonyme, serait donc une donnée dont on ignore tout de l'identité de l'individu qui en est à l'origine.

[91] Décret n° 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé, JORF n° 0075 du 29 mars 2017.

[92] Dictionnaire Petit Robert, édition 2017.

42. Les données de santé peuvent parfaitement être anonymes dès lors qu'elles ne concernent pas un individu[93]. Cependant, l'intérêt de l'étude est de traiter des enjeux de l'accès à des données anonymisées qui ont perdu leur caractère personnel. Il n'en demeure pas moins que les données de santé anonymes font pleinement partie du champ d'intérêt de la présente étude et concourent à l'alimentation des différentes réflexions envisagées.

43. Au-delà des données personnelles et des données anonymes se trouvent des données au caractère particulier : les données publiques.

3) La donnée publique de santé

44. Les informations publiques, qui deviennent des données à l'issue d'un traitement informatique spécifique[94], ont été définies par la loi portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, dite loi "CADA" (commission d'accès aux documents administratifs) comme étant « *les informations figurant dans des documents produits ou reçus par les administrations mentionnées l'article 1er, quel que soit le support, peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus* »[95]. Cette loi a été codifiée par ordonnance[96] dans le code des relations entre le public et l'administration, notamment à son livre III, entré en vigueur le 1er janvier 2016. L'article L. 300-2 dudit code propose une définition implicite remaniée des informations publiques qui sont « *quels que soient leur date, leur lieu de conservation, leur forme et leur support, les documents produits ou reçus, dans le cadre de leur mission de service public, par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission. Constituent de tels documents notamment les dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions et décisions* »[97].

---

[93] *Supra* n° 17.

[94] *Supra* n° 10 et 11.

[95] Article 10 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, dite loi "CADA" (Commission d'accès aux documents administratifs), JORF 18/07/1978.

[96] Ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration, JORF n° 0248, 25/10/2015.

[97] Article L. 300-2 du code des relations entre le public et l'administration.

Dans la continuité de la codification est venue la loi pour une République numérique[98] qui transpose la directive européenne de 2013 créant l'obligation pour les Etats membres de rendre disponibles les informations publiques et de les rendre réutilisables[99]. La loi vise alors à favoriser la circulation des données en ouvrant le plus largement possible les accès aux données publiques, dans le respect de la loi Informatique et libertés.

45. Le champ de la donnée publique de santé trouve sa limite dès lors qu'il existe un risque d'atteinte à la vie privée des individus. La Cour des comptes décrit parfaitement cette frontière en expliquant que les informations relatives, notamment, aux soins de ville et aux soins hospitaliers et qui sont contenues dans les bases de données médico-administratives, « *ne peuvent pas être considérées comme des informations publiques au sens de la « loi CADA »* » car elles sont « *de nature à porter atteinte à la vie privée ou au secret médical* […] *leur communication ne constitue donc pas un droit* »[100].

46. L'autre particularité de la donnée publique de santé est qu'elle peut provenir d'une myriade d'acteurs tels que l'Etat, les collectivités territoriales, toute autre personne de droit public ou les personnes de droit privé chargées d'une mission de service public. C'est donc à travers cette typologie de données que la question de l'accès aux données de santé sera traitée par l'étude.

Paragraphe 2 : La donnée de santé : une notion aux nombreux enjeux

47. L'accès aux données de santé conservées dans les bases médico-administratives est un sujet qui multiplie les enjeux. Cet accès semble être revendiqué comme un droit par une partie des acteurs qui y voient une source d'opportunités sans précédent, mais cet accès ne peut se faire au détriment du droit au respect de la vie privée et des droits et libertés fondamentaux (A). Outre le respect de mesures de sécurité qui sont intrinsèques à certaines catégories de données de santé[101], la question de la place des données de santé dans le monde actuel est tout autant cruciale (B) que celle des acteurs qui peuvent être amenés à y avoir accès (C). La structure de

[98] Loi n° 2016-1321 du 7 octobre 2016, *op. cit*.

[99] Directive 2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public.

[100] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 112

[101] *Supra* n° 27 à 39.

l'étude nous permettra d'aborder les problématiques soulevées par le sujet selon trois angles distincts (D).

A) Les données de santé entre transparence et vie privée

48. L'accès étendu aux données de santé est revendiqué comme un droit tant leur étude par le plus grand nombre promet de grandes avancées (1). Mais les limites opposées à cette transparence sont nombreuses et peuvent affaiblir l'ouverture des données de santé (2). L'ouverture des bases de données de santé est d'autant plus prudente que les textes ont été nombreux à se superposer ces dernières années, nécessitant un temps d'adaptation non négligeable (3).

1) Les opportunités de la transparence des données de santé

49. La réflexion qui entoure l'accès ouvert aux données de santé en France a été progressivement légitimée par la littérature, des rapports et des études sur les potentialités offertes. La revendication d'un accès aux données de santé s'est développée, dès les années 1990, dans le même temps que la naissance de la statistique publique en santé[102]. Le paragraphe 5 de la déclaration de Washington de l'Assemblée médicale mondiale sur les considérations éthiques concernant les bases de données de santé précisait dès 2002 que « *les progrès de la médecine et des soins de santé sont tributaires de l'assurance de qualité, des activités de gestion des risques et de la recherche, notamment des études épidémiologiques rétrospectives, qui se fondent sur les renseignements de santé des personnes, des communautés et des sociétés. Les bases de données sont de précieuses sources d'information lorsqu'elles sont utilisées* »[103]. Cette déclaration révisée pose désormais, à son paragraphe 8, le principe selon lequel « *la recherche et les autres activités en lien avec les bases de données de santé et les biobanques doivent contribuer au bénéfice de la société, en particulier aux objectifs de santé publique* ».

[102] Comme le note Jean-Marie JOB à la page 2 de son article « La loi "Informatique et libertés" et les données de santé », *Revue Lamy droit de l'immatériel*, 01/01/2008, n° 34, p. 86-94 : les premiers observatoires régionaux de santé sont nés en 1985, le Réseau national de santé publique est né en 1991 et a été transformé en Institut de veille sanitaire en 1998.

[103] Assemblée médicale mondiale, « Déclaration de l'AMM sur les considérations éthiques concernant les bases de données de santé et les biobanques » adoptée par la 53e Assemblée générale à Washington, Etats-Unis, en 2002 et révisée par la 67e Assemblée générale à Taipei, Taiwan, le 22/10/2016.

L'utilisation des bases de données de santé est donc considérée comme l'un des moyens incontournables pour améliorer nos sociétés modernes.

50. En France, dès 2008, des acteurs importants du système de santé, en l'occurrence il s'agissait des médecins qui s'exprimaient par la voix du Conseil national de l'Ordre des médecins[104], exposaient la nécessité de participer à la gouvernance des systèmes d'information en santé. Le simple fait d'être associé à la mise en place des systèmes permettant de stocker et d'échanger des données de santé devait permettre, selon l'Ordre des médecins, d'améliorer leur fonctionnement et, par conséquent, d'améliorer la qualité des soins.

Par ailleurs, la Cour des comptes s'inquiétait en mars 2016[105] de l'utilisation beaucoup trop restreinte des données de la principale base de données de santé en France : le SNIIRAM. Le fait que l'assurance maladie soit l'organisme qui détienne plus des trois quarts des habilitations est le signe d'une sous-utilisation des données de santé disponibles. La Cour estimait alors que « *l'Etat se prive ainsi d'un outil précieux pour le pilotage du système de santé* ». Au-delà du pilotage du système de santé, qui pourrait générer des économies substantielles si les données étaient utilisées au maximum de leurs capacités, c'est la santé publique (au travers du suivi de la population, de la pharmacovigilance, de la recherche) et la qualité des soins (par l'étude des pratiques professionnelles, l'évaluation des politiques de santé publique) qui sont touchées par le manque d'ouverture des données de santé. D'autres auteurs voient aussi dans l'étude des données de santé une opportunité de produire des documents de recherche sur la population française, notamment à travers les inégalités sociales de santé[106]. Des exemples de recherche ont ainsi été produits pour démontrer toutes les potentialités offertes par les données de santé contenues dans les bases de données administratives.

51. A l'international, les bénéfices attendus par l'utilisation des données de santé sont aussi mis en avant comme en témoigne l'étude rendue par l'OCDE en mai 2013 dans laquelle on pouvait lire : « les données de santé représentent une ressource considérable dans la plupart des

[104] SMALLWOOD O., « L'amélioration de la qualité des soins par le truchement de l'informatisation de la santé », *RDS*, 2008, n° 25, p. 622-624.

[105] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 74.

[106] DUCROS D., NICOULES V., CHEHOUD H., BAYLE A., SOUCHE A., TANGUY M., VALIERE J.-P., CAYLA F., GROSCLAUDE P., « Les bases médico-administratives pour mesurer les inégalités sociales en santé », *Santé Publique*, 3/2015, Vol. 27, p. 383-394.

pays de l'OCDE et il existe une logique économique et éthique à utiliser ces données autant que possible »[107]. Le rapport de la Commission open data en santé propose à ce titre un document très intéressant[108] qui établit un panorama international de l'ouverture des bases de données en santé. Une quinzaine de pays sont ainsi répertoriés parmi lesquels se trouvent le Royaume-Uni, les Etats-Unis, le Canada, le Danemark ou encore Singapour. Tous les Etats relevés se sont lancés dans une réforme de l'ouverture de leurs données de santé entre 2009 et 2013, la France est donc légèrement en retard sur ce mouvement. Le rapport souligne que les pays qui agissent en faveur de l'ouverture des données de santé peuvent avoir plusieurs approches. Il s'agit pour le Danemark ou le Canada de favoriser l'information du patient sur le système de soins. Du côté du Royaume-Uni et des Etats-Unis, l'accent est plutôt mis sur l'autonomisation du patient au cours de son parcours de soins. D'une toute autre manière, Singapour pousse à une réutilisation des données de santé en proposant un meilleur accompagnement. Chaque Etat est donc maître de l'impact qu'il souhaite donner à l'ouverture de ses bases de données en santé. Les usages qui seront faits des données de santé en France dans les années à venir seront alors très intéressants à analyser.

52. Les « biens-faits » de l'accès ouvert aux données de santé sont très fortement connotés par la notion d'intérêt général tant du point de vue de la gestion du système de santé, et donc de son économie, que de celui de l'amélioration de la santé publique et du parcours du patient. Les défenseurs de cette transparence tant convoitée déplorent notamment depuis plusieurs années que si les données de santé sont inaccessibles en France, c'est en partie dû à un manque d'offre en matière de systèmes d'informations performants et respectueux des exigences légales et réglementaires[109]. Les bénéfices pouvant être tirés d'une utilisation vertueuse des données de santé seraient alors retardés par l'absence d'offre technologique adaptée.

Toute la difficulté du processus d'ouverture et de partage des données de santé, à laquelle semble vouloir répondre la loi du 26 janvier 2016[110], résidera dans l'évolution des usages et dans la compatibilité du système avec les exigences légales et réglementaires. Pour certains

[107] OCDE, « Strengthening health information infrastructure for health care quality governance, Good Practices, New Opportunities and Data Privacy Protection Challenges », *OECD Health policy Studies*, 2013.

[108] V. l'annexe 7 du rapport de la Commission open data en santé du 9 juillet 2014, p. 86.

[109] BOURRET R., DEBOST C., MARTINEZ E., VIALLA F., « Lorsque le respect des droits fondamentaux l'emporte [encore] sur la quête de la performance », *RDS*, 2014, n° 57, p. 864-868.

[110] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

auteurs, cette compatibilité est capitale et il « semble indispensable – car l'enjeu éthique est sociétal est de taille –, de trouver un accord entre le droit des personnes concernées (patients ou non) et les besoins des professionnels de santé (soin ou recherche) »[111]. Mais si un tel accord est difficile à obtenir, c'est en raison des nombreuses limites qui sont posées à l'ouverture des données de santé, même dans un cadre contrôlé par la loi.

2) Les risques de la transparence des données de santé

53. La volonté d'ouverture des données de santé en France est accompagnée de nombreux signaux d'alertes quant à la protection des droits et libertés fondamentaux. Ainsi l'auteure J. BOSSI se demandait, dès 2010, « *comment garantir aujourd'hui, alors que se développent des projets nationaux d'envergure comme le dossier médical personnel, la confidentialité des données de santé personnelles* »[112].

54. Cette notion de donnée personnelle a avant tout émergé pour permettre d'assurer la protection du respect de la vie privée. Le concept de vie privée, tel que nous le connaissons, est apparu à la fin du XVIIIe siècle comme s'accordent à le dire sociologues[113] et historiens[114]. Pour les historiens, c'est plus précisément à partir de 1789 que la vie privée a émergé pour prendre son essor au XIXe siècle. Qualifié de phénomène social[115], la vie privée a d'abord été saisie par le droit pénal en deux temps : d'abord indirectement[116] au début du XIXe siècle, puis directement par la loi sur la presse en 1868[117]. En l'absence de dispositions légales équivalentes en droit civil, le juge a dû innover en proposant une jurisprudence de circonstance : la première à véritablement protéger la vie privée est un jugement interdisant à un peintre de reproduire l'image d'une célèbre tragédienne sur son lit de mort[118]. Il est reconnu que la notion particulière

[111] BERANGER J. et BOUADI R., « Approche éthico-juridique de l'usage des données médicales à caractère personnel », *Les Cahiers du numérique*, 2014/2, vol. 10, p. 93-123.

[112] BOSSI J., « Comment organiser aujourd'hui en France la protection des données de santé », *RDSS*, 01/03/2010, n° 2, p. 208.

[113] PARDAILHE-GALABRUN A., « La naissance de l'intime », *PUF*, 1988, 528 p.

[114] ARIES P. et DUBY G. (ss. dir. de), « Histoire de la vie privée », *Seuil*, 1999, 640 p.

[115] SAINT-PAU J.-C., « Droit au respect de la vie privée. Définition conceptuelle du droit subjectif », *Jurisclasseur Communication*, Fascicule 34, 2016.

[116] Loi du 26 mai 1819 relative aux crimes et aux délits commis par la voie de presse ou par tout autre moyen de communication, article 20.

[117] Loi du 11 mai 1868 sur la presse, article 11.

[118] T. civ. Seine, 16 juin 1858, DP, 1858, jurisprudence, p.62.

de droit au respect de la vie privée est née en 1890 du travail de deux avocats américains de Boston qui ont inventé le « *right of privacy* »[119]. Le droit américain a alors proposé une déclinaison du droit au respect de la vie privée en quatre catégories de torts : « *l'intrusion physique ou autre dans l'intimité d'une personne, le fait de présenter quelqu'un sous un jour faux (false light privacy), la révélation de faits de nature privée en l'absence d'intérêt légitime du public et l'utilisation de l'image dans un but commercial* »[120]. Toujours est-il que proposer une liste exhaustive des éléments qui relèvent de la vie privée, et donc de sa protection, n'aurait qu'un intérêt relatif tant ses composantes sont vastes[121]. La vie privée serait alors composée d'actions qui relèvent de la sphère personnelle : ce qui relève de l'identité (nom, adresse physique, adresse électronique, géolocalisation, numéros de sécurité sociale, de téléphone, informations sur le patrimoine), ce qui relève de l'intimité (qu'elle soit physique, corporelle, ou spirituelle et morale, relative à la génétique, à la santé, à la famille comprenant ainsi les enfants, les liens de parenté, les relations amicales). Tous les sujets dits dérivés comme le domicile, les correspondances, l'image de l'individu ou même sa voix[122] entrent aussi dans le champ de la vie privée[123].

55. *A fortiori*, cette protection de la vie privée ne découle pas naturellement de la Constitution. En effet, l'étude du bloc de constitutionnalité[124] français indique que la protection des données personnelles et de la vie privée n'est pas abordée explicitement[125]. Pourtant, la Convention de sauvegarde des droits de l'homme et des libertés fondamentales[126], dite CEDH, précise, à son article 8, que « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ». Cette protection a d'abord été édictée pour « *prémunir la personne*

[119] WAREN S. D. et BRANDEIS L. D., « The Right To Privacy », *Harward Law review,* vol. 4, 1890, P192-220.

[120] PROSSER William L., « Privacy », California Law Review 383, vol. 48, august 1960.

[121] CEDH, 8 janvier 2009, n° 29002/06, Schlumpf c/ Suisse, §100 : « la notion de « vie privée » est une notion large, non susceptible d'une définition exhaustive ».

[122] CADOUX L., « Voix, image et protection des données personnelles / Commission nationale de l'informatique et des libertés », *la Documentation française*, 1996, 119 p.

[123] SAINT-PAU J.-C., *op. cit.*

[124] Le bloc de constitutionnalité écrit comprend la Constitution du 4 octobre 1958, la Déclaration des droits de l'Homme et du citoyen du 26 août 1789, le préambule de la Constitution du 27 octobre 1946 et la Charte de l'environnement du 24 juin 2004.

[125] BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé*, 9 juillet 2014, p. 14.

[126] Convention de sauvegarde des droits de l'homme et des libertés fondamentales ou Convention européenne des droits de l'homme du 4 novembre 1950, entrée en vigueur le 3 septembre 1953, ratifiée par la France le 3 mai 1974.

contre les ingérences arbitraires des pouvoirs publics »[127] mais avec l'essor des nouvelles technologies et de la numérisation des informations, elle prend un tout autre sens aujourd'hui et va bien au-delà des seuls pouvoirs publics. En outre, le Conseil de l'Europe, par la convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[128], affirme dans son préambule « *qu'il est souhaitable d'étendre la protection des droits et des libertés fondamentales de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisé* ». Cette déclaration est considérée[129] comme une application des principes édictés par l'article 8 de la CEDH précité.

56. C'est seulement à partir de 1995 que le Conseil constitutionnel, par sa jurisprudence, a souhaité rattacher le droit au respect de la vie privée au bloc de constitutionnalité, sans toutefois en faire un principe fondamental reconnu par les lois de la République[130]. Une première décision du 18 janvier 1995[131] a conduit le Conseil constitutionnel à reconnaître, pour la première fois, que « *la méconnaissance du droit à la vie privée peut être de nature à porter atteinte à la liberté individuelle* ».

57. Or, la liberté, qu'elle soit individuelle ou non, fait partie des 4 « *droits naturels et imprescriptibles de l'Homme* » énoncés par l'article 2 de la Déclaration des droits de l'Homme et du citoyen (DDHC) qui fait partie intégrante du bloc de constitutionnalité. S'en sont suivies 3 autres décisions[132] rendues au cours de l'année 1999 qui sont bien plus explicites[133] dans le

---

[127] BABUSIAUX C., BREAS L., ESLOUS L., THOUVENIN D., *Rapport, L'accès des assureurs complémentaires aux données de santé des feuilles de soins électroniques, op. cit.*, p. 26.

[128] Convention n° 108-81 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, entrée en vigueur le 1er octobre 1985.

[129] BABUSIAUX C., BREAS L., ESLOUS L., THOUVENIN D., *Rapport, L'accès des assureurs complémentaires aux données de santé des feuilles de soins électroniques, op. cit.*, p. 44.

[130] BRAIBANT G., *Données personnelles et société de l'information : transposition en droit français de la directive n° 95-46 / rapport au Premier Ministre*, la Documentation française, 1998, p. 20.

[131] Conseil constitutionnel, décision n° 94-352 DC du 18 janvier 1995 *relative à la loi d'orientation et de programmation relative à la sécurité*, JORF n° 18, 21/01/1995.

[132] Conseil constitutionnel, décision n° 99-416 DC du 23 juillet 1999 *relative à la loi portant création d'une couverture maladie universelle*, JORF n° 172, 28/07/1999 ; Conseil constitutionnel, décision n° 99-419 DC du 9 novembre 1999 *relative à la loi relative au pacte civil de solidarité*, JORF n° 265, 16/11/1999 ; Conseil constitutionnel, décision n° 99-422 DC du 21 décembre 1999 *relative à la loi de financement de la sécurité sociale pour 2000*, JORF n° 302, 30/12/1999.

[133] BABUSIAUX C., BREAS L., ESLOUS L., THOUVENIN D., *Rapport, L'accès des assureurs complémentaires aux données de santé des feuilles de soins électroniques, op. cit.*, p. 24.

lien qui existe entre le droit au respect de la vie privée et l'article 2 de la DDHC : « *considérant qu'aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen : « le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression » ; que la liberté proclamée par cet article implique le respect de la vie privée* ». Plus de dix ans après ces trois décisions importantes, le Conseil constitutionnel s'est également prononcé directement sur le droit à la protection des données personnelles découlant du droit au respect de la vie privée par une décision du 22 mars 2012[134] : « *la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée ; que, par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif* ». Le Conseil constitutionnel, par sa jurisprudence, a donc pris soin de défendre le droit au respect de la vie privée et à la protection des données personnelles en les liant explicitement au droit fondamental qu'est la liberté.

58. La notion de la protection des données de santé qui, dès lors qu'elles sont réidentifiantes, même indirectement, ont un caractère sensible, ne s'est officiellement insérée dans le corpus juridique qu'avec la directive européenne de 1995[135] et son article 8 qui dresse la liste des données dont le traitement est, en principe, prohibé. Soulignons ici que ledit article 8 vise les « *données relatives à la santé* » sans faire de distinction entre les données à caractère personnel et les autres. Dans l'attente de la transposition de cette directive[136], la seule référence au traitement des données de santé dans le droit français était contenue dans les chapitres V bis, puis ter de la loi relative à l'informatique et aux libertés[137] qui développaient les conditions dans lesquelles des données de santé nominatives, et plus tard[138] à caractère personnel, pouvaient être traitées.

---

[134] Conseil constitutionnel, décision n° 2012-652 DC du 22 mars 2012 *relative à la loi relative à la protection de l'identité*, JORF n° 0075, 28/03/2012.

[135] Directive 95/46/CE 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 des données*.

[136] La transposition aura lieu tardivement en France avec 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.*

[137] Loi n° 78-17 du 6 janvier 1978 *op. cit*., dans sa version antérieure à la loi n° 2004-801 du 6 août 2004, *op. cit*.

[138] V. chapitre V bis de la loi n° 78-17 du 6 janvier 1978 *op. cit*., créé par la loi n° 94-548 du 1 juillet 1994 *relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi*

59. Prévu par l'article 9 du Code civil[139], et consacré comme principe à valeur constitutionnelle depuis la signature de la Convention européenne des droits de l'homme[140], le principe du droit au respect de la vie privée a été adapté, en France, à la technologisation du monde par l'article 1er de la loi Informatique et Libertés qui précise à ce sujet que « *l'informatique […] 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* »[141]. Le même article précise que les personnes disposent de « *droits* […] *de décider et de contrôler les usages qui sont faits des données à caractère personnel les concernant* ». L'individu semble alors prioritaire lorsqu'il s'agit du contrôle de ses données personnelles numérisées, dans les limites fixées par la loi.

60. Cette protection est d'autant plus accrue lorsqu'il s'agit de données personnelles dites sensibles[142]. La loi interdit tout simplement, par principe, le traitement de « *données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter 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* ». Tous ces sujets sont intimement liés à la vie privée de chaque individu[143]. Les données sensibles sont considérées comme des données relatives à la vie privée tellement liées à l'intimité d'une personne que, sauf disposition contraire, il est formellement interdit de les recueillir.

---

n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF*, n° 152, 02/07/1994, et chapitre V ter de la loi n° 78-17 du 6 janvier 1978 *op. cit*., créé par la loi n° 99-641 du 27 juillet 1999 *portant création d'une couverture maladie universelle*, *JORF*, n° 0172, 28/07/1999.

[139] Code civil, article 9, « *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* ».

[140] Convention de sauvegarde des droits de l'homme et libertés fondamentales du 4 novembre 1950.

[141] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, article 1.

[142] *Ibid.*, article 6, modifié par l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[143] Commission européenne, *Avis n° 13 du 30 juillet 1999 : Aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information*, Journal international de bioéthique, 2001/3, vol. 12, p. 113-117 : « *Les données personnelles de santé sont partie intégrante de la personnalité de l'individu qu'elles concernent* ».

61. La question de la protection de la vie privée est ainsi la principale source de craintes lorsqu'il s'agit de l'accès aux données de santé. Avant la réforme qui a mené à la création du système national des données de santé en 2016, les réflexions sur la place à donner au principe de libre réutilisation des données publiques étaient nombreuses alors que la maîtrise des données de santé contenues dans les bases de données administratives était incertaine. En réalité ce n'est pas tant l'ouverture des données de santé qui est questionnée mais plutôt les modalités de cette ouverture[144].

Plusieurs interrogations se posent ainsi sur la sécurisation des données de santé une fois mises à dispositions, mais aussi sur le contrôle qu'il est fait du traitement réservé à ces données une fois acquises par le demandeur d'accès. Dans son rapport remis en 2016[145], la Cour des comptes émet à ce sujet de sérieux doutes quant à la capacité de la CNIL à contrôler *a posteriori* les acteurs qui accèdent aux données de santé. Ces doutes s'étendent également à la capacité du nouveau système appelé SNDS ou Système national des données de santé, à permettre l'examen, dans les temps impartis et avec la même rigueur, de toutes les demandes d'accès aux données de santé. Le dilemme est puissant : jusqu'à la réforme, l'ouverture des données de santé était très limitée au nom du droit au respect de la vie privée car il n'existait pas de certitude quant à la capacité de l'administration à sécuriser les données mises à disposition. Désormais, la politique de transparence est bel et bien lancée avec pour seule garantie un encadrement légal et réglementaire dont la mise en pratique soulève autant de doutes, si ce n'est plus, que l'ancien système. Avant la réforme, la question était plutôt de savoir comment il était possible d'obtenir un accès aux données souhaitées. Aujourd'hui, cette question est plutôt tournée vers les acteurs « rouages » du SNDS et sur leur capacité à faire fonctionner, de manière sereine, l'édifice.

62. L'une des autres inconnues de l'accès aux données de santé, et plus précisément aux données personnelles de santé, réside dans son coût, tant pour l'administration que pour les demandeurs d'accès. En principe, cette réutilisation est gratuite depuis la loi du 17 juillet 1978, dite loi CADA[146], et codifiée depuis dans le livre III du code des relations entre le public et

[144] LAUDE A., « De quelques problématiques relatives à l'ouverture des bases de données en santé », *JDSAM*, Chronique 2, Droits des malades et bioéthique, 01/07/2014, n° 3, p. 30 à 34.

[145] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit*., p. 105.

[146] Loi n° 78-753 du 17 juillet 1978, *op. cit.*

l'administration. Le code de la santé publique[147] indique d'ailleurs que les données du SNDS mises à disposition du public sont accessibles gratuitement. Cependant, avant d'être rendues accessibles par l'administration, les données personnelles de santé doivent subir un traitement destiné à les rendre anonymes ou non réidentifiantes. Cette opération justifie, d'après l'article L. 324-1 du code des relations entre le public et l'administration modifié par la loi pour une République numérique[148], l'établissement d'une redevance : ce que confirme la Cour des comptes ans son rapport[149]. Par conséquent, l'accès sur demande à des données personnelles de santé du SNDS a de grandes chances de faire l'objet d'une redevance. L'existence aléatoire de ce type de redevance a notamment été souligné dans le rapport TROJETTE en 2013 qui remarque une diversité de redevances variées, plus ou moins bien justifiées. La question du coût de la transparence des données de santé, tant pour l'administration qui les met à disposition que pour les acteurs qui veulent y accéder fait donc partie intégrante du débat.

3) La transparence des données de santé affectée par la succession des réformes

63. La réforme de l'accès aux données de santé[150] contenues dans les bases médico-administratives a entièrement remis à plat le fonctionnement d'un système imaginé il y a une vingtaine d'années. L'objectif clairement affiché était de rendre accessible le plus grand nombre de données de santé possible, dans le respect de la vie privée des individus, par des techniques d'anonymisation irréversible associées à des procédures revues pour être plus simples à comprendre et plus rapides à mettre en œuvre. Une telle réforme est, à elle seule, déjà lourde à appréhender comme nous allons le comprendre dans les développements de cette étude. Pourtant elle a été suivie de plusieurs autres textes qui ont apporté des modifications substantielles aux conditions d'accès aux données.

[147] V. article L. 1461-2 du code de la santé publique : « *Les données du système national des données de santé qui font l'objet d'une mise à la disposition du public sont traitées 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. Ces données sont mises à disposition gratuitement. La réutilisation de ces données ne peut avoir ni pour objet ni pour effet d'identifier les personnes concernées.* »

[148] Loi n° 2016-1321 du 7 octobre 2016, *op. cit.*

[149] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit*., p. 112.

[150] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

64. Nous l'avons déjà présenté dans cette introduction, le Règlement général relatif à la protection des données[151] a été voté le 27 avril 2016 en vue d'une entrée en vigueur le 25 mai 2018. Ce Règlement a harmonisé, pour l'ensemble des pays de l'Union européenne, un socle juridique commun relatif à la protection des données : les données de santé à caractère personnel y figurent en bonne place. Alors même qu'un Règlement européen est d'application directe en droit national et ne nécessite pas que les Etats membres votent une loi de transposition, la France a souhaité adopter une loi pour adapter le texte de la loi relative à l'informatique et aux libertés[152] au nouveau droit européen : c'est la loi du 20 juin 2018[153].

65. Cette réforme a réécrit en grande partie les dispositions de la loi relative à l'informatique et aux libertés[154], notamment celles qui concernent la procédure d'autorisation préalable nécessaire à l'accès et au traitement des données de santé issues des bases médico-administratives. En effet, le chapitre IX[155] relatif aux « *Traitements de données à caractère personnel dans le domaine de la santé* » se trouvait découpé en deux sections distinctes, la première instaurant des règles générales, la seconde entièrement dédiée aux « *traitements à des fins de recherches, d'études ou d'évaluation dans le domaine de la santé* ». Tous les acteurs souhaitant accéder à des données de santé issues du nouveau SNDS pour les traiter ont donc dû s'adapter à cette structure mise à jour du texte de loi, quelques semaines seulement après l'entrée en vigueur du Règlement européen.

66. Si nous pensions que la révision des dispositions relatives aux données personnelles s'arrêterait à ce stade, nous avions tort. Le Gouvernement a pris une ordonnance le 12 décembre 2018[156] afin de réécrire intégralement la loi relative à l'informatique et aux libertés : nouvelles numérotations, nouvelles références au Règlement européen, et surtout, nouvelle structure. Alors que l'ancienne version du texte comptait 72 articles, la nouvelle rédaction en compte 128 : la loi a donc quasiment doublé de volume. Nous sommes bien loin de la simplification législative mise en avant lorsque la réforme créant le SNDS a été votée en janvier 2016. En

[151] Règlement 2016/679 du 27 avril 2016, *op. cit*.

[152] Loi n° 78-753 du 17 juillet 1978, *op. cit.*

[153] Loi n° 2018-493 du 20 juin 2018 *relative à la protection des données personnelles*, JORF n° 0141 du 21/06/2018.

[154] Loi n° 78-753 du 17 juillet 1978, *op. cit.*

[155] Loi n° 78-753 du 17 juillet 1978, *op. cit.*, modifiée par la loi n° 2018-493 du 20 juin 2018, op. cit., chap. IX.

[156] Ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

effet, la réécriture de la loi relative à l'informatique et aux libertés par ordonnance entraine la modification subséquente du décret précisant les modalités réglementaires d'accès aux données de santé à des fins de recherche dans le domaine de la santé. La publication de ce décret, avant le 1er juin 2019, est une condition *sine qua non* à l'entrée en vigueur de l'ordonnance.

67. Les acteurs qui entendent accéder aux données de santé du SNDS pour effectuer une recherche ont donc dû s'adapter à tous les changements légaux et réglementaires depuis la création du nouveau système. Cette instabilité est très inconfortable sur un sujet aussi sensible que le traitement des données de santé. Dans la pratique, il y a fort à espérer que l'activité du législateur en la matière retourne en eaux calmes après la parution du décret tant attendu.

B) Les données de santé au cœur du monde numérique moderne

68. La question du contrôle des données de santé et de leur ouverture s'est accentuée ces dernières années d'une part en raison du mouvement dit d'*open data*, littéralement « données ouvertes », qui s'est développé à travers le monde et en France (1), d'autre part avec le développement du *big data* et des technologies liées à l'économie numérique qui sont indissociables du monde moderne (2).

1) La revendication d'un open data en santé

69. L'*open data*[157] est un concept traduit par la commission de terminologie de l'Académie française par les mots « *données ouvertes* »[158]. Une définition plus développée, mais peut être sujette à plus d'interprétations, a été donnée par la Commission open data en santé en 2014 : les données ouvertes seraient alors « *l'ouverture et le partage de données par leur mise en ligne dans des formats ouverts, en autorisant la réutilisation libre et gratuite par toute personne* »[159]. L'idée principale qui ressort de ces deux traductions indique la nécessité d'un accès libre et ouvert aux données concernées.

[157] Nous utiliserons la traduction française de cette notion, « données ouvertes », à travers la présente étude.

[158] Traduction proposée par la Commission générale de terminologie et de néologie de l'Académie française et inscrite au Journal officiel, texte n° 107, *JORF*, n° 0103, 03/05/2014. Le texte les définit comme étant des « *données qu'un organisme met à la disposition de tous sous forme de fichiers numériques afin de permettre leur réutilisation* ».

[159] BURNEL P. et VON LENNEP F., *op. cit.*, p. 9.

70. Le concept de données ouvertes s'est développé dans un contexte d'informatisation du monde qui a conduit à la multiplicité des données produites et récoltées dans des bases de données[160]. Ces bases de données étant, pour la plupart, fermées, c'est logiquement que des voix se sont progressivement élevées pour en demander l'ouverture. C'est relativement tôt, en 1966, que la revendication d'une ouverture des bases de données scientifiques a vu le jour aux Etats-Unis[161]. Plus tard c'est une publication[162] datant de 1995 du National Research Council américain qui revendiquait le libre accès et la libre réutilisation des données géophysiques et environnementales disponibles. Plus récemment, la Déclaration internationale sur le libre accès aux archives de Budapest[163], et la Déclaration de Berlin[164] ont porté la question des données ouvertes du côté des bases de données administratives. Saisie par le droit européen[165] et par le droit français[166], l'ouverture des bases de données administratives est devenue un objectif à atteindre dans tous les domaines.

71. S'agissant des données de santé, l'idée d'une ouverture des bases de données s'est beaucoup manifestée et a vécu un regain d'intensité du côté de l'administration[167] comme de celui des demandeurs d'accès[168]. Les différents travaux précédant la loi santé du 26 janvier 2016 ont d'ailleurs beaucoup fait penser que le principe des données ouvertes s'annonçait[169] en santé. Mais, comme l'étude le montrera, telle n'a pas été la voie choisie.

---

[160] Selon le dictionnaire Le Petit Robert, édition 2017, une base de données est un ensemble de données logiquement reliées entre elles et accessibles au moyen d'un logiciel spécialisé.

[161] *The Educational Resources Information Center* (ERIC) créé en 1966 est la première initiative visant à créer une base de données bibliographiques électronique en accès ouvert.

[162] *National Research Council*, « *On the Full and Open Exchange of Scientific Data* », 1995.

[163] Initiative de Budapest pour l'accès ouvert lancée lors du congrès des 1er et 2 décembre 2001 par les institutions les plus avancées dans le domaine des archives ouvertes et diffusée le 14 février 2002.

[164] Déclaration de Berlin sur le libre accès à la connaissance définie lors du congrès de Berlin du 22 octobre 2003 tenu à la société Max-Planck.

[165] Directive 2003/98/CE du 17 novembre 2003 concernant la réutilisation des informations du secteur public et Directive 2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public.

[166] Loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public, JORF n° 0301 du 29/12/2015.

[167] GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *Pour une meilleure utilisation des bases de données administratives et médico-administratives nationales pour la santé publique et la recherche*, 2012, 56 p.

[168] Initiative transparence santé, « Liberté pour les données de santé », *Manifeste*, 2013.

[169] DEBOST C., « Publication du rapport sur la gouvernance et l'utilisation des données de santé, la promesse d'un entrebâillement de l'Open data dans le secteur de la santé ? », *RDS*, janvier 2014, n° 57, p. 947 à 949 ; BURNEL

72. Les données ouvertes sont souvent assimilées, peut-être à tort, au concept de transparence. Or, il est important d'opérer une différence, ne serait-ce que sur le point sémantique. Avant de comprendre ce que peut induire la transparence des données de santé, il est nécessaire de s'intéresser au sens même de la transparence. Etymologiquement, le terme vient du latin *transparens* : *trans* signifiant « à travers » et *parens*, étant le participe présent du verbe *parere*, signifiant « paraître, apparaître »[170]. La transparence serait donc la possibilité pour une chose d'apparaître à travers une autre chose. S'agissant des données de santé, cela pourrait se traduire par la capacité de ces données à être visibles par les personnes qui sont extérieures aux bases qui contiennent ces données. Le dictionnaire donne, sur ce point, une définition plutôt appropriée et directement attachée à la transparence de la donnée : c'est le « caractère d'une donnée accessible à tous, en matière économique, politique, administrative… »[171]. Si l'alliance terminologique de la transparence et de la donnée est appréhendée par la langue française, le droit, lui, est plus limité sur la question.

73. En droit français, la transparence a été d'abord saisie par le droit fiscal. Il s'agit alors d'une transparence caractérisée par la « *situation au regard du fisc des sociétés qui sont réputées ne pas avoir de personnalité distincte de celle de leurs membres pour l'application des impôts directs, des droits d'enregistrement et des taxes assimilables* »[172]. La transparence est aussi évoquée dans le secteur marchand. La transparence d'un marché a alors vocation à rendre accessibles « *les informations relatives notamment aux prix de revient et aux conditions de vente qui y ont cours* »[173]. L'idée qui imprègne ces deux approches différentes de la notion de transparence est bien l'absence de barrière (qu'elle soit physique, règlementaire, technique…) entre des informations et les personnes susceptibles d'être directement intéressées. Mais le droit français n'explore pas plus la notion de transparence et il n'existe pas de mention directe du caractère transparent de la donnée, pas même dans la loi Informatique et Libertés.

P. et VON LENNEP F., *op. cit.*

[170] Dictionnaire de vocabulaire juridique Gérard CORNU, *PUF*, édition 2011.

[171] Dictionnaire Petit Robert, édition 2017.

[172] Dictionnaire de vocabulaire juridique Gérard CORNU, *op. cit*.

[173] *Ibid.*

74. Pourtant, dès la directive européenne de 1995[174], et notamment ses considérants 62 et 63, les autorités nationales de contrôle des traitements de données à caractère personnel se voyaient confier la mission de « *contribuer à la transparence du traitement de données effectué dans l'Etat membre dont elles relèvent* »[175]. Le droit européen s'est donc saisi en amont de la transparence s'agissant de la donnée. Le règlement européen de 2016 est venu insister sur la notion de transparence en proposant des références bien plus nombreuses, la transformant alors en un principe inamovible du traitement de la donnée à caractère personnel.

75. La transparence dans le domaine de la santé existe bel et bien en France car un site gouvernemental officiel porte ce nom depuis sa mise en ligne en 2014 : c'est le site « transparence santé »[176]. Ce site officiel permet à toute personne d'accéder aux informations relatives aux relations entre les entreprises privées et les acteurs du secteur de la santé. La page d'accueil précise que la transparence est « *une condition indispensable pour préserver la confiance* ». Les données alors proposées ne sont évidemment pas des données personnelles de santé mais sont bien des données relatives au secteur de la santé et précisément à celui du médicament. Cette base de données ouvertes concernant les liens entre l'industrie pharmaceutique et les professionnels du secteur de la santé peut s'interpréter comme le premier pas vers l'ouverture des données de santé en France.

76. Le mouvement d'ouverture des données de santé en France procède donc de ces deux notions très proches que sont les données ouvertes d'une part, et la transparence des données d'autre part. C'est en réponse à ces volontés que la loi Santé a été mise en œuvre.

2) Le big data en santé au service de l'économie numérique

[174] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[175] Directive 95/46/CE du 24 octobre 1995, *ibid.*, considérants 62 et 63 : « *considérant que l'institution , dans les États membres, d'autorités de contrôle exerçant en toute indépendance leurs fonctions est un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel ; considérant que ces autorités doivent être dotées des moyens nécessaires à l'exécution de leurs tâches, qu'il s'agisse des pouvoirs d'investigation et d'intervention, en particulier lorsque les autorités sont saisies de réclamations , ou du pouvoir d'ester en justice; qu'elles doivent contribuer à la transparence du traitement de données effectué dans l'État membre dont elles relèvent* ».

[176] V. site www.transparence.sante.gouv.fr créé par la loi n° 2011-2012 du 29 décembre 2011 *relative au renforcement de la sécurité sanitaire du médicament et des produits de santé*, JORF, n° 0302, 30/12/2011.

77. La dynamique des données ouvertes s'accompagne d'une technologisation incessante représentée ces dernières années par le *big data*[177]. Cet anglicisme désigne l'ensemble des données générées par les nouvelles technologies, caractérisées par leur volume colossal[178]. Traduit par les termes mégadonnées ou données massives[179], le *big data*[180] est défini par M. A. TROJETTE[181] comme un type de donnée à mettre dans une base ayant plusieurs millions d'entrées et nécessitant de très grandes capacités de calcul pour être traité : la caractéristique principale des données massives est que leur volume est gros, cela regroupe nécessairement des millions de données. Mais, pour d'autres, comme H. NABARETTE[182], l'une des caractéristiques essentielles des données massives est intrinsèquement liée à l'objectif d'usage de la donnée : l'objectif du procédé serait nécessairement de traiter les données et d'en tirer une information particulière.

78. Cette technique de traitement de données se caractérise donc par l'immensité des données disponibles et par l'usage qui va découler de cette collecte. Les données massives, si elles sont traitées de manière vertueuse, peuvent aboutir à des progrès très importants, comme le souligne J. RICHARD[183], que cela soit pour « *améliorer les politiques publiques, évaluer plus facilement les risques sanitaires ou encore optimiser les performances des entreprises* ». Certains y trouvent aussi des capacité prédictives[184] permettant d'anticiper des mouvements sociaux ou économiques. La place des données massives dans l'économie mondiale est primordiale avec, pour le simple marché français, une évaluation à 190 millions d'euros en 2015 pour atteindre

[177] BROUDOUX E., CHARTRON G., *Big data – open data : quelles valeurs ? Quels enjeux ? : actes du colloque "Document numérique et société"*, De Boeck supérieur, 2015, 282 p.

[178] Dictionnaire Le Petit Robert, édition 2017.

[179] Traduction proposée par la Commission générale de terminologie et de néologie de l'Académie française et inscrite au Journal officiel, texte n° 89, JORF, n° 0193, 22/08/2014. Le texte les définit comme étant des « *Données structurées ou non dont le très grand volume requiert des outils d'analyse adaptés* ».

[180] Nous utiliserons la traduction française de cette notion, « données massives », à travers la présente étude.

[181] Mohammed Adnène. TROJETTE a été magistrat à la Cour des comptes, il est notamment l'auteur du Rapport au Premier ministre*, Ouverture des données publiques. Les exceptions au principe de gratuité sont-elles toutes légitimes ?*, juillet 2013.

[182] Hervé NABARETTE est conseiller technique à la Direction de l'évaluation économique, médicale et de santé publique de la Haute Autorité de Santé.

[183] RICHARD J., « Le numérique et les données personnelles : quels risques, quelles potentialités ? », *RDP*, 01/01/2016, n° 1, p. 87-100.

[184] MARINO Laure, « Le big data bouscule le droit », *Revue Lamy droit de l'immatériel*, 01/12/2013, n° 99, p. 55-58.

un peu moins de 500 millions d'euros en 2017[185]. Ces données massives sont souvent désignées, à raison, comme le carburant de l'économie numérique : un véritable or noir du XXIe siècle[186].

79. Les opportunités offertes par les données massives sont très nombreuses mais sa maîtrise reste encore réservée à quelques entreprises, si bien qu'en 2013, un professeur américain lançait que le « *big data c'est comme le sexe chez les adolescents : tout le monde en parle, personne ne sait vraiment comment le faire, tout le monde pense que les autres le font, donc tout le monde prétend le faire* »[187]. La littérature sur le sujet oscille d'ailleurs bien souvent entre, d'une part, l'émerveillement devant les nouvelles possibilités et, d'autre part, les nouveaux risques qui courent sur les données et particulièrement sur les données personnelles. Les données massives sont ainsi souvent analysées comme un « *moyen très efficace pour percer l'anonymat des bases de données* »[188], autrement dit, pour réidentifier des individus grâce à des données anonymisées, voire pour les identifier avec des données anonymes. De nombreuses craintes portent sur la vie privée des individus et sur la capacité, ou l'incapacité[189], du droit à les protéger de tout usage frauduleux de leurs données.

80. Les craintes émises face au développement des données massives prennent tout leur sens lorsqu'il s'agit des données personnelles de santé. Les questionnements se sont ainsi multipliés après l'annonce d'une réforme du système d'accès aux données de santé en France. C. CASTETS-RENARD y voit un risque clair de réidentification des individus par des données de santé pourtant anonymisées et supposées être non réidentifiantes[190]. Les processus de croisement d'informations sont de plus en plus sophistiqués et des données qui étaient

---

[185] BEYNEIX I., *op. cit.*

[186] KALTENBACH L. et LE GUAY O., « Ces données personnelles qui valent de l'or », *JCP E*, 11/09/2014.

[187] Formule de Dan ARIELY, professeur de psychologie et d'économie comportementale à l'Université Duke, Caroline du Nord, janvier 2013.

[188] GORCE G. et PILLET F., Rapport d'information au Sénat, *La protection des données personnelles dans l'open data : une exigence et une opportunité*, 16 avril 2014, p. 49.

[189] MARINO L., *op. cit.*

[190] Comme le précise Céline CASTETS-RENARD dans les références de son article « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data », *Revue Lamy de Droit de l'Immatériel*, 01/10/2014, supplément au n° 108, p.38-45, différentes équipes de recherche dans le monde ont démontré la possibilité de réidentifier les individus à partir d'informations prétendument anonymisées. Cynthia DWORK, chercheuse chez Microsoft, a démontré en 2006 l'impossibilité d'assurer une protection complète des données dites « *sensibles* » (maladie, salaire, chiffre d'affaires d'une entreprise), dès lors que l'« attaquant » dispose d'informations annexes dites « *quasi identifiantes* » telles que l'âge, le lieu de résidence, le sexe... V. également : Jon P. Daries, Justin Reich, Jim Waldo, Elise M. Young, Jonathan Whittinghill, Daniel Thomas Seaton, Andrew Dean Ho, Isaac Chuang, Privacy, *Anonymity, and Big Data in the Social Sciences*.

correctement anonymisées il y a quelques années sont potentiellement réidentifiantes aujourd'hui. Tout l'enjeu est alors de réfléchir à un usage des données massives qui puisse bénéficier aux personnes tout en respectant leur vie privée. Bien conscients des questions qui restent en suspens, certains auteurs comme A. MENDOZA-CAMINADE pose d'emblée le fait que « *les régulations juridiques n'en sont qu'à leurs balbutiements* »[191], notamment dans la perception des données personnelles de santé produites par les objets connectés qui prolifèrent. Elle reconnait que « *le cadre juridique actuel est sans nul doute inadapté aux nouvelles évolutions numériques* ». Il est vrai que le phénomène du *quantified self*, littéralement, le soi quantifié, permet aux individus de produire et transmettre des données personnelles de santé directement à destination des entreprises privées propriétaires de l'objet connecté ou de l'application utilisée, ce qui soulève de nouvelles interrogations[192].

81. Les possibilités offertes par les données massives apparaissent donc comme une chance pour la société et un danger pour la protection des données personnelles. Cette technologisation des données a un impact inévitable sur le processus actuel d'ouverture des données en santé.

C) Les données de santé au centre de l'attention d'une multiplicité d'acteurs

82. L'intérêt suscité par les données de santé recueillies dans les bases médico-administratives françaises est immense. Cette convoitise est d'autant plus grande que les accès sont autorisés au compte-goutte alors qu'une multitude d'acteurs, aussi bien publics que privés sont intéressés. Ces acteurs peuvent être distingués en quatre catégories : les acteurs publics qui exercent une mission de service public dont le bon fonctionnement exercice suppose un accès aux données de santé autorisé par arrêté ou décret publié au Journal officiel ; les acteurs publics qui n'exercent pas une telle mission de service public ; les acteurs privés à but non lucratif ; et enfin les acteurs privés à but lucratif. Cette catégorisation des acteurs est née avec le deuxième arrêté pris pour la mise en œuvre du SNIIRAM en 2005[193]. Elle a perduré au fil des arrêtés

[191] MENDOZA-CAMINADE A., *op. cit.*

[192] V. notamment DESMARAIS P., « Quel régime pour la m-Health ? », *Communication Commerce Electronique*, 01/03/2013, n° 3, p. 15-18 ; MEURIS F., « Les dangers du "soi quantifié" », *Communication Commerce Électronique*, 01/07/2014, n° 7-8, p. 2-2 ; de SILGUY S., « Les objets connectés, un risque pour la protection de nos données personnelles », *RLDC*, 01/10/2014, n° 119, p. 66 à 69 ; LAUDE A., « Introduction au colloque : Applis smartphone et santé : promesses et menaces », *JDSAM*, 01/12/2014, p. 3-4 ; DREYFUS N., « Jusqu'où aller dans la collecte des données de santé ? », *L'Usine nouvelle*, n° 3405, semaine du 8 au 14 janvier 2015, p. 48.

[193] Arrêté du 20 juin 2005 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance*

successifs[194] et la réforme mise en œuvre par la loi de modernisation de notre système de santé n'a pas apporté d'approche réellement différente.

83. La première catégorie d'acteurs est celle des acteurs publics dont la mission nécessite un accès à certaines données de santé, voire à toutes les données de santé. Ce sont les seuls à avoir un accès permanent aux données contenues dans la base SNIIRAM. Dans son rapport de 2016, la Cour des comptes analyse que seulement dix organismes avaient un accès permanent au SNIIRAM en 2001 contre 25 en 2015[195]. Et parmi ces derniers seulement sept ont un accès aux données de santé individuelles exhaustives : ce sont les caisses d'assurance maladie obligatoire (Caisse Nationale d'Assurance Maladie des Travailleurs Salariés, Caisse Centrale de la Mutualité Sociale Agricole et Régime Social des Indépendants devenu Sécurité Sociale des Indépendants), la Caisse nationale de solidarité pour l'autonomie (CNSA), l'Institut de veille sanitaire (INVS), l'Agence nationale de sécurité et du médicament (ANSM) et la Haute autorité de santé (HAS). Bon nombre d'autres acteurs publics exercent une mission qui nécessite un accès permanent à certaines données de santé, comme l'Institut national de la santé et de la recherche médicale (INSERM), l'Agence de la biomédecine (ABM) ou encore l'Agence technique de l'information hospitalière (ATIH). Mais ces derniers acteurs n'ont accès qu'à l'échantillon généraliste des bénéficiaires (ou EGB)[196]. Ne serait-ce que dans cette première catégorie d'acteurs, les nouvelles revendications et sollicitations pour accéder en permanence aux données de santé doivent indéniablement créer des tensions entre ceux qui ont accès à l'ensemble des données, et ceux qui n'ont accès qu'à un échantillon.

84. Face à ces acteurs publics qui bénéficient d'un accès permanent, la majorité des autres acteurs publics sont soumis à une procédure d'accès sur demande. Les centres hospitaliers universitaires[197] (CHU) mais aussi tous les chercheurs travaillant dans des organismes tels que des laboratoires de recherche, des universités, sont tenus de suivre une procédure très stricte

maladie, JORF, n° 192, 19/08/2005.

[194] Depuis le 1er arrêté relatif au SNIIRAM pris en 2002, des arrêtés relatifs à la mise en œuvre du système national d'information interrégimes de l'assurance maladie ont été pris en 2005, 2006, 2008, 2011, 2012, 2013, 2014 et 2016.

[195] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 52.

[196] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *ibid.*, p. 53.

[197] D'après le rapport remis au Parlement par l'Institut des données de santé en 2015, 40% des 149 demandes d'utilisation des données approuvées de 2009 à 2015 proviennent des CHU, Institut des données de santé, « Ouverture, qualité, partage : des avancées », Rapport au Parlement, 2015, p. 27.

pour obtenir quelques données de santé sur lesquelles travailler. Ces acteurs publics, que nous pouvons qualifier d'ordinaires de par la nécessité de suivre la procédure « classique » d'accès aux données de santé, sont très demandeurs d'informations détaillées et peuvent se sentir relativement frustrés lorsque ceux qui bénéficient d'un accès permanent ne font aucun usage de ce privilège[198]. Ce constat d'un accès permanent qui existe et qui n'est pas utilisé par ses bénéficiaires, allié à la difficulté de faire aboutir une demande d'accès aux données a découragé plus d'un acteur public ordinaire. Ainsi, à la fin 2010, l'Institut des données de santé[199] (IDS) dernièrement remplacé par l'Institut national des données de santé[200] (INDS), n'avait enregistré que 18 demandes d'accès au SNIIRAM[201]. Cette situation a notamment été l'un des éléments déclencheurs de la réforme de l'accès aux données de santé.

85. Au-delà des acteurs publics se trouvent les acteurs privés. Ceux-ci se divisent en deux catégories bien distinctes : les organismes de droit privé à but non lucratif et les organismes de droit privé à but lucratif.

86. Les acteurs privés à but non lucratif sont souvent décrits par la loi Informatique et Libertés comme toute « *association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical* »[202]. Leur activité peut nécessiter une connaissance des

---

[198] V. encadré p.74 du document publié par la Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.* : hormis la CNAMTS, la Cour souligne que les autres régimes d'assurance maladie n'ont qu'un recours très marginal, voir nul, aux données de santé du SNIIRAM.

[199] L'IDS a été créé par l'article 64 de la loi n° 2004-810 du 13 août 2004 *relative à l'assurance maladie*, *JORF*, n° 0190, 17/08/2004, son rôle est « *d'assurer la cohérence et de veiller à la qualité des systèmes d'information utilisés pour la gestion du risque maladie et de veiller à la mise à disposition de ses membres, de la Haute Autorité de Santé, des Unions Régionales des Médecins exerçant à titre Libéral ainsi que d'organismes désignés par décret en Conseil d'Etat, à des fins de gestion du risque maladie ou pour des préoccupations de santé publique, des données issues des systèmes d'information de ses membres, dans des conditions garantissant l'anonymat fixées par décret en Conseil d'Etat pris après avis de la Commission Nationale de l'Informatique et des Libertés* ».

[200] L'INDS a remplacé l'IDS conformément à l'article 193 de la loi n° 2016-41 du 26 janvier 2016, *op.cit*. Sa création est entérinée par la publication de l'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 », *JORF*, n° 0096 du 23/04/2017. L'INDS possède plus de membres que l'IDS et voit son rôle, dans la mise à disposition des données de santé, augmenter.

[201] V. GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *op. cit.*, p. 13. On remarque ici un conflit entre ce rapport qui affirme que moins de 20 demandes d'accès au SNIIRAM ont été reçues par l'IDS en 2010, alors que le rapport produit par l'IDS en 2015 semble indiquer à sa page 28 que plus de 10 demandes ont été admises pour une extraction de données, et plus de 10 demandes ont aussi été admises pour un accès temporaire direct.

[202] V. article 8, 3° de la loi n° 78-17 du 6 janvier 1978, *op. cit.,* dans sa version modifiée par la loi n° 2018-493 du 20 juin 2018 *relative à la protection des données personnelles, JORF*, n° 0141, 21/06/2018. L'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*, a supprimé la référence aux acteurs privés à but non lucratif.

pratiques dans le secteur sanitaire. L'accès aux données de santé contenues dans les bases administratives leur est alors autorisé. Cet accès est soumis à plusieurs conditions et procédures que l'étude ne manquera pas de détailler plus en avant. D'une manière similaire aux acteurs publics ordinaires, le manque d'effectivité de la procédure d'accès aux données de santé a pu être l'un des moteurs de la mise en place du nouveau système d'accès aux données de santé.

87. Enfin, les acteurs privés à but lucratif ferment la marche de l'accès au système des données de santé. Il s'agit de toutes les entreprises dont l'objectif premier est de produire de la valeur, de traiter les données récupérées et d'en tirer des résultats et des informations qui soient monétisables. Ces entreprises peuvent aussi bien être des industriels de santé (produits pharmaceutiques, dispositifs médicaux) que des assureurs (santé, retraité) ou même des bureaux d'études travaillant dans le secteur sanitaire et social. Initialement, l'accès des acteurs à but lucratif aux données de santé était totalement interdit[203]. Puis c'est petit à petit qu'un semblant d'accès s'est formé avec l'obligation pour les organismes à but lucratif de passer par un prestataire extérieur comme le soulignait le Haut Conseil de la santé publique en 2012[204]. La réforme proposée par la loi Santé permet désormais un accès aux données de santé[205] très encadré qui doit encore faire la preuve de son effectivité.

88. Il ressort de cela que la richesse et les opportunités représentées par les données de santé contenues dans les bases de données administratives attisent la convoitise d'acteurs venus de tous les horizons. Chacun de ces demandeurs d'accès peut y voir une multitude d'intérêts : il peut s'agir d'un intérêt économique, d'un intérêt sanitaire, d'un intérêt commercial. Et cet intérêt peut aussi bien être général (concernant la santé publique par exemple) que restreint à quelques bénéficiaires. La multiplication des données de santé produites et leur omniprésence a poussé le ministère de la santé à proposer une réforme adaptant les modalités d'ouverture des bases de données françaises, ce qui suscite autant de craintes que d'espérances.

D) La structure thématique de l'étude

[203] Arrêté du 20 juin 2005 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, *JORF*, n° 192, 19/08/2005.

[204] V. GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *op. cit.*, p. 38.

[205] V. article 193 de la loi n° 2016-41 du 26 janvier 2016, *op. cit.*, codifié aux articles L. 1461-1 et suivants du code de la santé publique.

89. La transparence des données de santé contenues dans les bases médico-administratives semble encore loin d'être acquise en France tant la balance entre les bénéfices qui pourraient en être tirés et les risques qui pourraient en découler paraît être à l'équilibre. Pourtant, le fait que la réforme découlant de la loi santé du 26 janvier 2016 soit en cours de mise en œuvre est un signe positif pour les partisans de l'ouverture des bases de données de santé. Un système censé être suffisamment performant et sûr a été mûrement réfléchi : la transparence devrait être accrue une fois qu'il sera entièrement opérationnel.

90. L'objectif de l'étude est de comprendre comment, et à qui, sont délivrées les différentes autorisations, ou interdictions, d'accès aux données de santé selon qu'un acteur est public, privé, à but lucratif ou non. Chaque partie est entièrement consacrée à l'analyse d'un type d'autorisation d'accès aux données de santé en partant de ceux qui existent depuis le premier arrêté relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie, jusqu'à ceux qui ont été initiés par la loi de modernisation de notre système de santé. Nous verrons ainsi qu'une liste d'acteurs publics, ou ayant une mission de service public, spécifiquement définie par arrêté puis par décret jouit d'un accès qualifié de permanent aux données de santé des bases médico-administratives (Partie 1). Puis nous étudierons la création et l'évolution, jusqu'à aujourd'hui, du système d'autorisation préalable permettant aux acteurs publics et privés sans but lucratif, ne figurant pas sur cette liste, d'accéder à des données de santé en vue de faire de la recherche (Partie 2). Enfin, le cas très particulier des acteurs privés à but lucratif fera l'objet de la dernière partie de l'étude en raison d'une interdiction totale d'accès aux données de santé qui s'est peu à peu muée en autorisation sous conditions (Partie 3). Cette structure permettra de mieux comprendre les caractéristiques et le bien-fondé de chaque autorisation donnée et interdiction formulée à l'égard de chaque type d'acteur. Les modalités d'obtention des données de santé sont-elles différentes selon les autorisations obtenues ? Comment ont-elles évolué ces dernières années ? La réforme du 21 janvier 2016 marque-t-elle un changement notable sur ce point ? Toutes ces questions s'inscrivent dans l'analyse de l'application du droit relatif à l'accès aux données de santé. La présente étude proposera, dans le même temps, une réflexion prospective et critique sur la mise en œuvre de la réforme et sur son contenu.

PARTIE I

LA TRANSPARENCE PERMANENTE DES DONNÉES DE SANTE RÉSERVÉE À DES ACTEURS PUBLICS PRIVILÉGIÉS

91. Le développement du régime juridique de l'autorisation d'accès aux données de santé s'est déroulé sur plusieurs années. Depuis l'entrée en vigueur de la loi du 1er juillet 1994[206] suivie de la création du SNIIRAM en 1998[207], une réflexion est menée pour déterminer quels acteurs pourraient accéder aux données et à quelles conditions. En effet, l'importance des enjeux liés à ces informations dites sensibles[208], associée à une doctrine catégorique sur ce sujet[209], avait poussé le législateur à créer un système d'accès très restrictif. Ce mécanisme reposait alors sur un principe simple, qui constitue encore aujourd'hui le socle de la réforme de la loi de modernisation de notre système de santé[210] : la nature de l'acteur et ses missions permettent de définir l'autorisation d'accès aux données de santé qui peut lui être conférée. D'une part, l'acteur, selon qu'il est public ou privé, n'est pas susceptible d'obtenir les mêmes autorisations d'accès. D'autre part, le type d'accès aux données de santé dépend de l'utilisation que l'acteur, bénéficiaire dudit accès, peut en faire. Ainsi, l'accès diffère selon que l'acteur est investi d'une mission de service public ou non, mais il varie aussi selon le contenu même de cette mission : l'étendue des données de santé accessibles ne sera pas la même selon que la mission concerne un domaine très précis et pointu (telle que l'étude de l'activité d'une catégorie particulière de praticiens médicaux) ou, bien au contraire, qu'elle concerne un vaste champ d'étude (telle que

[206] Loi n° 94-548 du 1 juillet 1994 *relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé* et modifiant la loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, JORF n° 152 du 02/07/1994.

[207] Le Système national interrégimes de l'assurance maladie a été créé par la loi n° 98-1194 du 23 décembre 1998 *de financement de la sécurité sociale pour 1999*, *JORF*, n° 300, 27/12/1998. V. *supra* n° 2.

[208] V. *supra* n° 60 et 61.

[209] Les auteurs sont nombreux à rappeler que seul l'intérêt public justifie qu'un accès aux données de santé soit ouvert à des organismes de recherche publique : voir notamment J. FRAYSSINET, P. PEDROT, « La loi du 1er juillet 1994 relative au traitement des données nominatives ayant pour fin la recherche dans le domaine de la santé », *JCP G*, 21/12/1994, n° 51, p. 561-570 ; J.-M. JOB, « La loi "Informatique et libertés" et les données de santé », *Revue Lamy droit de l'immatériel*, 01/01/2008, n° 34, p. 86-94 ; KHODOSS H., « L'exploitation des données de santé », *RGDM*, 30/09/2004, n° 4, p. 65-76.

[210] Loi n° 2016-41 du 26 janvier 2016 *de modernisation de notre système de santé*, JORF n° 0022, 27/01/2016.

la récolte de toutes les informations sur les consommations de soins à travers l'ensemble de la France).

92. Par ce raisonnement, différents types d'accès ont été mis en œuvre par arrêté dès 2002[211], soit près de quatre ans après la création de la base de données SNIIRAM. Le premier est un accès permanent défini par les textes à tout ou partie des données de santé. Ce droit s'est peu à peu développé pour s'ouvrir plus largement en 2016[212]. Comme l'ont remarqué certains auteurs[213], son évolution vers plus d'assouplissement a tardé à venir.

93. En créant le SNIIRAM, l'une des plus grandes bases de données de santé au monde[214], le législateur français savait que son contenu devait être protégé. Il en a résulté un principe de restriction d'accès découlant de la volonté de protéger la vie privée des individus producteurs desdites données. Mais la création d'une gigantesque base proposant une myriade d'informations numérisées ne semble pas avoir beaucoup d'utilité dès lors qu'elle n'est pas exploitée.

94. Comme l'écrivait G. BRAIBANT dans son rapport remis au Premier Ministre en 1998[215], le traitement des données personnelles devrait se faire au nom de l'intérêt général. Il considérait alors que le traitement des données personnelles de santé devait permettre une meilleure gestion des services publics en renforçant leur efficacité au bénéfice direct des administrés[216]. L'informatisation de l'information était alors perçue – c'est toujours le cas aujourd'hui – comme un moyen de travailler plus vite, de communiquer plus facilement entre les services, et finalement d'améliorer l'action publique. D'après ce rapport, la création de bases de données

---

[211] Arrêté du 11 avril 2002 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, *JORF*, n° 89, 16/04/2002.

[212] La loi n° 2016-41 du 26 janvier 2016, *op. cit.*, propose un accès aux données de santé pour les acteurs de droit privé.

[213] V. PAQUEL N. et BERTHAULT D., « Données de santé : Quoi ? Pour quoi ? Pour qui ? Comment ? », *op. cit.*

[214] Le SNIIRAM est considéré comme l'un des plus grands ensembles de données de santé centralisées comme le souligne P.-L. BRAS dans son Rapport sur la gouvernance et l'utilisation des données de santé, *op. cit*., p. 21. Comme le précise le rapport de la Cour des comptes relatif aux Données personnelles de santé gérées par l'Assurance maladie, *op cit.*, à sa page 25, le SNIIRAM reçoit chaque année toutes les informations relatives aux 500 millions d'actes médicaux pratiqués, aux 1,2 milliards de feuilles de soins produites, aux séjours hospitaliers (plus de 11 millions rien que pour la chirurgie-obstétrique).

[215] BRAIBANT G., Données personnelles et société de l'information : transposition en droit français de la directive n° 95-46 / rapport au Premier Ministre, *la Documentation française*, 1998, 95 p.

[216] *Ibid.*, p. 4.

personnelles et leur bonne utilisation devaient faciliter la continuité des missions de service public. L'un des autres avantages attendus était la simplification des procédures administratives. Concernant le sujet particulier de la santé publique[217], le rapport détectait un potentiel immense d'amélioration tant dans la « *garantie des droits individuels à la santé* » que dans *« une démarche globale de santé publique* ». Force est de constater que, si ce rapport a été rédigé à l'aube de la mise en place de la carte vitale, dite SESAM, incontournable aujourd'hui, son auteur posait déjà les jalons de la création du SNIIRAM et des enjeux de contrôle et de sécurité des données de santé stockées et traitées. Ainsi, le rapport estimait que l'utilisation des données de santé devait être réalisée dans la « *stricte limite des finalités de santé, de recherche et d'assurance maladie* ».

95. C'est dans ce climat de forte attente que les premiers accès aux données de santé ont été mis en place[218], après la création du SNIIRAM, afin de tirer tous les avantages et bénéfices attendus du traitement et de la compréhension des données. Il est important de souligner qu'entre la loi prévoyant la création du SNIIRAM et le premier arrêté ministériel du 11 avril 2002[219], plus de trois années se sont écoulées, permettant entre-temps aux technologies informatiques d'évoluer. Les premiers accès ont été ouverts afin de réaliser des traitements répondant à trois finalités exposées à l'article 2 de l'arrêté du 11 avril 2002[220] : l'amélioration de la qualité des soins ; la contribution à une meilleure gestion de l'assurance maladie ; la transmission aux prestataires de soins des informations pertinentes relatives à leur activité, à

---

[217] *Ibid.,* p.5.

[218] Arrêté du 11 avril 2002 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, *op. cit.*

[219] *Ibid.*

[220] *Ibid.*

« *Les traitements mis en œuvre dans le cadre du système national d'information inter-régimes de l'assurance maladie ont pour finalités :*
1° D'améliorer la qualité des soins, notamment par la comparaison des pratiques aux référentiels, au sens de l'article L. 162-12-15 du code de la sécurité sociale, et moyennes professionnels ;
2° De contribuer à une meilleure gestion de l'assurance maladie, notamment par :
- la connaissance des dépenses de l'ensemble des régimes d'assurance maladie par circonscription géographique, par nature de dépense, par catégorie de professionnels responsables de ces dépenses et par professionnel ou établissement ;
- l'évaluation des transferts entre enveloppes correspondant aux objectifs sectoriels de dépenses fixés, en fonction de l'objectif national de dépenses d'assurance maladie, dans le cadre de la loi annuelle de financement de la sécurité sociale ;
- l'analyse quantitative des déterminants de l'offre de soins et la mesure de leurs impacts sur l'évolution des dépenses d'assurance maladie ;
3° De transmettre aux prestataires de soins les informations pertinentes relatives à leur activité, à leurs recettes et, s'il y a lieu, à leurs prescriptions. »

leurs recettes et, s'il y a lieu, à leurs prescriptions. Ces objectifs convergent avec les attentes exprimées dans le rapport BRAIBANT[221]. Le protocole du 15 octobre 2001[222] approuvé par l'arrêté du 11 avril 2002[223] a donc établi la liste exhaustive des acteurs ayant un accès au SNIIRAM ainsi que la liste des données de santé accessibles. Ni le protocole, ni l'arrêté n'évoquent la notion d'accès permanent. Pourtant, à la lecture de l'article 4 de l'arrêté du 11 avril 2002, la lettre du texte permet de déduire que des accès permanents sont délivrés à une sélection d'acteurs spécifiques[224]. La principale catégorie d'accès aux données de santé créée en ce début de XXIe siècle est celle qui permet d'accéder de façon permanente aux données de santé. L'accès permanent fait cependant l'objet d'un fractionnement, comme nous le verrons dans le premier chapitre qui va suivre : certains acteurs bénéficient d'un accès à toutes les données de santé alors que d'autres ne sont autorisés à accéder qu'à une sélection prédéfinie de données.

96. Avant d'aller plus loin, il convient de s'attarder un instant sur ce que recouvre la notion d'accès permanent. Il est tentant d'y voir la possibilité pour ceux qui en sont détenteurs d'obtenir toutes les informations qu'ils désirent, sans aucune limite et sans contrôle. Cependant, compte tenu de la nature hautement sensible des données dont il est question ici, les plus grandes précautions ont été prises pour définir un mécanisme qui soit maîtrisé. L'accès permanent aux données de santé est donc encadré strictement par arrêté ou par décret. Pour chaque accès

---

[221] BRAIBANT G., Données personnelles et société de l'information : transposition en droit français de la directive n° 95-46 / rapport au Premier Ministre, *op.cit.*

[222] Protocole du 15 octobre 2001 définissant les modalités de gestion et de renseignement du système national d'information inter-régimes de l'assurance maladie (SNIIRAM), signé par la Caisse nationale de l'assurance maladie des travailleurs salariés, la Caisse centrale de la mutualité sociale agricole et la Caisse nationale d'assurance maladie et maternité des travailleurs non salariés des professions non agricoles.

[223] Arrêté du 11 avril 2002, *op. cit.*

[224] V. article 4 de l'arrêté du 11 avril 2002, *op. cit.* :

« *Les destinataires des informations contenues dans le système national d'information inter-régimes de l'assurance maladie sont, à raison de leurs fonctions et selon les règles d'habilitation détaillées à l'annexe 2 du protocole :*

1° Pour l'ensemble des informations visées à l'article 3 : les médecins-conseils 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 nommément désignés, suivant leur rattachement administratif, par les directeurs ou les agents comptables des caisses et des unions.

Seuls les médecins-conseils et les personnels placés sous leur responsabilité, nommément désignés par les médecins responsables selon l'organisation des régimes, sont autorisés à effectuer des recherches mettant en oeuvre simultanément plus d'une des trois variables sensibles (code commune, date des soins, mois et année de naissance) avec d'autres données. »

permanent, deux éléments essentiels sont définis : qui en sont les bénéficiaires, et à quelles données l'accès est ouvert.

97. La notion d'accès permanent étant maintenant délimitée, il est opportun de s'intéresser à l'identité des acteurs qui peuvent en bénéficier. Comme l'indique l'article 4 de l'arrêté du 11 avril 2002[225], les médecins-conseils[226] et les personnels placés sous leur responsabilité ainsi que les agents administratifs des caisses des régimes de base d'assurance maladie et des unions régionales des caisses d'assurance maladie désignés par les directeurs ou agents comptables des caisses et des unions ont accès en permanence à l'ensemble des informations du SNIIRAM. En des termes plus courts et usuels, la Cour des comptes, dans son rapport sur les données de santé remis en 2016[227], indique que « *seules les caisses d'assurance maladie (au niveau national et local) peuvent accéder aux informations individuelles mais anonymisées relatives aux bénéficiaires ainsi qu'aux données individuelles identifiantes des professionnels de santé* ».

98. Les bénéficiaires d'un accès permanent aux données de santé sont donc, avant tout, les personnels travaillant pour certains organismes publics dont l'activité est directement liée aux questions relatives à l'assurance maladie, à la sécurité sociale, et par extension à la santé publique. Cette volonté de limiter l'accès permanent à des acteurs prédéterminés est parfaitement compréhensible de par la nature sensible des données et l'usage, ou plutôt le mésusage[228], qui pourrait en être fait. Cet accès vise alors prioritairement à permettre le bon fonctionnement du service public par la mise à disposition d'informations essentielles (Titre I). Cependant, la priorité qui semble être attachée à la proposition d'un accès permanent réservé à quelques acteurs publics mérite d'être regardée sous un angle critique. En effet, les raisons justifiant cet accès permanent paraissent parfois déséquilibrées par rapport aux résultats finalement produits, faisant apparaître des limites qu'il convient de détailler (Titre II).

[225] *Idem.*

[226] Les médecins conseils sont les médecins attachés aux organismes d'assurance maladie qui sont chargés de donner des avis médicaux motivés sur les cas qui leurs sont soumis.

[227] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 138.

[228] On entend par mésusage le fait de traiter des données brutes sans prendre en compte, volontairement ou non, tous les paramètres qui peuvent impacter leur interprétation : par exemple le fait d'analyser la consommation de soins dans deux zones géographiques différentes sans tenir compte des caractéristiques de la population (âge…) constitue un mésusage.

TITRE I

L'ACCÈS PERMANENT AUX DONNÉES DE SANTÉ JUSTIFIÉ PAR LE MEILLEUR FONCTIONNEMENT DU SERVICE PUBLIC

99. La création de la base de données de santé SNIIRAM, puis la mise en œuvre des premières autorisations d'accès en 2002 ont, comme nous l'avons vu[229], été motivées par l'ambition d'améliorer le fonctionnement du service public. Ce dernier semble alors dominer le droit au respect de la vie privée des individus : mais les mesures de sécurités qui encadrent l'accès aux données de santé permettent de rétablir l'équilibre[230]. Cette notion de service public repose, en droit français, sur les trois critères bien connus que sont le rattachement à une personne publique[231], bien que le service public puisse être géré par une personne privée[232] ; la gestion d'une activité d'intérêt général[233] ; et la soumission au droit public[234]. En France, tous les services publics, y compris ceux qui nous intéressent dans le cadre de l'étude, répondent aux principes fondamentaux de fonctionnement définis dans les « lois de Rolland » : il s'agit de

[229] *Supra* n° 49 à 52.

[230] *Infra* n° 114 à 120 et n° 126 à 131.

[231] Conseil d'Etat, 29 mars 1901, 94580, recueil Lebon, Casanova. V. M. HAURIOU, note sous Conseil d'Etat, 29 mars 1901, Casanova, S. 1901.3.73.

[232] Arrêts Conseil d'Etat, 6 février 1903, 07496, recueil Lebon, Terrier ; et Conseil d'Etat, 4 mars 1910, 29373, recueil Lebon, Thérond. V. M. HAURIOU, note sous Conseil d'Etat, 6 février 1903, Terrier, S. 1903.3.25 ; AJ 2003.153, art. D. Costa ; M. HAURIOU, note sous Conseil d'Etat, 4 mars 1910, Thérond, S. 1911.3.17 ; RD publ. 110.249, note Jèze.

[233] Arrêt du Conseil d'Etat Casanova, *op. cit*, et arrêt Conseil d'Etat Section, 30 mai 1930, 06781, recueil Lebon, Chambre syndicale du commerce en détail de Nevers. V. S. 1931.3.73, concl. Josse, note Alibert.

[234] Tribunal des conflits, 8 février 1873, 00012, recueil Lebon, Blanco. v. S. 1873.3.153, concl. David.

l'égalité devant le service public[235] ; de la mutabilité, ou adaptabilité, du service public[236] ; et enfin de la continuité du service public[237].

100. Le droit européen n'a pas manqué d'apporter sa pierre à l'édifice de la notion de service public. Au niveau européen, le service public n'existe pas en tant que tel, il est remplacé par les services d'intérêt général, ou SIG[238], et par les services d'intérêt économique général, ou SIEG. La politique européenne a progressivement entraîné la mise au ban de plusieurs situations monopolistiques de services publics en les ouvrant à la concurrence[239] : seuls les SIEG sont cependant concernés. Dans la pratique, les SIG[240] sont des services marchands et non marchands qui présentent un intérêt général justifiant leur soumission à des règles spécifiques liées au service public. *A contrario*, les SIEG regroupent des services ayant une activité économique qui sont soumis à des règles permettant aux règles de concurrence de s'appliquer, à la condition que l'accomplissement de leur service public ne soit pas en péril. La Commission européenne, dans un Livre blanc du 12 mai 2004[241], indique que tous les services non

[235] Précisons que le principe de neutralité est ici assimilé au principe d'égalité. Il s'agit d'un principe à valeur constitutionnelle découlant de la Déclaration des Droits de l'Homme et du Citoyen de 1789, consacré par l'arrêt Conseil d'Etat Section, 9 mars 1951, 92004, recueil Lebon, Société des concerts du conservatoire pour l'égalité appliquée aux usagers du service public. Puis consacré par l'arrêt Conseil d'Etat, Assemblée, 28 mai 1954, 28238 28493 28524 30237 30256, recueil Lebon, Barel. v. S. 1951.3.81, note C.H. ; Dr. Soc. 1951.168, concl. Letourneur, note Rivero ; RD publ. 1954.509, concl. Letourneur, note M. Waline ; RPDA 1954.149, concl. Letourneur, note Eisenmann ; RA 1954.393, concl. Letourneur, note Liet-Veaux ; AJ 1954.II.396, note Long ; D. 1954.594, note G. Morange ; S. 1954.3.97, note Mathiot.

[236] Corollaire du principe de continuité, ce principe est consacré par l'arrêt Conseil d'Etat, 10 janvier 1902, 94624, recueil Lebon, Compagnie Nouvelle du Gaz de Déville-lès-Rouen. v. S. 1902.3.17, note Hauriou.

[237] Principe à valeur constitutionnel depuis la décision du Conseil Constitutionnel, 25 juillet 1979, n° 79-105 DC. Qualifié de principe fondamental dans l'arrêt Conseil d'Etat, 13 juin 1980, 17995, recueil Lebon, Madame Bonjean.

[238] Les SIG ont fait l'objet de plusieurs publications de la Commission européenne, comme son Livre vert du 21 mai 2003 et son Livre blanc du 12 mai 2004. Ces deux ouvrages ont réaffirmé que les services d'intérêt général participent à l'amélioration de la qualité de vie des citoyens et à lutter contre l'exclusion sociale. A ce titre, une résolution du Parlement européen du 13 janvier 2004 est venue préciser que les services d'intérêt général concernant la santé sont à exclure du champ d'application des règles de concurrence.

[239] CAPONETTI L., « Le cadre réglementaire européen en matière de services publics : législation, financement et contraintes », *Ciriec* (Centre international de recherches et d'information sur l'économie publique, sociale et coopérative) n° 2016/10. L'annexe I rappelle que le Traité sur le fonctionnement de l'Union européenne (TFUE) du 13/12/2007, à son article 106, impose à toutes « *les entreprises chargées de la gestion d'un SIEG ou présentant le caractère d'un monopole fiscal sont soumises aux règles des traitées, notamment aux règles de concurrence* ».

[240] Comme l'indique le schéma réalisé par GHEKIERE L. en annexe II du document produit par CAPONETTI L., *ibid.*, les services d'intérêt général ou SIG sont les services qui relèvent de fonctions de puissance publique ou de fonctions exclusivement sociales comme la Police, la Justice, la Défense. Or un secteur bien identifié balance généralement entre les SIG et les SIEG : il s'agit des services sociaux et de la protection sociale. Certains sont de nature économique, d'autres non, ce qui les place dans une zone grise.

[241] *Ibid.*

marchands, qui sont alors des services régaliens[242], sont exclus de la logique du marché et échappent aux règles de la concurrence : dès lors, des règles spécifiques de service public peuvent s'imposer à eux. C'est à ce type de services publics, en France, que les données de santé sont ouvertes en priorité.

101. Dès l'arrêté du 11 avril 2002[243], les acteurs qui bénéficient des premiers accès permanents aux données de santé ont une mission de service public tout à fait particulière car leur activité est intrinsèquement liée à la gestion de la sécurité sociale et, par extension, à la santé publique. Mais cet accès permanent, parfois limité à une liste spécifique de données, n'est pas resté figé à sa version initiale, fort restrictive. Cependant, l'évolution du contenu et des bénéficiaires de l'accès permanent a manqué de fluidité. Avant de proposer une analyse de l'étendue des données de santé mises à disposition de manière permanente (Chapitre 2), il est nécessaire de savoir qui sont les acteurs ayant une mission de service public qui ont obtenu leur accès permanent aux données de santé (Chapitre 1).

[242] Exemples non exhaustifs de missions régaliennes : sécurité, justice, santé, éducation, mais aussi la culture ou encore l'environnement.

[243] Arrêté du 11 avril 2002, *op. cit.*

CHAPITRE I
L'ACCES PERMANENT OUVERT UNIQUEMENT À DES ACTEURS PRIVILÉGIÉS DU SERVICE PUBLIC

102. Le premier arrêté paru le 11 avril 2002 est venu proposer[244] le détail des acteurs pouvant disposer d'un accès permanent aux données de santé contenues dans le SNIIRAM. Depuis la publication de cet arrêté, la liste des bénéficiaires de l'accès permanent a changé à maintes reprises. Nous nous intéresserons dans un premier temps à l'identité des acteurs ayant une mission de service public qui bénéficient de l'accès permanent (Section 1), puis nous aborderons la question de la pertinence et du contrôle de cet accès permanent (Section 2).

SECTION 1 : LES ACTEURS CENTRAUX DU SERVICE PUBLIC SEULS BÉNÉFICIAIRES DE L'ACCÈS PERMANENT

103. La liste des acteurs pouvant accéder en permanence aux données de santé n'a pas été gravée dans le marbre à sa création. Au contraire, la possibilité d'étendre l'accès permanent à de nouveaux acteurs disposant d'une mission de service public est un atout. Cependant, l'élargissement des bénéficiaires de l'accès permanent a souvent été irrégulier et difficile à appréhender. Nous étudierons donc avec précision la liste des acteurs qui ont obtenu le droit d'accéder en permanence aux données de santé depuis 2002 jusqu'avant la réforme de la loi de modernisation de notre système de santé[245] (§1), puis nous examinerons le contenu de la réforme en apportant un regard pratique sur sa mise en œuvre qui, bien qu'ayant été préparée en amont, est critiquable sous certains aspects (§2).

Paragraphe 1 : L'hésitante évolution des bénéficiaires de l'accès permanent

104. Le premier arrêté relatif à la mise en œuvre du SNIIRAM[246] est venu poser les fondations de l'accès permanent aux données de santé. Il a essentiellement défini deux éléments indispensables : la liste des bénéficiaires de l'accès permanent et la délimitation des données accessibles à ces bénéficiaires[247]. C'est principalement sur ce modèle qu'ont été publiés la

[244] *Ibid.,* art. 4.

[245] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[246] Arrêté du 11 avril 2002, *op. cit.*

[247] V. Partie I, Titre I, Chapitre II.

plupart des textes, lois, décrets et arrêtés[248], venus apporter une évolution à la liste des bénéficiaires de l'accès permanent aux données de santé. Les tous premiers accès permanents ont été délivrés à une liste variée d'acteurs : étaient visés les médecins des caisses d'assurance maladie ainsi que les personnels sous leur responsabilité et les agents administratifs desdites caisses ; les agents des ministères chargés du travail, de l'agriculture, des finances ; les agents des agences régionales de l'hospitalisation (ARH), devenues agences régionales de santé (ARS) ; les prestataires de soins[249] ; et enfin les unions régionales de médecins libéraux, devenues unions régionales des professionnels de santé (URPS). En dehors de cette liste, aucun autre acteur disposant pourtant d'une mission de service public n'avait d'accès permanent aux données de santé. Cette première vague d'autorisations d'accéder de manière permanente aux données de santé amène trois observations.

La première observation est qu'il y a un déséquilibre entre les personnes morales, peu nombreuses, et les personnes physiques, bien plus représentées, qui obtiennent un accès permanent aux données de santé. En effet, la présence de tous les prestataires de soins parmi les bénéficiaires de l'accès permanent laisse entendre que des milliers de professionnels de santé sont concernés : ce qui peut faire craindre le pire pour la protection de la vie privée des individus à l'origine des données de santé. Cependant, cet apparent déséquilibre est immédiatement corrigé par la nature des données qui sont rendues accessibles à chacun de ces acteurs[250].

Deuxièmement, nous retrouvons dans l'arrêté certains acteurs essentiels dans le fonctionnement du système de santé : les médecins-conseils et agents de l'Assurance maladie, les agents des ARH, l'ensemble des prestataires de soins. Ces bénéficiaires ont assurément un avantage à accéder aux données de santé dans le cadre de leurs missions. Pourtant nous constatons avec étonnement l'absence d'acteurs qui semblent pourtant incontournables dans le domaine

[248] Pas moins de dix arrêtés ont été publiés pour apporter des précisions relatives à l'accès au SNIIRAM, et trois lois ont également été votées sur ce sujet. Il s'agit 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*, JORF, n° 0167, 22/07/2009, de la loi n° 2011-2012 du 29 décembre 2011 *relative au renforcement de la sécurité sanitaire du médicament et des produits de santé*, JORF, n° 0302, 30/12/2011, et de la loi n° 2016-41 du 26 janvier 2016, op. cit.

[249] Cette notion de « *prestataires de soins* » n'est pas définie par l'arrêté mais deux exemples sont donnés dans le texte avec les professions médicales et les pharmaciens. Dès lors, il est possible d'en déduire que tous les professionnels qui participent au parcours de santé du patient, depuis le médecin de ville jusqu'au docteur en pharmacie en passant par les établissements médicaux hospitaliers publics ou privés, disposent d'un accès permanent aux données délimitées par arrêté.

[250] V. Partie I, Titre I, Chapitre II.

sanitaire avec en premier lieu les agents du ministère chargé de la santé. Nous remarquons aussi l'absence de l'Institut de veille sanitaire (INVS), devenu Santé publique France[251], et de l'Agence française de sécurité sanitaire des produits de santé (AFSSAPS), devenue Agence nationale de sécurité du médicament et des produits de santé (ANSM)[252]. Cette absence a été corrigée par la parution d'un arrêté supplémentaire en 2005[253] mais elle révèle le symptôme principal dont souffre l'accès permanent : le souci d'exhaustivité voulu par les textes, parfois associé à l'utilisation de formules très évasives, a pu provoquer de grandes incertitudes concernant l'identité des acteurs pouvant accéder en permanence aux données de santé.

Enfin, dans le premier arrêté paru en 2002, nous notons la présence d'agents de ministères dont la mission paraît bien éloignée des missions sanitaires de service public. En effet, il est difficile de concevoir que les ministères chargés du travail, de l'agriculture ou des finances puissent avoir la même utilité à obtenir des données de santé que les agents de l'Assurance maladie. Pourtant l'accès à certaines informations par lesdits ministères avait un objectif bien précis et rattaché à leur mission de service public : ainsi, les agents du ministère de l'agriculture ont obtenu l'accès aux données spécifiquement liées aux ressortissants des régimes de protection sociale agricole. Il n'est pas aisé d'en dire autant des prestataires de soins qui, convenons-en, peuvent remplir une mission qui participe du bon fonctionnement du service public de la santé. Leur capacité d'accès aux données de santé en permanence fait d'ailleurs l'objet d'un débat au sein de cette étude[254].

105. L'arrêté fondateur des accès permanents aux données de santé a par la suite été modifié ou remplacé à plusieurs reprises. Les textes les plus significatifs sont notamment parus en

[251] Ordonnance n° 2016-462 du 14 avril 2016 *portant création de l'Agence nationale de santé publique*, JORF n° 0089, 15/04/2016.

[252] Loi n° 2011-2012 du 29 décembre *2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé*, JORF n° 0302 du 30/12/2011.

[253] Arrêté du 20 juin 2005 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, *JORF*, n° 192, 19/08/2005.

[254] V. Partie I, Titre II.

2005[255], 2011[256], 2012[257], 2013[258], 2014[259] et 2016[260]. Cette succession de changements apportés à la liste des bénéficiaires des accès permanents aux données de santé peut être perçue de deux façons, l'une positive, l'autre négative. Si l'on adopte un point de vue positif, le fait que la liste des bénéficiaires évolue de manière régulière est un avantage : cela pourrait signifier que le système d'accès permanent aux données fonctionne et que son efficacité et son utilité sont prouvées. *A contrario*, d'un point de vue plus critique, cet empilement de textes au fil des années peut être perçu comme une instabilité et un manque de maîtrise et de connaissance des acteurs qui, dans le cadre de leur mission de service public, ont un intérêt à accéder aux données. Dans les faits, notre analyse emprunte aux deux visions.

106. L'apport progressif de nouveaux bénéficiaires d'un accès permanent aux données de santé démontre la volonté de maîtriser l'ensemble du processus. Chaque nouvel accès n'est délivré que lorsque les besoins de l'acteur ont été exprimés et analysés pour que les données accessibles en permanence correspondent à l'usage qu'il pourra en faire dans le cadre de sa mission de service public. C'est comme cela que le Haut Conseil pour l'avenir de l'assurance maladie[261], l'InVS, l'AFSSAPS, les agents de la Caisse nationale de solidarité pour l'autonomie, les chercheurs de l'IRDES (Institut de recherche et de documentation en économie de la santé), les agents du CETAF (centre technique d'appui et de formation des centres d'examens de santé), les chercheurs de l'INSERM (Institut national de la santé et de la recherche médicale) et ceux du CNRS (Centre national de la recherche scientifique) ont obtenu leur accès en 2005[262]. Puis

[255] Arrêté du 20 juin 2005, *op. cit.*

[256] Arrêté du 1er décembre 2011 relatif à la mise en œuvre du système national d'information inter-régimes de l'assurance maladie, JORF, n° 0019, 22/01/2012.

[257] Arrêté du 11 juillet 2012 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, JORF, n° 0171, 25/07/2012.

[258] Arrêté du 19 juillet 2013 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, JORF, n° 0187, 13/08/2013.

[259] Arrêté du 14 février 2014 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, JORF, n° 0052, 02/03/2014.

[260] Arrêté du 6 octobre 2016 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, JORF, n° 0244, 19/10/2016.

[261] Le Haut Conseil pour l'avenir de l'assurance maladie, ou HCAAM, a été créé par le décret n° 2003-959 du 7 octobre 2003. Il a pour mission d'évaluer le système d'assurance maladie et ses évolutions, de décrire la situation financière et les perspectives des régimes d'assurance maladie et apprécier les conditions requises pour assurer leur pérennité à terme ; de veiller à la cohésion du système d'assurance maladie au regard de l'égal accès à des soins de haute qualité et d'un financement juste et équitable ; de formuler, le cas échéant, des recommandations ou propositions de réforme de nature à répondre aux objectifs de cohésion sociale et de pérennité financière des régimes d'assurance maladie.

[262] Arrêté du 20 juin 2005, *op. cit.*

en 2008[263], c'est l'agence technique de l'information sur l'hospitalisation (ATIH)[264] et les membres de l'Institut des données de santé qui ont reçu leur accès. Ensuite, en 2011[265] et 2012[266], de nouveaux acteurs[267] ont été précisés dans la liste des bénéficiaires de l'accès permanent, parmi lesquels se trouvent les agences régionales de santé (ARS). Enfin, le dernier arrêté relatif à la mise en œuvre du SNIIRAM, pris le 6 octobre 2016[268], a permis aux agents de la direction de la recherche, des études, de l'évaluation et des statistiques (DREES) de bénéficier nommément d'un accès permanent.

107. L'un des marqueurs de l'aspect hésitant du processus d'élargissement des bénéficiaires des accès permanents réside aussi dans la création d'accès à titre temporaire ou expérimental. Ces « essais » indiquent que le bénéfice qui peut être tiré de l'accès aux données de santé est reconnu mais que cet accès reste bien trop sensible pour être accordé à titre permanent. Ainsi, l'arrêté du 19 juillet 2013[269] a permis aux médecins de l'InVS et aux personnels placés sous leur responsabilité, d'effectuer pendant 3 ans des traitements en croisant simultanément plus d'une des quatre variables sensibles[270] : la condition posée était que ces variables devaient être strictement nécessaires aux missions de surveillance et d'alerte sanitaires. Plus tard[271], cette possibilité a aussi été offerte aux médecins et personnels placés sous leur responsabilité participant aux expérimentations relatives aux personnes âgées en risque de perte d'autonomie (PAERPA)[272] : la limite étant que les traitements ne pouvaient s'effectuer que dans le champ de la compétence régionale des médecins à la condition que les variables sensibles soient nécessaires aux expérimentations.

---

[263] Arrêté du 16 octobre 2008 relatif à la mise en œuvre du système national d'information inter-régimes de l'assurance maladie, JORF, n° 0252, 28/10/2008.

[264] L'ATIH est l'agence qui gère la base de données PMSI, v. *supra* n° 23.

[265] Arrêté du 1er décembre 2011, *op. cit*.

[266] Arrêté du 11 juillet 2012, *op. cit.*

[267] Les acteurs sont : les ARS, l'Agence de biomédecine, les membres de l'Union nationale des professions de santé, mais aussi les agents du fonds CMU, et des membres de l'Observatoire français des drogues et de la toxicomanie (OFDT) et de l'UNOCAM.

[268] Arrêté du 6 octobre 2016, *op. cit.*

[269] Arrêté du 19 juillet 2013, *op. cit.*

[270] *Infra* n° 150.

[271] Arrêté du 14 février 2014, *op.cit.*

[272] Cette expérimentation était prévue par l'article 48 de la loi n° 2012-1404 du 17 décembre 2012 relative au financement de la sécurité sociale pour 2013. Les médecins participant à l'expérimentation étaient nommément désignés par l'autorité médicale de chacune des ARS participant aux expérimentations en question. L'autorisation d'utiliser plus d'une des quatre variables sensibles n'a existé que pendant la durée de ladite expérimentation.

Ce même arrêté de 2013[273] a aussi créé un accès permanent spécialement dédié aux personnels des ARS. Il s'agit d'une mise en conformité avec la charte d'engagement[274] pour la mise à disposition et les principes d'utilisation des données issues du SNIIRAM dans les ARS. Les données individuelles des bénéficiaires de l'assurance maladie ont ainsi été rendues accessibles pour les médecins membres des ARS dans le but de réaliser des recherches dans leur seul champ de compétence régionale. Quant aux données individuelles des professionnels de santé, elles ont été rendues accessibles aux médecins membres des ARS afin d'effectuer des recherches localisées (code commune et données infra communales) sur leur champ de compétence régionale.

108. L'ajout de tous ces nouveaux acteurs parmi les bénéficiaires de l'accès permanent peut démontrer une maîtrise dans la délivrance des autorisations : mais cette maîtrise reste relative car le processus a montré quelques imperfections. D'abord, comme nous l'avons évoqué[275], des acteurs qui semblent avoir un intérêt certain à accéder aux données de santé en permanence n'ont spécifiquement obtenu le précieux sésame que tardivement : c'est le cas des membres de la DREES[276]. L'utilisation de certaines expressions extrêmement floues a également été un facteur d'instabilité. Dans l'arrêté de 2005[277], par exemple, de nouveaux bénéficiaires de l'accès permanent ont été définis par la formule « *agences placées sous tutelle du ministère chargé de l'assurance maladie et de la santé* ». Aucune liste exhaustive desdites agences n'était donnée par ailleurs. La DREES était-elle incluse dans ces termes imprécis ? C'est l'interprétation qu'en font les différents rapports[278] sur le sujet. Pourtant, si tel était vraiment le cas, pourquoi l'arrêté de 2016 aurait-il pris soin de nommer distinctement les agents de la DREES comme

[273] Arrêté du 19 juillet 2013, *op. cit.*

[274] La charte d'engagements pour la mise à disposition et les principes d'utilisation des données issues du SNIIRAM dans les ARS entre les membres de l'UNCAM, le ministère du travail, de l'emploi et de la santé et l'Union nationale des professionnels de santé est mentionnée par les arrêtés successifs relatifs au SNIIRAM sans que la source de cette charte ne soit indiquée.

[275] *Supra* n° 104.

[276] *Supra* n° 106.

[277] Arrêté du 20 juin 2005, *op. cit.*

[278] V. notamment Rapport de P.-L. Bras, *op. cit.*, p. 34 ; Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 76.

bénéficiaires de l'accès permanent ? Il est probable que le COPIIR[279] se soit rendu compte, bien trop tardivement, de l'imprécision des arrêtés.

109. Des oublis ont aussi été constatés à plusieurs reprises, créant une grande confusion chez les acteurs qui auraient dû bénéficier d'un accès permanent et qui n'apparaissaient pas dans la liste des bénéficiaires. C'est ce qui est arrivé aux agents de la Haute Autorité de santé et de l'Institut national du cancer qui auraient dû figurer dans l'arrêté de 2005 et dont la mention a finalement été apportée par l'arrêté rectificatif du 26 septembre 2006[280]. Les agents des ARS ont aussi été victimes d'un oubli : bien présents dans la liste des bénéficiaires de l'arrêté du 1er décembre 2011[281], ils disparurent de la liste dans l'arrêté du 11 juillet 2012[282] avant d'être réintégrés par arrêté du 7 septembre 2012[283]. L'impact de ces erreurs de rédaction sur l'activité des bénéficiaires n'a pas été mesuré, cependant, il ne fait aucun doute qu'une telle instabilité n'a pas été favorable à une utilisation optimisée du droit d'accès permanent aux données de santé.

110. Au-delà des maladresses et des erreurs dans la rédaction des textes conférant un accès permanent, il est aussi arrivé qu'une loi ouvre cet accès à un nouvel acteur mais que le décret relatif à son application ne paraisse pas. C'est précisément ce qui est arrivé à l'accès qui devait être délivré au groupement d'intérêt public créé par la loi du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé[284]. Ce groupement d'intérêt public, constitué par l'Etat, la HAS, l'ANSM, l'InVS et la CNAMTS, devait avoir pour mission d'autoriser ou non les accès aux données de santé à des fins d'études en santé publique. Pour réaliser sa mission, il était donc impératif qu'il puisse lui-même avoir un accès permanent aux données de santé, d'autant plus qu'il pouvait conduire lui-même les études en

[279] Le COPIIR est le Comité d'Orientation et de Pilotage d'Information Inter-Régimes, v. Institut des données de santé, « Processus d'élaboration de l'arrêté permettant l'utilisation des données anonymisées de l'assurance maladie obligatoire ».

[280] Arrêté du 26 septembre 2006 modifiant l'arrêté du 20 juin 2005 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, JORF, n° 244, 20/10/2006.

[281] Arrêté du 1er décembre 2011, *op. cit*.

[282] Arrêté du 11 juillet 2012, *op. cit*.

[283] Arrêté du 7 septembre 2012 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, JORF, n° 0245, 20/10/2012.

[284] Loi n° 2011-2012 du 29 décembre 2011 *relative au renforcement de la sécurité sanitaire du médicament et des produits de santé*, JORF, n° 0302, 30/12/2011. v. RAJOT B., « Renforcement de la sécurité sanitaire du médicament et des produits de santé », *Responsabilité civile et assurances*, n° 1, 01/2012.

question. Tout cela était bien prévu par l'article 33 de la loi susmentionnée qui créait l'article L. 5121-28 du code de la santé publique. Cependant, l'ensemble de cet article ne pouvait être effectif qu'à la condition qu'un décret en Conseil d'Etat, pris après avis de la CNIL, soit pris et publié. Or, comme le déplore P.-L. BRAS dans son rapport[285], ledit décret n'était toujours pas paru en 2013. Il ne l'avait toujours pas été avant la réforme engagée par la loi de modernisation de notre système de santé.

111. Le dernier élément de critique qui pourrait être formulé concerne les délais de création des accès permanents qui semblent, par endroits, très tardifs. Le problème des délais d'ouverture des accès permanents s'est ainsi illustré par le cas des ARS : la loi du 21 juillet 2009[286] a bien ouvert aux ARS un accès permanent aux données de santé mais ce n'est que suite à la parution de l'arrêté de 2011[287], paru le 22 janvier 2012 au Journal officiel, que l'accès est devenu effectif. Deux ans et six mois se sont écoulés entre la volonté du législateur d'ouvrir l'accès permanent aux ARS et la réalisation, dans les faits, de cette volonté.

112. Il ressort de toutes ces réflexions que le processus de choix des acteurs bénéficiaires des accès permanents est aussi louable que critiquable. Nous pouvons penser que les initiateurs des arrêtés successifs ont conservé comme préoccupation principale la protection de la vie privée : il leur fallait alors trouver l'équilibre entre l'ouverture d'un accès aux données les plus sensibles qui soient, et le droit au respect de la vie privée qui ne doit en aucun cas être violé. C'est probablement pour cette raison que les arrêtés délivrant les autorisations d'accès permanent ont été publiés avec parcimonie. Certes, la maîtrise du dispositif passe avant tout par la proposition de listes exhaustives des bénéficiaires et par un calendrier progressif d'ouverture des accès. Mais les nombreuses lacunes constatées dans les différents textes publiés et la délivrance trop lente des autorisations d'accès ont été à l'encontre de l'objectif même de ces accès qui était d'aider les acteurs à exercer leurs missions de service public. Ces anomalies sont autant d'éléments qui ont servi à critiquer ce mécanisme d'accès permanent, comme nous le verrons dans le prochain titre[288].

[285] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.,* p. 31.

[286] Loi n° 2009-879 du 21 juillet 2009, *op. cit.*

[287] Arrêté du 1er décembre 2011, *op. cit*.

[288] V. Partie I, Titre II.

113. Après avoir étudié les acteurs bénéficiant d'un accès permanent aux données de santé et leur évolution depuis la mise en place du dispositif en 2002 jusqu'en 2016, il convient de s'intéresser à la pertinence du nouveau système créé par la loi du 26 janvier 2016 relative à la modernisation de notre système de santé[289].

Paragraphe 2 : La réforme pertinente et maîtrisée de l'accès permanent

114. La mise en place du nouveau système national des données de santé, ou SNDS, par la loi du 26 janvier 2016[290] a donné lieu à la refonte de l'intégralité du dispositif d'accès aux données. Les accès permanents ont donc, eux aussi, été repensés pour être mieux compris et ouverts à un maximum d'acteurs dont la mission de service public le nécessite. Les rédacteurs de cette loi réformant le système d'accès aux données de santé ont tiré parti des rapports relatifs aux données de santé[291], à la protection des données personnelles[292], aux données ouvertes en santé[293], ou encore au coût de l'accès aux données ouvertes[294], pour construire le nouveau système. C'est l'article 193 de ladite loi qui définit le Système national des données de santé, ou SNDS. Il a créé l'article L. 1461-3 du code de la santé publique qui indique à son III que « *la liste des services de l'Etat, des établissements publics ou des organismes chargés d'une mission de service public autorisés à traiter des données à caractère personnel du système national des données de santé pour les besoins de leurs missions* » est fixée par décret pris en Conseil d'Etat. Ce décret doit préciser « *pour chacun de ces services, établissements ou organismes, l'étendue de cette autorisation, les conditions d'accès aux données et celles de la gestion des accès* ». Le décret[295] a finalement été pris le 26 décembre 2016 et il a fait l'objet d'une publication au Journal officiel deux jours plus tard.

---

[289] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[290] *Ibid.*

[291] V. notamment BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.* ; GOLDBERG M., *Rapport du Haut Conseil de la Santé publique de mars 2012, op. cit.*

[292] GORCE G. et PILLET F., *Rapport d'information au Sénat, op. cit.*

[293] BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé, op. cit.*

[294] TROJETTE M. A. avec le concours de LOMBARD R., *Rapport au Premier ministre, op. cit.*

[295] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

115. Les auteurs de la réforme semblent aussi avoir appris des errements constatés depuis le premier arrêté SNIIRAM du 11 avril 2002[296]. Tout a été mis en œuvre pour que la réforme soit la plus limpide et rapide possible, sans qu'aucune ambiguïté ne soit présente, ce qui n'a pas empêché quelques imprévus comme nous le verrons[297].

116. Le décret paru le 28 décembre 2016[298] a créé l'article R. 1461-12 du code de la santé publique. Les auteurs du texte ont choisi d'innover en proposant une présentation des bénéficiaires de l'accès permanents radicalement différente de ce qui semblait être l'usage depuis 2002. En effet, tous les arrêtés parus depuis cette date, jusqu'au dernier arrêté du 6 octobre 2016[299], étaient plutôt difficiles à déchiffrer tant leur rédaction était dense. Chacun de ces arrêtés proposait une liste, ou mettait à jour la liste existante, de tous les acteurs qui pouvaient bénéficier d'un accès permanent aux données de santé. La complexité résidait dans le fait que le type de données accessibles était directement associé aux acteurs concernés. Il en ressortait alors une liste peu digeste pour le profane[300] qui s'avérait même parfois difficile à bien déchiffrer pour les spécialistes. Cette première difficulté que nous pouvons qualifier de barrière rédactionnelle est désormais levée avec la rédaction proposée par le nouveau décret[301].

---

[296] Arrêté du 11 avril 2002, *op. cit*.

[297] *Infra* n° 118.

[298] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

[299] Arrêté du 6 octobre 2016, *op. cit.*

[300] Par exemple, voici des extraits de la liste issue de l'arrêté du 19 juillet 2013, *op. cit.* :

« *Les destinataires des informations contenues dans le Système national d'information interrégimes de l'assurance maladie sont, à raison de leurs fonctions et selon les règles d'habilitation détaillées à l'annexe 2 du protocole :*
1° Pour l'ensemble des informations énumérées à l'article 3, les médecins-conseils et les personnels habilités placés sous leur responsabilité ainsi que les agents administratifs habilités des caisses des différents régimes de base d'assurance maladie ou de la Caisse nationale de solidarité pour l'autonomie nommément désignés, suivant leur rattachement administratif, par les directeurs ou les agents comptables des caisses ;
[…]
4° Pour les données relatives à leur activité, leurs recettes ou leurs prescriptions, l'ensemble des prestataires de soins ; les professions médicales et les pharmaciens ayant seuls accès aux informations médico-administratives (numéro d'affection de longue durée au sens de l'article D. 322-1 du code de la sécurité sociale, numéro de maladie professionnelle, codes de pathologie suivant la codification internationale des maladies en vigueur) ;
[…]
7° Pour l'ensemble des informations énumérées à l'article 3, à l'exclusion de l'échantillon généraliste, sous forme de statistiques agrégées, les données relatives aux bénéficiaires de l'assurance maladie comprenant l'ensemble des données relatives aux professionnels de santé ou aux établissements de santé à l'exclusion de toute donnée d'identification :
– les 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 pour le partage et la mise en commun des données de remboursement agrégées ou individuelles anonymisées issues de leurs systèmes d'information, présentée en annexe 6. »

[301] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

Désormais, deux listes distinctes sont proposées : la première est celle des acteurs qui bénéficient de l'accès permanent aux données de santé, la seconde est celle des caractéristiques des données utilisables par chacun des bénéficiaires. Il en ressort un texte plus simple et aisément compréhensible. Ce choix de rédaction est tout à fait avantageux car il limite les risques de confusion. Ainsi, 25 catégories d'acteurs[302] sont directement visées par le décret et bénéficient depuis son entrée en vigueur fixée au 1er avril 2017 (un retard de quelques mois s'est malheureusement imposé comme précisé ci-après[303]), d'un accès permanent aux données prévues par ledit texte. Cette liste est très variée et ajoute de nombreux bénéficiaires à ceux qui étaient déjà visés avant la réforme : des acteurs comme l'Autorité de sûreté nucléaire, l'Agence nationale de santé publique ou l'Etablissement français du sang font leur apparition. Les équipes de chercheurs de l'Institut national de la santé et de la recherche médicale, des centres hospitaliers universitaires (CHU), des centres de lutte contre le cancer, mais aussi les équipes de recherche et de formation de l'Ecole des hautes études en santé publique (EHESP) bénéficient désormais d'un accès permanent aux données de santé. La liste a été complétée à la

[302] Les 25 catégories d'acteurs prévus par le décret n° 2016-1871 du 26 décembre 2016, *ibid*., sont :

« *1- La direction de la recherche, des études, de l'évaluation et des statistiques, la direction générale de la santé et la direction générale de l'offre de soins, la direction de la sécurité sociale, la direction du budget et le service de santé des armées ;*
2- Les agences régionales de santé ;
3- Les caisses nationales des régimes de l'assurance maladie obligatoire, les organismes locaux et régionaux de l'assurance maladie obligatoire ;
4- La Caisse nationale de solidarité pour l'autonomie ;
5- La Haute Autorité de santé ;
6- L'Autorité de sûreté nucléaire ;
7- L'Agence nationale de santé publique ;
8- L'Agence nationale de sécurité du médicament et des produits de santé ;
9- L'Agence de biomédecine ;
10- L'Institut de radioprotection et de sûreté nucléaire ;
11- L'Institut national du cancer ;
12- L'Etablissement français du sang ;
13- L'Agence technique de l'information sur l'hospitalisation ;
14- L'Agence nationale d'appui à la performance des établissements de santé et médico-sociaux ;
15- L'Institut national des données de santé ;
16- L'Institut de recherche et documentation en économie de la santé ;
17- L'Institut national d'études démographiques ;
18- L'Observatoire français des drogues et toxicomanies ;
19- Le Haut Conseil pour l'avenir de l'assurance maladie ;
20- Le Fonds de financement de la couverture maladie universelle ;
21- Les observatoires régionaux de la santé ;
22- Les unions régionales de professionnels de santé ;
23- Les équipes de recherche de l'Institut national de la santé et de la recherche médicale ;
24- Les équipes de recherche des centres hospitaliers universitaires et des centres de lutte contre le cancer ;
25- Les équipes de recherche et de formation de l'Ecole des hautes études en santé publique. »

[303] *Infra* n° 118.

fin de l'année 2018 par un décret[304] ajoutant à aux bénéficiaires de l'accès permanent la direction générale du Trésor.

117. Le simple changement de présentation des acteurs disposant d'un accès permanent s'accompagne d'un travail de terrain qui consiste dans un suivi accru de la part des équipes chargées de la bonne mise en œuvre de la réforme. M. GIRARD, responsable de la mission « *données de santé* » à la DREES, précise que plusieurs séminaires d'information ont suivi la publication du décret. Ces séminaires[305], organisés avec la CNAM, destinés aux seuls acteurs bénéficiaires des nouveaux accès permanents, ont permis de présenter le nouveau SNDS auprès des participants et de les sensibiliser à la sécurité à mettre en place pour protéger les données. Ces réunions ont permis de rencontrer les bénéficiaires d'un accès permanent, de dialoguer avec eux dans une démarche pédagogique : leurs questions, nombreuses, sont un moyen d'améliorer la compréhension des enjeux de l'accès permanent aux données de santé et du fonctionnement du système. Tout ce travail a été préparé en amont afin que la réforme permette à tous les acteurs de repartir sur des bases saines, claires et bien cadrées.

118. Malgré une préparation intense de la réforme, des retards et des anomalies ont été constatés. L'accès permanent qui devait officiellement être effectif le 1er avril 2017, date d'entrée en vigueur du décret créant le SNDS, a été reporté au mois de septembre 2017. L'ensemble du calendrier initial prévu par la DREES a donc été décalé de plusieurs semaines, voire plusieurs mois : les séminaires n'ont pas souffert de ce retard mais les formations relatives à l'utilisation du SNDS ont été remises à septembre 2017 au lieu du mois de juin de la même année.

Des soucis de transmission de l'information aux bénéficiaires de l'accès permanent ont aussi été relevés. Comme indiqué par M. GIRARD, certains acteurs ne se sont pas présentés aux séminaires d'information. C'était le cas de nombreux CHU au sein desquels l'information n'avait pas été bien diffusée. Les retards pris dans le calendrier de mise en place de l'accès permanent ont donc permis d'organiser des séminaires de rattrapage. L'ensemble du dispositif a été pensé pour que les bénéficiaires de l'accès permanent ne soient pas livrés à eux-mêmes et

[304] Décret n° 2018-1056 du 29 novembre 2018 *complétant le décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »*, JORF, n° 0278, 1er décembre 2018.

[305] Quatre séminaires d'information se sont tenus le 20 mars, le 21 mars, le 24 avril et le 9 juin.

puissent être opérationnels pour utiliser les données de santé mises à disposition aussi rapidement que possible. Cela concerne également les acteurs situés dans les départements et régions d'outre-mer pour lesquels des audio-conférences et des vidéo-conférences ont été organisées.

119. Le travail de pédagogie mené par les équipes de la DREES s'est aussi porté vers les acteurs qui disposaient d'un accès permanent avant la réforme et qui n'en disposent plus. Ainsi, dans la dernière liste des bénéficiaires de l'accès permanent, prévue par l'arrêté de 2013[306], « *l'ensemble des prestataires de soins* » avaient accès aux données relatives à leur activité, leurs recettes ou leurs prescriptions. Désormais, seules les « *équipes de recherche des centres hospitaliers universitaires et des centres de lutte contre le cancer* » ont le droit d'accéder aux données de santé en permanence. De la même manière, l'accès conféré aux « *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* » avant la réforme a maintenant disparu. Un travail d'information destiné à rassurer ces acteurs est mené. En effet, les accès permanents déjà existants avant la réforme de la loi du 26 janvier 2016 demeurent actifs, dans les mêmes conditions, jusqu'en 2019. Tous les anciens bénéficiaires qui ne sont plus cités dans les textes continuent donc d'avoir les mêmes accès. Or, tout est mis en œuvre par les équipes responsables du nouveau SNDS pour que des procédures d'accès simplifiées et rapides[307] soient effectives.

120. La nouvelle présentation des acteurs ayant un accès permanent aux données de santé a donc été pensée pour être facilement comprise et rapidement effective. Le travail de pédagogie qui accompagne les textes est un atout indispensable qui permettra à l'ensemble des bénéficiaires des accès d'être opérationnel avec l'objectif d'exploiter, dans les limites fixées par les textes, tout le potentiel des bases de données en santé. Cette grande ouverture des données de santé accessibles en permanence à un large panel d'acteurs nouveaux est le signe que l'Etat a compris l'importance de maîtriser le parcours des données de santé. Cette maîtrise se traduit nécessairement par le contrôle de l'usage des informations que peuvent avoir les bénéficiaires de l'accès permanent. C'est aussi grâce à cela que la protection de la vie privée des individus peut pleinement s'exercer.

[306] Arrêté du 19 juillet 2013, *op. cit.*

[307] *Infra* n° 413, 420 à 427.

SECTION 2 : LES ACTEURS CENTRAUX DU SERVICE PUBLIC CONTRÔLÉS DANS LEUR USAGE DE L'ACCÈS PERMANENT

121. L'objectif recherché d'amélioration de l'action des acteurs bénéficiaires de l'accès permanent aux données semble accessible dans la mesure où les études qui sont menées utilisent de plus en plus de données (§1), cela se déroule néanmoins dans un cadre très normé de contrôle des individus qui consultent et manient lesdites données (§2).

Paragraphe 1 : L'utilité avérée de l'accès permanent

122. L'existence de l'accès permanent aux données de santé du SNIIRAM, et aujourd'hui du SNDS, a toujours été connue et relatée dans la doctrine depuis sa mise en place[308]. Mais il est moins fréquent de rencontrer des éléments permettant d'attester que cet accès a réellement permis, avec le temps, une amélioration des missions de service public.

123. Sur ce sujet, on peut citer H. KHODOSS qui, dans un article paru en septembre 2004[309], reconnaît l'utilité de disposer de données de santé pour en tirer des statistiques et des études permettant d'améliorer le pilotage de la politique de santé publique. L'auteure isole d'emblée une problématique susceptible d'amoindrir la portée de l'utilité des données de santé pour l'intérêt général : les données de santé sont utilisées pour l'intérêt de la collectivité alors même qu'elles ont bien souvent été produites dans un intérêt thérapeutique individuel. Mais si cette question est pertinente, H. KHODOSS conclut que les professionnels de santé aussi bien que les bénéficiaires du système de santé sont demandeurs d'informations précises qui ouvrent la voie à la définition de politiques de prévention, de gestion de l'offre de soins et du risque sanitaire. Dans l'article, parmi les exemples d'usage des données de santé recueillies et utilisées à des fins de mission de service public se trouve l'usage fait par l'INSERM[310], qui a obtenu l'accès permanent en 2011[311], et dont le travail sur la statistique nationale des causes de décès

[308] DEBOST C. dans son article « Publication du rapport sur la gouvernance et l'utilisation des données de santé, la promesse d'un entrebâillement de l'Open data dans le secteur de la santé ? », *RDS*, janvier 2014, n° 57, p. 947 à 949, évoque notamment des accès permanents « nombreux » sans réellement en dessiner la portée, ni l'impact.

[309] KHODOSS H., « L'exploitation des données de santé », *RGDM*, 30/09/2004, n° 4, p. 65-76.

[310] *Supra* n° 106.

[311] Arrêté du 1er décembre 2011, *op. cit*.

permet d'améliorer la surveillance des cancers. Plus tard, l'InVS[312], dont l'accès permanent a été délivré dès 2002[313], a pu utiliser les données collectées par l'INSERM à des fins de surveillance et d'alerte sanitaire. Ces quelques premiers exemples de missions de service public de santé voient leur efficacité démultipliée par l'obtention de l'accès permanent aux données.

124. La finalité et l'utilité des données de santé accessibles en permanence se retrouve aussi dans une meilleure mesure des inégalités sociales en santé comme le soulignent neuf auteurs dans un article paru en mars 2015[314]. Les organismes bénéficiant de l'accès permanent que sont les ARS et les composantes de l'assurance maladie ont pu accéder à des données de santé du SNIIRAM afin de les utiliser pour réaliser une étude globale sur les inégalités sociales de santé dans une région donnée. La réalisation de telles études est indispensable à la mise en œuvre ultérieure d'une politique cohérente de réduction de ces inégalités. C'est grâce aux informations sur les adresses des individus présentes dans la base de données que des croisements ont pu être réalisés pour obtenir un résultat satisfaisant.

125. Il est remarquable que l'impact, qu'il soit positif, négatif, ou nul, de l'accès permanent aux données de santé ouvert depuis 2002 à certains acteurs n'ait pas fait l'objet d'une littérature plus abondante sur le sujet. En effet, depuis sa mise en place, l'accès permanent aux données de santé n'a été que peu commenté, que ce soit par des tiers ou par les bénéficiaires dudit accès eux-mêmes. Nous aurions pu nous attendre à des analyses relatives à l'évolution des politiques de santé en fonction du développement des accès permanents, ou qui s'intéressent aux liens entre, d'une part, la multiplication des études grâce aux accès permanents et, d'autre part, l'amélioration de l'offre de soins issue d'une connaissance accrue de la situation. Mais, étrangement, l'apport des accès permanents au SNIIRAM dans un objectif d'intérêt général n'a pas été analysé plus concrètement[315]. Ce constat amène plusieurs commentaires de notre part : l'absence d'études relatives à l'impact de l'accès permanent aux données de santé dont les acteurs bénéficient est un symptôme de la difficulté à tirer parti des informations disponibles pour les exploiter au maximum de leur potentiel. En d'autres termes, il est fort probable que la

[312] *Supra* n° 106.

[313] Arrêté du 11 avril 2002, *op. cit*.

[314] DUCROS D., NICOULES V., CHEHOUD H., BAYLE A., SOUCHE A., TANGUY M., VALIERE J.-P., CAYLA F., GROSCLAUDE P., « Les bases médico-administratives pour mesurer les inégalités sociales en santé », *Santé Publique,* 3/2015, Vol. 27, p. 383-394.

[315] *Infra* n° 180 à 182.

masse des données de santé disponibles depuis l'ouverture des accès permanent n'ait pas été entièrement appréhendée et, par conséquent, insuffisamment utilisée. Cette situation révèle également la complexité de la procédure d'accès aux données : les identifier, les sélectionner, les récupérer, les trier, les comprendre puis finalement les utiliser dans le cadre d'une mission spécifique ; toutes ces étapes nécessitent inévitablement du personnel qualifié dont la formation peut être coûteuse et longue. C'est peut-être en partie à cause de cette complexité et de l'absence d'évaluation des bénéfices de l'accès permanent que l'intégralité du système a fait l'objet d'une remise en cause.

Quoi qu'il en soit, l'accès permanent, s'il a été ouvert dans un intérêt général à plusieurs acteurs, ne bénéficie pas sans contrôle à tous les membres de ces acteurs.

Paragraphe 2 : Le contrôle individuel du bénéfice de l'accès permanent

126. L'accès permanent aux données de santé dans un objectif d'améliorer l'action d'acteurs exerçant des missions de service public a été mis en place en raison de l'utilité prévisible de l'usage des informations disponibles. Sa création fut précédée de la rédaction d'un protocole soumis à l'approbation de l'autorité la plus compétente sur le sujet du droit au respect de la vie privée en France : la CNIL.

127. Ce protocole, qui a déjà été présenté dans l'étude[316], a vu sa première version approuvée par délibération de la CNIL le 18 octobre 2001[317]. La CNIL doit nécessairement rendre un avis relatif au protocole, toutefois cet avis reste consultatif. Il est cependant difficile de penser que, suite à un avis défavorable, un arrêté soit pris en application du protocole ayant donné lieu audit avis. Ainsi, en 2001, l'avis rendu était favorable avec quelques réserves portant notamment sur la mise en œuvre effective de toutes les dispositions visant à la sécurité des données prévues par le protocole. On peut voir dans la validation des premiers acteurs qui ont un droit d'accès permanent aux données de santé par la Commission chargée d'assurer le respect de la loi relative à l'informatique, aux fichiers et aux libertés[318], un premier signe fort que la sécurité et

[316] *Supra* n° 95.

[317] Délibération n° 01-54 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 SNIIRAM).

[318] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

le contrôle de l'accès aux données de santé du SNIIRAM n'est pas négligé. Chacun des arrêtés relatifs à l'accès permanent aux données de santé a d'ailleurs systématiquement fait l'objet d'un avis préalable de la CNIL. C'est toujours en tenant compte de cet avis que chaque arrêté a été pris et publié au Journal officiel de la République. Le décret[319] pris pour l'application de l'article 193 de la loi de modernisation de notre système de santé[320] a, lui aussi, fait l'objet d'un avis de la CNIL en date du 13 octobre 2016[321]. Cet avis favorable n'est pas exempt de réserves : ces dernières portent essentiellement sur les modalités de sécurisation des données mises à disposition dans le nouveau SNDS et seront examinées plus en avant dans cette étude[322].

128. Depuis le premier arrêté jusqu'au dernier décret, les textes ont toujours proposé un système alliant une liste d'acteurs bénéficiaires de l'accès permanent avec les modalités de désignation des personnes physiques pouvant réellement avoir un accès au sein desdits acteurs. Cette procédure a pour but de limiter les risques d'un accès non autorisé à des données de santé. Surtout, elle permet de responsabiliser les personnes physiques disposant d'un accès permanent en leur accordant des accès individuels : dans le cas où des données de santé seraient extraites de la base et diffusées à des tiers, la source de la fuite serait plus facilement identifiable. L'objectif est de limiter au maximum les risques pesant sur la sécurité des données et de sensibiliser les personnes physiques bénéficiaires de l'accès permanent au droit au respect de la vie privée. Ainsi, au lancement du système en 2002, les seules personnes aptes à accéder à l'intégralité des informations contenues dans le SNIIRAM étaient les agents des caisses d'assurance maladie et des unions régionales de ces caisses nommément désignés par les directeurs ou les agents comptables des caisses et des unions. Par ailleurs, les personnes autorisées à effectuer des recherches en utilisant plus d'une des trois variables sensibles[323] ne pouvaient être que des médecins-conseils et les personnels placés sous leur responsabilité qui étaient nommément désignés par les médecins responsables. Etant donné la quantité d'informations disponibles pour ce premier accès permanent qui était le plus large possible, la maîtrise des individus ayant l'autorisation de travailler avec ces données paraît un prérequis nécessaire ne serait-ce que pour la traçabilité des usages qui sont faits. Ce mécanisme

[319] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*.

[320] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[321] Délibération n° 2016-316 du 13 octobre 2016 portant avis sur un projet de décret en Conseil d'Etat relatif au Système national des données de santé.

[322] *Infra* n° 145 à 154.

[323] *Infra* n° 142.

d'identification individuelle est reproduit à travers les autres modalités d'accès permanent. Ainsi, les agents du ministère chargé du travail[324] devaient être nommément désignés par les directeurs d'administration centrale ou des services déconcentrés du ministère ; les agents des ARH[325] devaient être nommément désignés par les directeurs de chaque agence ; et les agents du ministère chargé de l'agriculture[326] devaient être nommément désignés par le directeur des exploitations, de la politique sociale et de l'emploi de ce ministère. Dans le même temps, les agents du ministère chargé de l'économie et des finances[327] devaient être nommément désignés par le directeur du budget ou le directeur de la prévision. Etonnamment, tous les membres des unions régionales de médecins libéraux avaient, dès 2002, accès aux données de santé sans à être nommément identifiés. Cette mesure de sécurité démontre l'importance capitale de la maîtrise des accès permanents au sein même des acteurs exerçant des missions de service public. Chaque personne bénéficiaire d'un accès devait être connue : l'une des utilités de ce dispositif est que, en cas de faille dans la protection des données, la source de cette faille peut être identifiée en connaissant directement la personne physique titulaire de l'accès permanent d'origine.

129. Cette mesure d'identification des personnes physiques jouissant de l'accès permanent aux données de santé semblait être la norme dans l'ancien système car l'arrêté de 2014[328] est venu créer un nouvel accès permanent[329] pour les médecins et personnels habilités placés sous leur responsabilité nommément désignés par l'autorité médicale de chacune des ARS participant aux expérimentations relatives aux personnes âgées en perte d'autonomie. Pourtant, la réforme engagée par la loi du 26 janvier 2016[330] a mis en œuvre une simplification dans le dispositif prévu par décret[331]. Au lieu de proposer des modalités de désignation des titulaires de l'accès permanent au sein de chaque acteur public spécialement habilité pour cela, le texte crée un article unique[332] dans le code de la santé publique précisant que les « *responsables des services*

[324] *Supra* n° 104.

[325] *Ibid.*

[326] *Ibid.*

[327] *Ibid.*

[328] Arrêté du 14 février 2014, *op. cit.*

[329] *Supra* n° 107.

[330] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[331] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*.

[332] Il s'agit de l'article R. 1461-16 du code de la santé publique.

de l'Etat, des établissements ou des organismes mentionnés à l'article R. 1461-12[333] *habilitent, sous leur responsabilité, au sein de la structure qu'ils dirigent ou, le cas échéant, dans le cadre d'un contrat de sous-traitance et dans le respect des dispositions de l'article 35 de la loi n° 78-17 du 6 janvier 1978*[334]*, des personnes nommément désignées pour accéder aux données du système national des données de santé. Le nombre des personnes habilitées est limité à ce qui est strictement nécessaire pour assurer l'exécution des traitements de données autorisés. Ces personnes doivent avoir été spécialement formées, dans le cadre de leurs fonctions, pour l'accomplissement de leurs missions* ». L'effet est en réalité le même tout en permettant une lecture plus limpide de la marche à suivre. Ainsi, tous les acteurs bénéficiaires de l'accès permanent, sans exception, ce qui inclut cette fois-ci les unions régionales de professionnels de santé, doivent constituer une liste des personnes physiques nommément désignées qui reçoivent une habilitation à faire usage de l'accès permanent. Une précision supplémentaire indique qu'il existe des limites aux personnes nommément désignées : seul le nombre de personnes nécessaire doit recevoir une habilitation. Cependant, aucune interprétation n'est donnée quant aux éléments permettant de mesurer le nombre de personnes « *strictement nécessaire pour assurer l'exécution des traitements de données autorisés* ». Toutes les personnes identifiées et nommées doivent finalement être renseignées dans un document spécifique décrivant leurs accès, les modalités de gestion et de contrôle de leurs habilitations. Ces listes devront être consultables sur le site du SNDS et la CNIL pourra en demander une copie à tout moment. Cette généralisation de l'individualisation de l'accès permanent aux données de santé est très importante s'agissant du respect du droit au respect de la vie privée car chaque personne autorisée est formée et sensibilisée aux problématiques qui en découlent. Cela permet également de détecter plus facilement les éventuels accès non autorisés. Le mécanisme n'en demeure pas moins critiquable en certains points comme nous le verrons plus loin dans l'étude[335].

---

[333] L'article R. 1461-12 du code de la santé publique dresse la liste exhaustive des bénéficiaires de l'accès permanent au SNDS. v. *supra* n° 116.

[334] L'article 35 de la loi n° 78-17 du 6 janvier 1978, *op. cit*., est devenu l'article 122 depuis l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit*. Il dispose notamment que seul le responsable de traitement peut donner à un sous-traitant ou à une personne agissant sous son autorité l'instruction d'effectuer un traitement de données à caractère personnel. Ainsi, des garanties suffisantes doivent être présentées par le sous-traitant pour assurer le respect des règles de sécurité et de confidentialité. Le responsable de traitement doit cependant continuer à veiller au respect de ces mesures, nonobstant les garanties présentées par le sous-traitant.

[335] V. Partie I, Titre II.

130. Un autre point crucial de la réforme mettant en œuvre le SNDS est l'obligation pour tous les bénéficiaires chargés d'une mission de service public et cités par l'article R. 1461-12 du code de la santé publique de nommer en leur sein un correspondant informatique et libertés[336]. C'est ce correspondant, identifié physiquement dans chaque structure, qui est responsable de la mise à jour de la liste et des caractéristiques de chaque traitement qui porte sur des données individuelles du SNDS et mis en œuvre dans le cadre de l'accès permanent. Cette liste doit être transmise chaque année à un comité stratégique comprenant des représentants des organismes responsables des bases de données alimentant le SNDS, le président de l'INDS et une personnalité qualifiée[337]. Les membres de ce comité doivent être définis par arrêté.

131. L'objectif de tout ce dispositif, qui va de la désignation de chaque organisme bénéficiaire de l'accès permanent, à la désignation de chaque personne pouvant jouir de cet accès en interne, à la publication de la liste de ces personnes, puis au suivi des traitements mis en œuvre par l'obligation de désigner un correspondant informatique et liberté, est de garder le contrôle sur les données qui sont diffusées. En effet, l'extension importante de l'accès permanent aux données de santé à de nombreux acteurs est source de craintes sur la sécurité des informations et sur le respect de la vie privée des individus dont les données sensibles sont traitées. C'est pour cela que le décret mettant en place le SNDS et les nouveaux accès permanents se veut clair et exhaustif dans le contrôle des accès permanents qui sont autorisés : l'objectif final est alors de maîtriser et prévenir les risques d'atteinte à la vie privée des individus à l'origine des données de santé accessibles.

[336] Le correspondant informatique et libertés ou CIL est né avec 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. C'est le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui a permis la mise en place effective du CIL. Ses missions sont d'abord d'être le référent de la structure en matière de questions de protection des données personnelles. Il doit conseiller son organisme sur la façon d'exploiter les données et sa présence est un facteur de confiance rassurant. Le CIL a été remplacé par le DPO (Délégué à la protection des données) avec l'entrée en vigueur du Règlement 2016/679, *op. cit.*

[337] La création du comité stratégique est prévue par l'article R. 1461-10 du code de la santé publique.

CONCLUSION DU CHAPITRE I

132. L'accès permanent aux données de santé contenues dans les bases de données médico-administratives est né de la volonté d'améliorer le fonctionnement du service public. La mise en œuvre de ce mécanisme n'a pu se faire que dans le respect du droit au respect de la vie privée des individus. Or, les données de santé comprises dans le champ de l'accès permanent, si elles ne sont ni nominatives, ni directement identifiantes, demeurent à caractère personnel en ce qu'elles sont indirectement identifiantes. Il en découle des obligations en matière de sécurité et de contrôle des accès et de l'utilisation faite des données rendues accessibles : les contrôles individuels permettent ainsi de vérifier directement les utilisations faites par les membres des acteurs bénéficiaires d'un accès permanent.

133. La délivrance des premiers accès permanents avec la parution de l'arrêté du 11 avril 2002[338] a été assortie de limites strictes. Seule une liste exhaustive d'acteurs spécialement désignés par arrêté est bénéficiaire de l'accès permanent aux données de santé, et un encadrement spécifique est mis en place pour contrôler les accès et l'usage qui est fait des données. La liste des acteurs bénéficiaires de l'accès permanent a beaucoup évolué au fil des dix arrêtés parus entre 2002 et 2016. Cette évolution a été marquée par de nombreux ajouts progressifs qui montrent une certaine désorganisation dans la construction du dispositif : à titre d'exemple, certains acteurs essentiels de l'organisation du système de santé manquaient à l'appel dans la liste du premier arrêté[339].

134. L'étendue des données de santé accessibles est aussi un facteur crucial. Pour que le fonctionnement du service public soit amélioré, il faut que les données aient une utilité à être traitées : l'intérêt de traiter les données de santé des bases médico-administratives a été très tôt reconnu. Cependant, l'impact réel de l'ouverture des accès permanents n'a fait l'objet d'aucun suivi ni d'aucune mesure : c'est un symptôme supplémentaire de la mauvaise organisation du dispositif.

[338] Arrêté du 11 avril 2002, *op. cit*.

[339] *Supra* n° 104.

135. La réforme du 26 janvier 2016[340] s'est montrée salutaire en ce qu'elle permet de rénover l'accès permanent aux données de santé en repartant sur une base textuelle unie, bien qu'un ajout ait déjà été effectué à la fin de l'année 2018[341]. Elle introduit également un suivi individuel des personnes physiques qui accèdent aux données de santé dans le cadre de l'accès permanent : l'ensemble des informations est centralisé par le SNDS. Le mécanisme rénové entend véritablement démocratiser l'accès aux données de santé et leur traitement par les acteurs qui ont un accès permanent. Un autre aspect de cet accès entre toutefois en ligne de compte et doit être appréhendé : il s'agit du type de données auxquelles ces acteurs peuvent accéder.

[340] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[341] Décret n° 2018-1056 du 29 novembre 2018 *complétant le décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »*, *op. cit.*

CHAPITRE II
L'ACCÈS PERMANENT PRUDEMMENT OUVERT AU NOM DE LA SÉCURITÉ DES DONNÉES

136. Le bénéfice de l'accès permanent aux données de santé doit nécessairement être maîtrisé et contrôlé afin de s'assurer du respect des normes nationales et internationales en matière de sécurité des informations. Ce contrôle est multiple : il y a d'un côté celui sur les acteurs qui bénéficient de l'accès permanent qui vient d'être étudié[342], de l'autre celui sur les données de santé mises à disposition de manière permanente. Le premier ayant déjà été analysé[343], il convient de s'intéresser au second. C'est en premier lieu la question de la sécurité des données accessibles en permanence qui sera étudiée (Section 1), cette sécurité a un impact direct sur le contenu des données de santé accessibles que nous analyserons ensuite en traitant de leur élargissement parfois balbutiant jusqu'à la réforme de la loi du 26 janvier 2016[344] (Section 2).

SECTION 1 : LA PRUDENCE : LA SÉCURISATION PRIORITAIRE DES DONNÉES DE SANTÉ

137. Lors de la création des premiers accès permanents aux données contenues dans le SNIIRAM, la première question à traiter fut celle de la manière dont les informations devaient être sécurisées. Cette sécurisation qui reste d'actualité propose plusieurs caractéristiques que nous analyserons à travers la nature des traitements préalables des données, puis par le prisme des modalités de suivi des usages dont les bénéficiaires d'un accès permanent peuvent faire de ces données (§1). Ces mesures ne sont toutefois pas immuables et nécessitent une remise en cause régulière à une époque où l'évolution des technologies est permanente, nous aborderons donc l'évolution de ces dispositifs de sécurité jusqu'à la réforme de la loi de modernisation de notre système de santé[345] qui a fait l'objet d'une réserve très importante de la part de la CNIL (§2).

[342] V. Partie I, Titre I, Chapitre I.

[343] *Ibid.*

[344] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[345] *Ibid.*

Paragraphe 1 : Le double contrôle des données accessibles en permanence

138. Les données de santé à caractère personnel sont des données sensibles[346] qui, comme nous l'avons déjà abordé en introduction[347], ne doivent pas être récoltées ni faire l'objet d'un traitement en principe. Cependant, dès lors qu'une exception à ce principe est créée pour des motifs légitimes, elles doivent nécessairement être traitées de manière à protéger la vie privée des individus auxquels elles peuvent être liées. L'encadrement de l'utilisation de ces données relève aussi bien du droit national avec la loi relative à l'informatique et aux libertés, que du droit international avec la directive européenne de 1995[348] ou plus récemment le règlement européen de 2016[349]. Ces données sont donc soumises à des modalités de contrôle très strictes de la part des autorités françaises afin d'éviter que les acteurs qui disposent d'un accès permanent ne puissent violer la loi. L'existence de ces mesures de sécurité a, par ailleurs, probablement conditionné la validation de l'arrêté du 11 avril 2002[350] par la Commission Nationale de l'Informatique et des Libertés qui a rendu sa délibération du 18 octobre 2001[351]. Dans cette délibération, la CNIL se prononce sur les dispositions prises pour garantir l'anonymat des bénéficiaires de soins, y compris dans le cadre de l'accès permanent aux données. Elle considère que « *eu égard à la finalité statistique assignée par la loi au dispositif, à la sensibilité des informations appelées à figurer dans le SNIIRAM et aux modalités d'exploitation de celles-ci, la mise en œuvre de l'ensemble* [des mesures de sécurité] *est nécessaire et adaptée pour garantir de façon satisfaisante l'anonymat des données concernant les bénéficiaires de soins* ». La maîtrise des données de santé accessibles en permanence s'illustre par la mise en place de deux types de contrôles que nous aborderons successivement : le premier est un contrôle en amont, qui s'exerce sur le contenu même des données de santé mises à disposition ; le second est un contrôle *a posteriori* qui concerne la vérification de l'utilisation que font les acteurs des données accessibles en permanence.

139. Ainsi, depuis le lancement de l'accès au SNIIRAM, toutes les données proposées en accès permanent sont sujettes à plusieurs traitements avant d'être mises en ligne. Toutes les données

---

[346] *Supra* n° 32 à 35.

[347] *Supra* n° 60.

[348] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[349] Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016, *op. cit.*

[350] Arrêté du 11 avril 2002, *op. cit*.

[351] Délibération n° 01-54 du 18 octobre 2001, *op. cit*.

de santé individuelles se sont vu retirer leur caractère nominatif et sont identifiées par un numéro d'anonymat chiffré : les informations comme le nom, le prénom, la date et le lieu de naissance ou encore le NIR[352] sont donc absentes du SNIIRAM. Dès lors, on peut parler de données de santé anonymisées, ou pseudonymisées[353]. Le chiffrement utilisé en 2002, dénommé FOIN (fonction d'occultation des informations nominatives) et recommandé alors par la CNIL est irréversible et doit empêcher de faire une table de correspondance entre les identifiants de départ de chaque donnée et leur numéro d'anonymat. Comme le note P.-L. BRAS dans son rapport[354], il n'est, en principe, pas possible de revenir au NIR à partir de l'identifiant provenant du SNIIRAM. Il précise que l'algorithme est utilisé par deux fois[355] avec des clés uniques détenues par des personnes différentes. Ce dispositif a prouvé sa valeur mais semble avoir atteint ses limites en raison de l'évolution parallèle des techniques informatiques de plus en plus sophistiquées. C'est pour cette raison que le programme de chiffrement FOIN qui était recommandé depuis 2002 a fait l'objet de réserves de la part de la CNIL dans son avis[356] relatif au décret du 26 décembre 2016[357]. Ces réserves, et leurs conséquences sur le nouveau SNDS seront abordées plus tard dans l'étude[358].

Les données relatives aux professionnels de santé font également l'objet d'un traitement préalable avant d'être intégrées au SNIIRAM. Les informations concernant le nom et le prénom de chaque praticien ne figurent pas dans les fichiers. Malgré cela, les données conservent un caractère indirectement identifiant notamment par le biais d'informations sur la date de naissance ou le sexe du praticien qui demeurent accessibles.

140. En plus de ce traitement, en amont, de l'intégralité des données de santé accessibles en permanence, la question de la durée de conservation des données s'est aussi imposée comme un facteur de sécurisation. Il a donc été prévu que les données auraient une durée de

[352] Le NIR est défini par l'Institut national de la statistique et des études économiques (INSEE) comme étant le Numéro d'inscription au répertoire qui lie chaque individu au Répertoire national d'identification des personnes physiques (RNIPP). Ce numéro unique est composé de 13 chiffres.

[353] *Supra* n° 36 à 39.

[354] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*

[355] Dans son Rapport du Haut Conseil de la Santé publique de mars 2012, *op. cit.,* M. GOLDBERG indique, à la page 17, que les deux étapes de l'anonymisation des données sont les suivantes : la première est au niveau locorégional, appelée FOIN-1, la seconde est réalisée au niveau national, appelée FOIN-2.

[356] Délibération n° 2016-316 du 13 octobre 2016, *op. cit.*

[357] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*.

[358] *Infra* n° 436 à 440.

conservation ment définie : deux ans, au-delà de l'année en cours, pour les données individuelles des bénéficiaires ; et dix ans, au-delà de l'année en cours, pour les données des professionnels de santé. Toutes les données de santé accessibles via l'accès permanent étaient donc, par définition, limitées dans le temps. Comme nous le verrons[359], ce facteur de conservation limitée posera question et sera vite soumis à évolution.

141. A ce premier contrôle *a priori* qui encadre le contenu des données accessibles en permanence s'ajoutent une deuxième strate toute aussi importante de régulation. Des mesures ont en effet été prises pour que les bénéficiaires de l'accès permanent ne soient pas totalement libres d'utiliser les données récupérées comme ils l'entendent. Des limites techniques ont donc été créées dès le premier arrêté du 11 avril 2002[360] et reproduites, avec quelques évolutions, jusqu'à la réforme de 2016[361].

142. La première de ces limites a trait au nombre critères différentes que les acteurs qui ont un accès permanent peuvent croiser pour effectuer des recherches. Le risque de réidentification demeure présent, malgré le chiffrement préalable des données via l'algorithme FOIN, et plus une base de données est importante et exhaustive, comme c'est le cas du SNIIRAM, plus le risque de réidentification est grand[362]. Par conséquent, les arrêtés relatifs aux accès permanents ont parfois fait mention d'individus directement identifiables titulaires d'un accès spécifique à des données de santé. Ces personnes, spécialement identifiées[363] et habilitées, ont donc la possibilité d'effectuer une recherche d'informations, parmi toutes les données, qui recouperait plus d'une des trois variables sensibles avec d'autres données. Ces trois variables sensibles sont le code de la commune, la date des soins, le mois et l'année de naissance. Ainsi, bien conscient du risque de réidentification, ce malgré l'affirmation de l'article L. 161-28-1 du code de la sécurité sociale selon lequel les « *données reçues et traitées par le système national d'information interrégimes de l'assurance maladie préservent l'anonymat des personnes ayant bénéficié des prestations de soins* »[364], le législateur a prévu que tout accès permanent, le plus

[359] *Infra* n° 149.

[360] Arrêté du 11 avril 2002, *op. cit*.

[361] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[362] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit*. p. 28.

[363] *Supra* n° 128 et 129.

[364] Dernier alinéa de l'article L. 161-28-1 du code de la sécurité sociale dans sa version en vigueur du 27 décembre 1998 au 7 août 2004.

étendu soit-il, ne permette pas de croisements de données trop variés afin de ne pas risquer de permettre de porter atteinte au droit au respect de la vie privée des individus.

143. Au-delà de cette première sécurité, la majorité des bénéficiaires d'un accès permanent n'a accès qu'à des données spécifiquement décrites par arrêté. L'arrêté du 11 avril 2002[365] impose à presque tous les bénéficiaires (les médecins-conseil et le personnel de l'assurance maladie disposent d'un accès[366] aux données individuelles) de n'accéder qu'à des données présentées sous une forme de de statistiques agrégées : comme l'écrit P.-L. BRAS dans son rapport[367], « *le risque* [de réidentification] *diminue ou disparaît lorsque les données sont agrégées* ». Certains bénéficiaires de l'accès permanent ont même été limités à des données statistiques agrégées à la fois pour les données individuelles et pour les données relatives aux professionnels de santé et aux établissements de santé : il s'agit des agents du ministère chargé de l'économie. Dans le même temps, l'accès aux données non agrégées relatives aux professionnels de santé a été autorisé « *à l'exclusion de toute donnée d'identification* ». Un autre critère limitatif est imposé aux unions régionales de médecins libéraux s'agissant des données des professionnels de santé : les unions ne peuvent consulter que les informations relatives aux professionnels de leur région. L'existence de ces restrictions supplémentaires démontre la lourde tâche qui consiste à sécuriser un accès permanent à des données sensibles.

144. La volonté de maîtriser le parcours des données de santé accessibles en permanence est bien prégnante depuis la création des accès. Cette sécurisation se retrouve dans chaque nouveau texte et n'a cessé d'évoluer pour s'adapter à la nature des nouveaux acteurs bénéficiaires d'un accès permanent mais aussi aux besoins exprimés par ces mêmes acteurs. Il convient donc d'analyser les changements successifs apportés à la sécurité du dispositif jusqu'aux dernières décisions prises par la CNIL[368].

[365] Arrêté du 11 avril 2002, *op. cit*.

[366] *Supra* n° 104.

[367] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.*

[368] Nous pouvons citer notamment la décision n° MED-2018-006 du 8 février 2018 mettant en demeure la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés, ainsi que les réserves émises à propos du décret relatif au SNDS dans la délibération n° 2016-316 du 13 octobre 2016, *op. cit.*

Paragraphe 2 : La nécessaire mise à l'épreuve de la sécurisation des données

145. Toutes les mesures de sécurité prises lors de la création de l'accès permanent aux données de santé pour des missions de service public ne sont pas immuables. Rappelons que les données récoltées et proposées dans le SNIIRAM afin d'être mises en accès permanent à des fins de service public sont des données sensibles[369]. C'est-à-dire qu'elles font apparaître, directement ou indirectement des informations sur la santé des individus qu'elles concernent. Pour pouvoir assumer le principe selon lequel toutes ces données sont accessibles de manière permanente, le législateur a dû s'adapter à chaque évolution textuelle. Lors de la mise en place des premiers accès, aussi bien la loi relative à l'Informatique aux fichiers et aux libertés[370] que la directive européenne de 1995[371], interdisaient (ce qui est toujours le cas) aux Etats membres de créer des traitements de données à caractère personnel relatives à la santé. C'est dans le cadre d'une dérogation prévue par le droit européen que le système français a pu voir le jour. Ladite directive prévoit[372] en effet que, si les garanties appropriées sont apportées, un Etat membre peut créer, pour un motif d'intérêt public, une dérogation à l'interdiction de principe. Dès lors, il est compréhensible que, ne serait-ce que pour justifier la création du SNIIRAM, la liste des finalités prévues par l'arrêté du 11 avril 2002[373] s'inscrive dans une logique d'intérêt général, et donc d'intérêt public. La création d'accès permanents, contrôlés et vérifiés, à des fins de service public, permet en outre d'asseoir la légitimité de cette dérogation au principe d'interdiction.

146. Plus récemment, le Règlement européen du 27 avril 2016[374] est venu réaffirmer cette possibilité de dérogation « *sous réserve de garanties appropriées, de manière à protéger les données à caractère personnel et d'autres droits fondamentaux, lorsque l'intérêt public le commande, notamment le traitement des données à caractère personnel dans le domaine* […] *du droit de la protection sociale* […] *et à des fins de sécurité, de surveillance et d'alerte sanitaire, de prévention ou de contrôle de maladies transmissibles et d'autres menaces graves pour la santé* ». Le texte renchérit en indiquant notamment que les « *catégories particulières*

[369] *Supra* n° 58 à 60.

[370] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, article 8, devenu l'article 6 depuis l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[371] Directive 95/46/CE du 24 octobre 1995, *op. cit.*.

[372] *Ibid.*, article 8.

[373] Arrêté du 11 avril 2002, *op. cit.*

[374] Règlement 2016/679 du Parlement européen, *op. cit.*, considérant 52.

de données à caractère personnel qui méritent une protection plus élevée ne devraient être traitées qu'à des fins liées à la santé, lorsque cela est nécessaire pour atteindre ces finalités dans l'intérêt des personnes physiques et de la société dans son ensemble, notamment dans le cadre de la gestion des services et des systèmes de soins de santé ou de protection sociale »[375].

147. Le législateur français s'est donc rapidement retrouvé dans un étau pour faire évoluer les accès permanents aux données de santé : l'objectif du dispositif est à la fois de permettre à tous les acteurs qui en ont une utilité d'exploiter un maximum de données au bénéfice de l'intérêt général, mais aussi de s'assurer que toutes les protections et restrictions soient mises en œuvre pour protéger l'intégrité des données et être ainsi conforme aux droits européen et français. En plus des mesures de sécurité initiales mises en place[376], de nouvelles propositions ont donc été faites pour concilier l'accès permanent à plus d'informations avec le maintien d'un bon niveau de protection de ces informations.

148. La première évolution du type de données accessibles en permanence est la création de l'EGB, ou échantillon général des bénéficiaires, par l'arrêté du 20 juin 2005[377]. Cet échantillon regroupe des données anonymisées et agrégées au 1/97[e] relatives aux personnes protégées par les régimes d'assurance maladie. Au moment de sa création, l'EGB représentait une amélioration significative car il permettait aux acteurs bénéficiaires d'accéder librement à des données sécurisées. En effet, le processus d'agrégation de données consiste à traiter des informations individuelles pour en proposer une représentation globale anonymisée. Cela permet notamment d'obtenir des informations sur des groupes d'individus aux caractéristiques communes. Signalons que la durée de conservations des données agrégées dans l'EGB a été fixée à vingt ans lors de sa création pour être légèrement modifiée aujourd'hui à « *dix-neuf ans en plus de l'année en cours* »[378]. Cela signifie que tous les échantillons créés ne peuvent être mis en accès permanent plus de vingt ans. Cette maîtrise de la durée de conservation des échantillons est un marqueur supplémentaire de sécurité. L'EGB semble avoir prouvé son utilité et son inviolabilité car il est toujours utilisé dans le cadre du nouveau SNDS[379] qui propose

[375] *Ibid.*, considérant 53.

[376] *Supra* n° 138 à 144.

[377] Arrêté du 20 juin 2005, *op. cit*.

[378] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*, dernier alinéa de l'article R. 1461-4 du code de la santé publique.

[379] *Ibid.*, article R. 1461-14 du code de la santé publique.

désormais plusieurs « *échantillons généralistes représentatifs de l'ensemble des bénéficiaires de l'assurance maladie* », ce qui nous permet maintenant de parler de plusieurs EGB au lieu d'un seul.

149. La deuxième évolution constatée vise la durée de conservation des données accessibles en permanence qui ne concerne pas seulement les échantillons. Elle porte sur toutes les données de santé contenues dans le SNIIRAM. Rappelons qu'initialement cette durée était de deux ans[380], les données étaient ensuite archivées pour dix ans et ne pouvaient faire l'objet d'un accès permanent. Or, la première modification du temps de conservation apparue dans l'arrêté du 1er décembre 2011[381] est directement liée à l'actualité du scandale du Mediator[382] qui a mis en lumière de larges prescriptions de ce médicament, un antidiabétique, en dehors du cadre d'autorisation de mise sur le marché (le Mediator était bien trop souvent prescrit comme coupe-faim) qui a provoqué des valvulopathies chez de nombreux patients. Alors que ledit médicament a été retiré du marché français le 30 novembre 2009, la récupération de données sur le sujet, pour effectuer des études sur les risques cardiaques que sa consommation présentait, était de plus en plus problématique. L'arrêté relatif à la mise en œuvre du SNIIRAM paru en 2011 a alors étendu la durée de conservation de toutes les données individuelles relatives aux bénéficiaires à trois ans au-delà de l'année en cours. Une fois ce délai dépassé, les données sont archivées pour dix ans supplémentaires. Cette augmentation du temps de conservation des données individuelles indique que les pouvoirs publics prenaient enfin conscience de l'utilité que pouvait avoir la base de données constituée en 2002 pour les études, notamment dans le secteur pharmaco-épidémiologique.

Ce temps de conservation des données individuelles de trois ans a été maintenu jusqu'à la réforme du 26 janvier 2016 qui propose aujourd'hui une durée de « *dix-neuf ans en plus de*

---

[380] *Supra* n° 140.

[381] Arrêté du 1er décembre 2011 relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie, *op. cit.*

[382] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 17. v. notamment CE, 1ère et 6e ch. réunies, 9 nov. 2016, n° 393108 : JurisData n° 2016-024113 ; CE, 1ère et 6e ch. réunies, 9 nov. 2016, n° 393902, 393926 : JurisData n° 2016-023458 ; CE, 1ère et 6e ch. réunies, 9 nov. 2016, n° 393904 : JurisData n° 2016-024909 ; J.-C. ROTOULLIE, « Affaire du Mediator : la responsabilité de l'Etat précisée », *JCPG*, n° 3, 16/01/2017 ; C. LANTERO, « L'affaire du Mediator : la police et la peur du risque », *Droit administratif*, n° 1, 01/2017 ; H. ARBOUSSET, « Mediator et indemnisation des victimes : retour sur une affaire d'Etat », *JCPA*, n° 50, 12/12/2011 ; J. KNETSCH, « Le nouveau dispositif d'indemnisation des victimes du Mediator issu de la loi du 29 juillet 2011 », *Responsabilité civile et assurances*, n° 12, 12/2011 ; B. RAJOT, « Le Mediator : antidiabétique ou coupe-faim ? Indemnisation des victimes et/ou responsabilités des professionnels de santé ? Vastes discussions en perspective… » ; *Responsabilité civile et assurances*, n° 6, 06/2011.

l'année au cours de laquelle elles ont été recueillies »[383]. Au-delà, elles sont archivées « *de façon à rester utilisables pour une durée de dix ans* »[384]. Une grande incertitude demeure cependant : qu'arrive-t-il aux données de santé qui ont dépassé leur durée d'archivage ? Sont-elles purement et simplement supprimées ? Ou restent-elles stockées dans une base de données entièrement fermée ? Aucune information n'est délivrée par aucun texte à ce sujet. Juridiquement, les données devraient faire l'objet d'une suppression totale sans qu'aucune trace ne soit conservée. Cependant, le fait que rien ne soit écrit laisse planer un doute quant à l'avenir des données de santé qui dépasseraient le délai d'existence de trente ans (si l'on additionne la durée de conservation dans le SNDS puis la durée d'archivage). Toujours est-il que l'allongement de la durée de conservation des données de santé est un élément qui peut augmenter les possibilités d'atteinte à la vie privée des individus : plus la profondeur est grande et plus la quantité de données disponibles est importante. C'est pour cette raison que les autres mesures destinées à sécuriser les données ont aussi été modifiées, que cela concerne le contrôle individuel des accès permanents[385] ou celui sur le contenu même des données et l'usage qui en est fait[386].

150. La troisième évolution a trait à la restriction du nombre de variables sensibles qui peuvent être utilisées simultanément pour faire une recherche, qui, comme nous l'avons vu, fait partie des modalités de sécurisation des données de santé accessibles en permanence[387]. Initialement fixée à trois variables sensibles, cette limite a été portée à quatre par l'arrêté du 16 octobre 2008[388]. Les données sensibles concernées sont alors le code de la commune, la date des soins, le mois et l'année de naissance, ainsi que la date de décès. Le nouveau système mis en œuvre par le décret du 26 décembre 2016[389] est venu réformer ce mécanisme qui permet de contrôler les risques de réidentification. En effet, l'article R. 1461-11 du code de la santé publique créé par ledit décret prévoit au 2° du I que les variables sensibles sont désormais appelées « *identifiants potentiels, dont la combinaison accroît le risque de réidentification* ». La liste de

[383] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*, dernier alinéa de l'article R. 1461-4 du code de la santé publique.

[384] *Ibid.*

[385] *Supra* n° 126 à 131.

[386] *Supra* n° 138 à 144.

[387] *Supra* n° 142.

[388] Arrêté du 16 octobre 2008, *op. cit.*

[389] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*.

ces identifiants potentiels est donc proposée, elle reprend les quatre variables sensibles déjà prévues par le décret de 2008 et en ajoute de nouvelles : ce sont « *la période de naissance exprimée en mois et année, le code de la commune de résidence et les données infracommunales de localisation, la date des soins, la date du décès et le code de la commune de décès* ». Il est précisé que chaque acteur bénéficiaire de l'accès permanent reçoit un accès spécifique qui lui permet, ou non, d'utiliser de manière simultanée plusieurs de ces identifiants potentiels. Cette nouvelle rédaction est la bienvenue car elle est claire, précise, et propose davantage de données à croiser tout en indiquant que chaque acteur se voit remettre sa propre feuille de route quant à l'utilisation qu'ils peuvent faire de ces identifiants potentiels.

151. La création du nouveau SNDS par la loi du 26 janvier 2016 a aussi présenté une occasion au législateur de proposer une évolution supplémentaire avec un la création d'un nouveau critère de sécurité : celui de la profondeur historique des données de santé[390]. Cette notion n'était pas mentionnée jusqu'alors et permet de définir une date à partir de laquelle les données ne peuvent plus être récupérées. Par exemple, si une profondeur historique est fixée à vingt ans, cela signifie que l'acteur qui souhaite effectuer un traitement ne peut accéder qu'à des données qui ont été produites il y a vingt ans ou moins. Ce critère permet de contrôler d'une manière plus restrictive l'étendue des informations auxquelles peuvent accéder les bénéficiaires d'un accès permanent. Cette maîtrise de la profondeur historique des données utilisées est un marqueur supplémentaire de sécurité qui s'ajoute au contrôle de la durée de conservation des informations dans le SNDS. Selon le type d'acteur, la profondeur historique va de 5 ans en plus de l'année en cours jusqu'à 19 ans en plus l'année en cours : cela permet au législateur de définir en amont l'historicité des données de santé auxquelles les bénéficiaires de l'accès permanents peuvent prétendre. Il s'agit là d'un élément supplémentaire qui permet de compartimenter davantage les types d'accès permanents pour les sécuriser et limiter au maximum les risques d'utilisation non conforme qui pourrait porter atteinte au droit au respect de la vie privée. Signalons que, quel que soit le bénéficiaire de l'accès permanent, la profondeur historique des EGB est toujours de 19 ans en plus de l'année en cours.

152. La sécurisation de l'accès permanent aux données de santé tient aussi au fait que la gestion de la base qui regroupe toutes les données de santé mises à disposition fasse l'objet d'un contrôle total. Dans le cadre de la réforme, un référentiel de sécurité a donc été pris le 22 mars

[390] *Ibid.,* article R. 1461-13 du code de la santé publique.

2017[391] afin de fixer durablement toutes les règles à respecter. Ce référentiel définit toutes les exigences reposant sur les gestionnaires de chacun des systèmes reliés au SNDS. Toutes les procédures et les engagements à tenir concernant le transfert de données, l'accès aux données, leur conservation, leur traçabilité mais aussi les modalités de contrôle par des audits internes et externes sont prévus par le référentiel. Bien que cela ne concerne pas uniquement l'accès permanent aux données de santé, cette nouvelle mesure est primordiale car elle fait reposer la responsabilité de l'intégrité des données à la fois sur les gestionnaires du SNDS et sur les acteurs qui accèdent aux informations.

153. Malgré toutes les nouvelles dispositions prises pour assurer le contrôle et la sécurité des données de santé accessibles en permanence, la CNIL a détecté une faille importante. Le système de pseudonymisation utilisé depuis 2002[392] serait devenu obsolète et ne permettrait plus d'assurer une protection suffisante contre les risques de réidentification. Dans son avis rendu le 13 octobre 2016[393] sur le projet de décret relatif au SNDS, la CNIL indique en effet que le système de chiffrement qui permet d'anonymiser les données de santé individuelles n'est plus optimal et, compte tenu des nouvelles technologies qui fleurissent dans le domaine des données massives, doit impérativement être retravaillé. Il est vrai que quinze années se sont déjà écoulées depuis la mise en place du FOIN[394] et, comme le haut conseil de la santé publique le signalait dès 2012, « *la richesse et la diversité des données, qui s'accroît régulièrement grâce aux appariements avec d'autres bases et à l'augmentation récente de la profondeur de durée de conservation du SNIIR-AM, rendra de plus en plus techniquement possible l'identification indirecte des personnes par croisement des données les concernant* »[395]. La réserve émise par la CNIL a bien été prise en compte. Comme nous l'a indiqué M. GIRARD, responsable de la mission « données de santé » à la DREES, la CNAM a enclenché, dès le mois de juin 2017, les premiers travaux de réflexion autour d'un nouveau moyen de pseudonymisation des données de santé. Cependant, le travail qui doit être accompli est « *colossal* » en raison de l'impact que la mise en place d'un nouveau processus de chiffrement aura sur l'ensemble des informations.

---

[391] Arrêté du 22 mars 2017 *relatif au référentiel de sécurité applicable au Système national des données de santé*, *JORF*, n° 0071 du 24/03/2017.

[392] *Supra* n° 139.

[393] Délibération n° 2016-316 du 13 octobre 2016 portant avis sur un projet de décret en Conseil d'Etat relatif au Système national des données de santé.

[394] *Supra* n° 139.

[395] GOLDBERG M., *Rapport du Haut Conseil de la Santé publique de mars 2012*, *op. cit.*

En effet, une fois que le nouveau mécanisme d'anonymisation sera défini, toutes les données du SNDS potentiellement exploitables devront être traitées pour correspondre à cette nouvelle norme : cela concernera donc à la fois les données directement consultables, mais aussi les données archivées, pouvant remonter à trente années. La CNAMTS envisageait probablement de préparer la mise à niveau du mécanisme de chiffrement des données de santé à caractère personnel dans un délai de plusieurs mois, mais la mise en demeure délivrée par la CNIL au début de l'année 2018[396] a sans doute bousculé l'emploi du temps initialement fixé. En effet, dans sa décision, la CNIL donnait trois mois à la CNAMTS pour « *prendre toute mesure pour garantir la sécurité et la confidentialité des données à caractère personnel traitées* ». La CNIL dénonçait « *les multiples insuffisances en termes de sécurité concernent, notamment, la pseudonymisation des données, les procédures de sauvegarde, l'accès aux données par les utilisateurs du SNIIRAM et par des prestataires, la sécurité des postes de travail des utilisateurs du SNIIRAM, les extractions de données individuelles du SNIIRAM ainsi que la mise à disposition d'extractions de données agrégées du SNIIRAM aux partenaires* ». Depuis lors, aucune nouvelle information sur ce dossier pourtant très sensible n'a été diffusée par la CNIL ou par la CNAMTS : sans tirer de conclusion hâtive, nous pouvons penser que le personnel de l'organisme gestionnaire du SNIIRAM a procédé en priorité aux mesures demandées par la Commission avant de se lancer dans la refonte du FOIN.

154. Il découle de tous ces éléments que les responsables de la mise en œuvre de l'accès permanent sont constamment amenés à penser de nouveaux moyens pour rester à la pointe des méthodes permettant d'assurer la sécurité des données de santé. Ceci est d'autant plus vrai que, comme nous allons l'étudier dans le prochain paragraphe, les données mises à disposition n'ont cessé d'être élargies depuis le premier arrêté SNIIRAM de 2002[397].

SECTION 2 : L'ÉLARGISSEMENT PERTINENT MAIS ERRATIQUE DES DONNÉES DE SANTÉ

155. Nous venons d'analyser les différentes restrictions de sécurité auxquelles les données de santé mises à disposition en permanence doivent être soumises. Il est nécessaire de garder cela en toile de fond pour étudier convenablement les données que les bénéficiaires de l'accès

[396] Décision n° MED-2018-006 du 8 février 2018 mettant en demeure la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés.

[397] Arrêté du 11 avril 2002, *op. cit*.

permanent peuvent obtenir. Ainsi, nous allons étudier le contenu des données de santé et les raisons qui justifient de proposer de telles informations en accès permanent (§1), puis nous aborderons le caractère instable de ces évolutions (§2).

Paragraphe 1 : L'ouverture prudente des données de santé en accès permanent

156. La lecture du premier arrêté relatif à la mise en œuvre du SNIIRAM[398] permet de prendre connaissance des acteurs qui ont, les premiers, bénéficié d'un accès permanent aux données de santé[399], mais aussi de savoir à quelles données l'accès a été ouvert. Ce premier texte dresse ainsi la liste des informations accessibles en décrivant leur contenu et en les distinguant selon plusieurs modalités de mise à disposition. En effet, chaque accès permanent dispose de son propre champ de données accessibles, et ce, en fonction des missions de service public exercées. Signalons que l'étendue des données disponibles dans le système d'informations est détaillée avec précision dans le rapport de P.-L. BRAS[400]. Elle est aussi évoquée dans le rapport de la Commission open data en santé[401].

157. Parmi les données initialement accessibles en permanence, d'après l'article 3 du premier arrêté relatif à la mise en œuvre du SNIIRAM, se trouvent des données sur les bénéficiaires de prestations de santé, sur les prestataires de santé, sur les décomptes des demandes de prise en charge et les réponses qui leurs sont apportées, mais aussi sur les sorties hospitalières[402]. Toutes

---

398 *Ibid.*

399 *Supra* n° 104.

400 BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, p. 14-18, *op. cit.*

401 Rapport de la Commission open data en santé, p. 29, *op. cit.*

402 V. article 3 de l'arrêté du 11 avril 2002, *op. cit.* :

« *Les informations nécessaires à l'établissement du système national d'information inter-régimes de l'assurance maladie* […] *concernent :*
- l'identification des organismes de prise en charge ;
- les caractéristiques des décomptes de remboursement ;
- les numéros d'anonymat de l'assuré et du bénéficiaire, le sexe, l'année et le mois de naissance, le département et la commune de résidence ;
- les informations relatives aux prestations servies :
- nature détaillée des actes, biens et services présentés au remboursement ;
- dates de soins et de remboursement ;
- mode de prise en charge ;
- informations médico-administratives (notamment le numéro d'affection de longue durée […]*) ;*
- montant, cotation et coefficient de la prestation ;
- le numéro d'identification du professionnel et, le cas échéant, de l'établissement de rattachement, le sexe, la date de naissance, la spécialité médicale, la nature d'exercice, le statut conventionnel, la caisse de rattachement, département et commune d'établissement ;
- les informations relatives à l'activité des établissements de santé : résumés de sorties anonymes […] *;*

ces informations avaient alors pour objectif d'être utilisées par les acteurs titulaires d'un accès permanent afin de faciliter et d'améliorer leur mission de service public[403]. Cependant, dès sa mise en place, l'accès permanent opérait une sélection dans les données accessibles : l'accès permanent à l'intégralité des données citées par l'article 3 de l'arrêté du 11 avril 2002 ne bénéficiait qu'à quelques rares acteurs identifiés comme légitimes en raison de leur mission[404]. A l'inverse, les autres acteurs cités par le texte[405] ne pouvaient accéder qu'à des données agrégées, jugées suffisantes pour l'accomplissement de leur mission de service public. Précisons que pour chacun des acteurs, l'arrêté dresse une liste exhaustive des données accessibles de manière permanente, en les identifiant à la fois dans leur contenu et leur forme.

158. La notion d'accès permanent ne signifie donc pas que tous les acteurs ont un droit de consulter et traiter l'intégralité des données de santé. Bien au contraire, chaque évolution, aussi légère soit-elle, a tenu compte de la sensibilité des informations et de la mission de chaque acteur pour définir des modalités d'accès adaptées. Ainsi, afin de faciliter la mise à disposition de données agrégées - qui est finalement le format de données que la majorité des bénéficiaires de l'accès permanent avaient le droit d'exploiter à partir de 2002 - l'échantillon généraliste des bénéficiaires (EGB)[406] a été créé et mis à disposition par l'arrêté de 2005[407]. Ce tout nouvel ensemble de données de santé fut constitué pour « *assurer le suivi de la consommation de soins et des taux de recours aux soins* » d'après l'arrêté. La création de l'EGB a permis d'ajouter de précieuses informations aux données agrégées et individuelles déjà présentes dans le SNIIRAM. Pour les études et les missions des organismes bénéficiaires de l'accès permanent, l'EGB a l'avantage d'être exhaustif sur la consommation de soins, qu'il s'agisse de soins de ville ou d'hospitalisation. Qui plus est, l'EGB est « *vivant* »[408] car il prend en compte toutes les entrées dans le système de l'Assurance maladie (naissances, affiliations nouvelles), et les sorties (décès, changement de régime). L'arrêté du 20 juin 2005 prévoyait même la possibilité de créer

- *les données comptables.* »

[403] *Supra* n° 122 à 124.

[404] Il s'agit des personnels des caisses d'assurance maladie, v. *supra* n° 104 et 143.

[405] Il s'agit des personnels des ministères chargés de l'emploi, de la solidarité, de l'agriculture, de l'économie, des agents des agences régionales de l'hospitalisation (devenus agences régionales de santé), de tous les prestataires de soins (établissements de soins, professionnels de santé), et enfin des unions régionales de médecins libéraux (devenues unions régionales des professionnels de santé). v. *supra* n° 104 et 143.

[406] Pour la présentation de l'EGB, v. *supra* n° 148.

[407] Arrêté du 20 juin 2005, *op. cit.*

[408] POLTON D., RICORDEAU P., « Le SNIIRAM et les bases de données de l'Assurance Maladie en 2011 », *op. cit.*, p. 31.

d'autres échantillons que l'EGB[409] dans le respect du chapitre X de la loi du 6 janvier 1978 relative à l'informatique et aux libertés[410].

159. Tous les arrêtés relatifs à la mise en œuvre du SNIIRAM n'ont pas eu le même impact sur l'étendue des informations contenues dans la base ou sur les types d'accès permanents appliqués. Ainsi, l'arrêté du 16 octobre 2008[411] a simplement apporté un ajout minime, non dénué d'intérêt, aux données individuelles : la date de décès, si elle existe, est en effet insérée à la suite du numéro d'anonymat de l'assuré et du bénéficiaire, du sexe, de l'année et du mois de naissance. L'arrêté suivant du 1er décembre 2011[412] a également ajouté à la base de données toutes les informations relatives au parcours de soins des bénéficiaires. Ces éléments nouveaux rapportés au fil des années d'utilisation du SNIIRAM ont, chacun, eu pour objectif d'apporter une plus-value à l'action de service public des acteurs bénéficiant d'un accès permanent. Notons toutefois que ces modifications sont très légères et surtout relativement espacées dans le temps : cela témoigne de la prudence qui est affichée par les autorités dès lors qu'il s'agit de l'accès aux données de santé afin de garder suffisamment d'espace pour la protection de la vie privée. Cette prudence, qui peut aussi être perçue comme de la frilosité voire comme une absence de maîtrise, ne signifie pas que chaque évolution des données proposées en accès permanent s'est nécessairement bien passée. Comme nous le décrypterons ultérieurement[413], la succession d'arrêtés modifiant le contenu et la forme des données de santé accessibles en permanence a donné lieu à quelques incohérences.

160. La révision complète du système de base de données en santé est intervenue très récemment avec la loi de modernisation de notre système de santé[414] qui a donné lieu à la publication de plusieurs décrets dont celui du 26 décembre 2016[415]. Ce décret a créé le Système

[409] *Infra* n° 165.

[410] Le chapitre X de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *op. cit*., a été abrogé par la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *op. cit*.. Ce chapitre visait à encadrer 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.

[411] Arrêté du 16 octobre 2008, *op. cit*.

[412] Arrêté du 1er décembre 2011, *op. cit.*

[413] *Infra* n° 163 à 164.

[414] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[415] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*.

national des données de santé (SNDS) qui devait entrer en fonctionnement le 1er avril 2017[416]. Ce nouveau système remplace désormais l'intégralité de l'environnement informatisé qui s'était développé autour du SNIIRAM. Aujourd'hui, ce guichet unique propose les informations relatives aux bénéficiaires de soins et de prestations médico-sociales, incluant les données relatives aux décès du CépiDc[417]. Sont aussi proposées les données relatives aux organismes d'assurance maladie obligatoire et aux organismes d'assurance maladie complémentaire qui interviennent dans la prise en charge financière du bénéficiaire. Le SNDS est également destiné à regrouper toutes les informations sur la prise en charge sanitaire, médico-sociale et financière de chaque bénéficiaire ainsi que les informations relatives aux professionnels et services de santé qui interviennent dans la prise en charge de ces bénéficiaires. De même, des données médico-sociales relatives aux personnes en situation de handicap sont intégrées dans le nouveau système. Enfin, le SNDS propose les informations concernant les arrêts de travail et les indemnités journalières ou capitaux versés au titre de prestations en espèce.

161. Le décret créant le SNDS ne propose pas uniquement une liste de données que le système contient et auxquelles peuvent accéder directement les bénéficiaires de l'accès permanent. Il s'accompagne d'une mise à jour des finalités du dispositif qui propose six axes[418] parmi lesquels nous noterons « *la surveillance,* […] *la veille et* […] *la sécurité sanitaires* » ainsi que « *la connaissance des dépenses de santé, des dépenses de l'assurance maladie et des dépenses médico-sociales* ». S'il est important de relever cette nouvelle description des finalités du SNDS, c'est parce que le contenu et la forme des données de santé mises à disposition dans le

[416] Comme nous l'avons étudié plus tôt, la mise en fonctionnement du SNDS a été reportée du 1er avril 2017 au mois de septembre 2017. V. *supra* n° 118.

[417] Le CépiDc est le Centre d'épidémiologie sur les causes médicales de décès qui fait partie intégrante de l'Institut national de la santé et de la recherche médicale (INSERM). Il gère la Base de Causes Médicales de Décès.

[418] L'article 1 du décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé », précise que le SNDS « *a pour finalité* […] *de mettre à disposition des données qu'il rassemble* […] *afin de contribuer :*
1° A l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité, l'orientation des usagers dans le système de santé, en permettant la comparaison des pratiques de soins […] *;*
2° A la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale, en favorisant l'identification des parcours de soins des patients […] *;*
3° A la connaissance des dépenses de santé, des dépenses de l'assurance maladie et des dépenses médico-sociales, en permettant d'analyser les dépenses des régimes d'assurance maladie […] *;*
4° A l'information des professionnels de santé, des structures et des établissements de santé ou médico-sociaux sur leur activité, en permettant la transmission aux prestataires de soins des informations pertinentes relatives à leur activité […] *;*
5° A la surveillance, à la veille et à la sécurité sanitaires, en développant l'observation de l'état de santé des populations […] *;*
6° A la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale. »

cadre du nouveau dispositif ont pour objectif de permettre d'atteindre ces finalités. Rappelons qu'initialement, les objectifs affichés du SNIIRAM était bien plus restreints et se décomposaient en trois parties[419] au lieu de six aujourd'hui.

Cela ne signifie pas pour autant que le dispositif de base de données en santé créé en 2002 manquait d'ambition. En effet, il semble évident que la définition des finalités du système est prise à la lumière des opportunités techniques de traitement des données avant leur mise à disposition. C'est-à-dire que si le SNDS peut maintenant proposer des objectifs qui semblent plus ambitieux que ne l'étaient ceux du SNIIRAM initial, c'est en grande partie grâce à l'évolution des systèmes informatiques et aux techniques de protection des informations de plus en plus poussées. Les différentes bases de données en santé sont en effet mieux maîtrisées aujourd'hui, des interconnexions durables ont été mises en place entre elles, ce qui n'était pas du tout le cas en 2002. Le fait que les finalités soient désormais très détaillées semble aussi être une façon indirecte de favoriser la mise à disposition continue de toutes les données qui permettront d'accomplir les objectifs fixés.

162. Pour conclure, nous pouvons supposer que les données de santé contenues dans le SNDS ne manqueront pas d'évoluer dans les années à venir compte tenu des innovations techniques permanentes et de l'omniprésence croissante de la récolte des données dans notre environnement quotidien[420]. Les précautions prises par le législateur pour adapter peu à peu la nature ; le contenu des données de santé accessibles et leurs modalités d'utilisation, témoignent de l'importance que reflète le principe du droit au respect de la vie privée en France. Si des changements continuent d'être apportés au contenu des données de santé, il serait toutefois souhaitable qu'ils soient mieux préparés et coordonnés que cela a pu l'être : c'est précisément l'objet des développements suivants.

Paragraphe 2 : L'élargissement instable des données en accès permanent

163. Nous avons déjà observé le caractère balbutiant des évolutions concernant les acteurs qui ont obtenu un accès permanent aux données de santé depuis le premier arrêté SNIIRAM de

[419] *Supra* n° 95.

[420] Le projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019 devrait aboutir à l'intégration de nouvelles données dans le SNDS.

2002[421]. Bien que la mise à disposition de nouvelles données de santé semble mieux maîtrisée[422], nous pouvons relever plusieurs imprécisions qui ont eu un impact important sur la mise en œuvre de l'accès aux nouvelles données de santé. Ainsi, il est arrivé que des données qui étaient supposées être mises en accès permanent selon un arrêté, ne puissent, pour des raisons techniques, être vraiment accessibles que plusieurs années après.

C'est notamment ce qui s'est produit lors de la publication du premier arrêté relatif à la mise en œuvre du SNIIRAM[423]. En effet, ledit arrêté prévoyait que les résumés de sortie hospitaliers devaient être intégrés à la base de données afin d'être accessibles. Pourtant, ces résumés de sortie hospitaliers n'ont été disponibles qu'à partir de 2007, soit un décalage de cinq ans entre la création de l'accès à ce type de données de santé et l'effectivité de cet accès. Si un tel retard est à déplorer, sa raison est simple : l'agence chargée de transmettre les informations n'a commencé cette mission qu'au cours de l'année 2007[424].

D'une façon similaire, les relevés de soins externes hospitaliers ne sont proposés en accès dans la base de données que depuis 2009 : c'est grâce à une évolution technique, le chaînage des données hospitalières du PMSI avec celles du SNIIRAM, que cela a été rendu possible[425]. Le décalage temporel entre l'annonce faite par arrêté est ici de sept ans.

Plusieurs années semblent avoir été nécessaires pour que l'ambition initiale portant sur le contenu de la base et l'accès permanent au bénéfice des acteurs ayant une mission de service public soient pleinement conformes au texte. Tout cela pose toutefois la question de l'impact sur l'information diffusée aux bénéficiaires d'un accès permanent. Ceux-ci pensaient pouvoir obtenir les données de santé prévues par les textes alors que certaines de ces données n'ont été mises à disposition que bien après la publication de l'arrêté les prévoyant. Il est facile d'imaginer la déception des titulaires d'un accès permanent qui pensaient pouvoir obtenir des

[421] *Supra* n° 104 à 113.

[422] *Supra* n° 122 à 125.

[423] Arrêté du 11 avril 2002, *op. cit*.

[424] Comme le précise le rapport de BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 14, l'Agence Technique d'Information sur l'Hospitalisation (ATIH) n'a commencé à transmettre les résumés qu'au cours de l'année 2007.

[425] Depuis 2009, les données hospitalières contenues dans le Programme Médicalisé des Systèmes d'Information (PMSI), géré par l'Agence Technique d'Information sur l'Hospitalisation (ATIH) sont chaînées de manière effective avec celles du SNIIRAM. C'est-à-dire que les données de santé provenant des deux systèmes mais concernant la même personne sont liées entre elles.

données citées dans l'arrêté de 2002 mais qui, dans la pratique, n'étaient pas encore intégrées au SNIIRAM.

Une question légitime se pose alors : pourquoi indiquer par arrêté que des données sont présentes dans la base SNIIRAM alors même que, ne serait-ce que techniquement, ce n'est pas encore possible ? Il aurait été préférable d'attendre que les obstacles techniques et juridiques soient levés avant d'annoncer l'intégration effective de nouvelles données de santé pouvant faire l'objet d'un accès. Pourtant, les auteurs de l'arrêté ont préféré annoncer, dès le lancement du système d'accès aux données de santé, la liste des informations destinées à être traitées en sachant bien qu'une partie d'entre elles n'était pas disponible. En réalité, cette méthode a pu avoir un effet positif de levier pour encourager et accélérer la mise à disposition des données prévues par arrêté qui n'étaient pas encore accessibles en pratique. Il est possible que, sans cette manœuvre, l'intégration des résumés de sortie hospitaliers et des relevés de soins externes hospitaliers n'en aurait été que plus retardée.

164. D'une façon toute aussi impactante sur les opportunités de traitements par les bénéficiaires d'un accès permanent, le contenu de l'EGB[426] créé en 2005 a longtemps été incomplet. Lors de son lancement, ce nouvel ensemble de données de santé a commencé à proposer des informations récupérées de l'historique depuis 2003. Une légère profondeur historique pouvait donc être mise à profit pour réaliser des études et favoriser la production d'analyses globales par les acteurs accédant à l'EGB. Mais ce que l'arrêté de 2005[427] ne précisait pas, c'est que toutes les informations qu'il contenait à cette date ne concernaient que le régime général de la sécurité sociale. Ce n'est que cinq ans plus tard, à partir de décembre 2010 que les données de la Mutualité Sociale Agricole (MSA) ont été prises en compte pour constituer l'EGB. Et c'est à partir du mois de mai 2011 que les informations provenant du Régime Social des Indépendants (RSI) ont pu être récupérées. Ce sont avant tout des obstacles techniques qui sont à l'origine des délais d'intégration de ces nouvelles données de santé. De 2005 à 2011, l'EGB ne pouvait donc pas être exploité au maximum de son potentiel : les agents habilités du ministère chargé de l'agriculture n'avaient, par exemple, pas de réelle utilité à le récupérer car les informations relatives aux affiliés à la MSA n'y étaient pas encore intégrées.

[426] *Supra* n° 148.

[427] Arrêté du 20 juin 2005, *op. cit.*

165. La création de l'EGB en 2005 s'est aussi accompagnée de l'opportunité, prévue par le dernier alinéa de l'article 3 de l'arrêté[428], d'élaborer de nouveaux échantillons selon une procédure prévue par la loi du 6 janvier 1978[429]. Cependant, ces nouveaux échantillons ne peuvent être constitués qu'après leur approbation par le conseil d'administration de l'Institut des données de santé (IDS), aujourd'hui remplacé par l'Institut national des données de santé (INDS). Or, l'IDS, bien qu'instauré par la loi du 13 août 2004[430], antérieure à l'arrêté de 2005, n'a vu son existence approuvée qu'en 2007[431]. Ainsi, pendant deux ans, la possibilité prévue par les textes de produire de nouveaux échantillons de données ne pouvait pas être mise en œuvre car l'un des chaînons de la procédure d'autorisation était encore inexistant.

Tout au long du parcours de l'élargissement des données de santé accessibles se trouvent des éléments indiquant qu'un décalage flagrant se dresse entre, d'une part, la volonté du législateur de proposer rapidement des bases de données riches, accessibles et opérationnelles ; et d'autre part, la réalité juridique, informatique et technique qui imposent leur propre calendrier. C'est pour cette raison que les données accessibles de façon permanente n'ont pu être ouverte que sporadiquement. Chaque organisme producteur de données a dû adapter son système pour sécuriser les données et les transmettre dans les normes en vigueur. Chaque nouvel acteur, comme l'IDS, a dû attendre que toutes les étapes de sa création soient respectées pour exercer sa mission en toute sérénité, en conformité avec la loi relative à l'informatique et aux libertés.

Aujourd'hui, la mise en œuvre du nouveau SNDS permet de penser que les difficultés qui ont pu être rencontrées depuis 2002 ont conduit les auteurs de la réforme à anticiper, autant que possible, les obstacles potentiels. La préexistence des différents systèmes informatiques et la disponibilité des services de l'Etat (notamment des agents de la DREES) pour épauler les acteurs qui ont un accès permanent indique une volonté de favoriser pleinement l'utilisation des données de santé dans le respect de toutes les normes, notamment de sécurité, en vigueur. La

---

[428] Voici ce que prévoit le dernier alinéa de l'article 3 de l'arrêté du 20 juin 2005, *op. cit.* :

« *D'autres échantillons de ces données peuvent être réalisés, conformément aux dispositions du chapitre X de la loi du 6 janvier 1978 susvisée. Ils sont soumis à l'approbation préalable du conseil d'administration de l'Institut des données de santé excepté lorsqu'ils sont réalisés pour le compte d'organismes d'assurance maladie obligatoires ou lorsqu'ils ont déjà fait l'objet d'un avis du Conseil national de l'information statistique.* »

[429] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[430] Loi n° 2004-810 du 13 août 2004 *relative à l'assurance maladie*, JORF, n° 0190, 17/08/2004.

[431] Arrêté du 30 avril 2007 portant approbation du groupement d'intérêt public « Institut des données de santé », JORF n° 109 du 11/05/2007.

réalité de la pratique, que nous observerons dans les années à venir, confirmera ou infirmera cette considération.

CONCLUSION DU CHAPITRE II

166. La création d'un accès permanent aux données de santé des bases médico-administratives n'est pas synonyme d'accès total à l'intégralité des données. Pour assurer la protection de la vie privée des individus, un ensemble de procédures de sécurité a été créé et imposé aux bénéficiaires de l'accès permanent. Toutes les données du SNIIRAM sont, par défaut, traitées pour être pseudonymisées. Elles ne contiennent aucune information directement identifiante et sont individualisées par un numéro d'anonymat généré par le programme de chiffrement FOIN. Dans le même temps, les données ne sont rendues accessibles que pour un temps donné : nous parlons alors de profondeur historique des données de santé.

167. Les acteurs bénéficiaires de l'accès permanent sont aussi limités, depuis la création du dispositif, par un nombre fixe de croisements de données possibles. Cette limite dans les traitements a été définie pour parer aux risques de réidentification. Au-delà de cette frontière technique, chacun des acteurs n'est autorisé à obtenir et traiter que des données qui sont spécifiquement prévues par arrêté ministériel. Ces bases de sécurité qui régissent l'accès permanent aux données de santé ne sont pas gravées dans le marbre et continuent d'évoluer encore aujourd'hui : la profondeur historique des données, le champ et le type de données accessibles, tout comme les modalités de chiffrement des données ont changé ou sont amenées à changer.

168. La quantité et la qualité des données de santé accessibles dans le cadre de l'accès permanent est aussi un enjeu durable. Au début des années 2000, une grande quantité de données concernées était seulement composée de données agrégées, difficiles à exploiter pour améliorer les missions de service public des acteurs jouissant de l'accès permanent. La diversification et l'enrichissement des données mises à disposition s'est prudemment opérée, non sans errements – nous faisons notamment référence aux arrêtés indiquant la mise à disposition de données qui, dans la pratique, ne l'ont été que plusieurs années plus tard – , jusqu'à la réforme du 26 janvier 2016[432] qui a conduit à une refonte complète du dispositif.

[432] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

CONCLUSION DU TITRE I

169. L'accès permanent aux données de santé dans un objectif de bon fonctionnement de service public s'est construit progressivement avec, en ligne de mire, la nécessité de protéger la vie privée des individus. L'usage du terme « *accès permanent* » ne signifie donc pas que toutes les données de santé à caractère personnel contenues dans les bases médico-administratives sont ouvertes à tous les agents et salariés des acteurs qui exercent une mission de service public. Au contraire, cet accès a été pensé en amont pour répondre aux critères de sécurité et de traçabilité relatifs aux données rendues accessibles. C'est ainsi que seuls les acteurs autorisés par arrêté ou par la loi bénéficient d'un accès permanent et que seul le personnel identifié et habilité au sein de chacun de ces acteurs peut mettre en œuvre ledit accès. Chaque bénéficiaire se voit également attribuer certaines catégories de données de santé auxquelles il peut accéder en fonction de ses missions : s'il souhaite obtenir et traiter des données qui ne figurent pas dans son champ d'action, il doit passer par une procédure d'autorisation préalable[433]. L'intégralité de ce dispositif a pour fonction principale de maîtriser le parcours des données de santé avec, pour pilier central, la protection de la vie privée. A ce titre, la CNIL est un acteur essentiel qui fait partie intégrante du processus de validation du cadre juridique afin de garantir aux individus le respect de leurs droits.

170. L'accès permanent a fortement évolué depuis sa mise en place par le premier arrêté du 11 avril 2002[434]. D'abord ouvert à une liste ciblée (et néanmoins vague par endroits) d'acteurs, incluant notamment les agents des agents des ministères du travail, de l'agriculture et des finances, ou encore les prestataires de soins, cet accès permanent s'est lentement développé pour véritablement atteindre ses objectifs d'amélioration des services publics de la santé. En effet, c'est au fil des arrêtés successifs que de nouveaux bénéficiaires ont été désignés avec l'ajout des agents travaillant à la HAS, à l'ANSM, à l'INSERM, à l'ATIH, ou encore à la DREES. Cette dernière n'a d'ailleurs obtenu son accès permanent qu'en 2016[435]. L'évolution de l'accès permanent a également été caractérisée par l'extension des données de santé rendues accessibles : ainsi des informations clefs comme la date de décès éventuelle de l'individu ou

[433] Procédure que nous qualifions d'accès sélectif et que nous étudions en Partie II de cette étude.

[434] Arrêté du 11 avril 2002, *op. cit*.

[435] Arrêté du 6 octobre 2016, *op. cit.*

les informations relatives à son parcours de soins ont été intégrées dans les données en accès permanent alors qu'elles n'en faisaient pas partie initialement. Nous l'avons observé tout au long de ce titre, la construction de l'accès permanent a débuté au début des années 2000 et continue aujourd'hui à se renouveler. La réforme du 26 janvier 2016[436] marque ainsi le renouveau de l'accès permanent avec la refonte de la liste des bénéficiaires dans un décret[437] qui détaille clairement les données de santé qui sont rendues accessibles. Cette remise à niveau totale du dispositif est salutaire car elle permet de clarifier l'identité des bénéficiaires et leur marge de manœuvre dans un seul et unique texte.

171. Toutefois, la version actuellement en vigueur de l'accès permanent soulève quelques interrogations et l'existence d'un tel accès pour quelques acteurs seulement peut être remis en question sur de nombreux points : l'étude et la discussion des différents arguments de contestation de l'accès permanent font l'objet du prochain titre.

[436] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[437] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*.

TITRE II

L'ACCÈS PERMANENT AUX DONNÉES DE SANTÉ LIMITÉ PAR LA PROTECTION DE LA VIE PRIVÉE

172. La mise en œuvre des nombreux accès permanents aux données de santé contenues dans le SNIIRAM est acquise depuis le premier arrêté paru en 2002[438]. Sa création avait pour objectif, comme nous venons de l'étudier[439], d'améliorer le fonctionnement du service public. L'intérêt général est au cœur de la réflexion du pouvoir réglementaire même si la protection de la vie privée des individus demeure centrale. L'accès et l'utilisation de toutes ces informations hautement sensibles sont donc, si l'on en croit les arrêtés successifs et le dernier décret[440] relatif au nouveau système national des données de santé (SNDS), subordonnés à l'accomplissement de missions très générales les premières années consistant à « *contribuer à une meilleure gestion de l'assurance maladie* »[441] ou encore à « *contribuer à une meilleure gestion des politiques de santé* »[442], pour devenir très précises aujourd'hui. En effet, le nouveau décret mettant en œuvre le SNDS[443] détaille, en six points complets[444], les nombreux usages attendus

[438] Arrêté du 11 avril 2002, *op. cit.*

[439] V. Partie I, Titre I.

[440] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*.

[441] Arrêté du 11 avril 2002, *op. cit.*

[442] Arrêté du 1er décembre 2011, *op. cit.*

[443] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*.

[444] *Ibid.*, les six objectifs attendus de l'utilisation du SNDS sont :

« *1°A l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité, l'orientation des usagers dans le système de santé, en permettant la comparaison des pratiques de soins, des équipements et des tarifs des établissements et des professionnels de santé ;*
2°A la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale, en favorisant l'identification des parcours de soins des patients, le suivi et l'évaluation de leur état de santé et de leur consommation de soins et de services d'accompagnement social, l'analyse de la couverture sociale des patients, la surveillance de la consommation de soins en fonction d'indicateurs de santé publique ou de risques sanitaires ;
3°A la connaissance des dépenses de santé, des dépenses de l'assurance maladie et des dépenses médicosociales, en permettant d'analyser les dépenses des régimes d'assurance maladie par circonscription géographique, par nature de dépense, par catégorie de professionnels ou de prescripteurs et par professionnel ou établissement, les dépenses d'assurance maladie au regard des objectifs sectoriels de dépenses fixés, dans le cadre de l'objectif national de dépenses d'assurance maladie, par les lois de financement de la sécurité sociale, l'analyse quantitative des déterminants de l'offre de soins et la mesure de leurs impacts sur l'évolution des dépenses d'assurance maladie ;
4°A l'information des professionnels de santé, des structures et des établissements de santé ou médico-sociaux sur leur activité, en permettant la transmission aux prestataires de soins des informations pertinentes relatives à leur activité, à leurs recettes et, s'il y a lieu, à leurs prescriptions et la mise à la disposition de leurs représentants de données ne faisant pas apparaître l'identité des professionnels de santé ;

des données de santé mises à disposition : nous pouvons y retrouver, entre autres attentes, « *la comparaison des pratiques de soins, des équipements et des tarifs des établissements et des professionnels de santé* » ou encore « *la surveillance de la consommation de soins en fonction d'indicateurs de santé publique ou de risques sanitaires* ».

L'accès permanent a donc été mis en œuvre et réformé récemment afin que les bénéficiaires dudit accès en tirent le meilleur parti afin d'améliorer la réalisation de leurs missions respectives. D'une certaine façon et bien que les textes ne le formulent pas ainsi, cela signifie que des améliorations visibles à tous les degrés d'implication des bénéficiaires de l'accès permanent étaient attendues bien qu'aucun objectif chiffré n'ait été formellement donné.

173. Cette ouverture permanente des données de santé à quelques acteurs sans que des résultats mesurables à atteindre ne soient définis est, en quelque sorte, le point de départ d'une série de contestations de l'existence même de cet accès permanent. Mais ce n'est pas le seul élément de nature à soulever des oppositions. Par exemple la question de la sécurité des données de santé qui fait partie des limites à l'accès permanent peut être évoquée : en effet, en quoi les données seraient-elles moins en sécurité si elles étaient accessibles par un acteur public qui ne dispose pas d'un accès permanent ? Dans le même ordre de questionnement, il est légitime de se demander quelles sont les raisons objectives qui poussent les auteurs des arrêtés à penser que certains acteurs qui disposent d'une mission de service public sont moins légitimes à avoir un accès permanent aux données de santé que d'autres. Plusieurs sujets liés aux accès permanents transparaissent donc déjà, celui de la quantification des résultats obtenus, celui de la justification « sécuritaire » de la restriction de l'accès permanent, mais aussi celui du choix des bénéficiaires de l'accès permanent.

174. Le principe de l'accès permanent aux données de santé semble avoir subi un examen minutieux avant d'être finalement conservé dans le nouveau système issu de la réforme du 26 janvier 2016[445]. Son maintien amène d'ailleurs plusieurs interrogations lorsque l'on sait que la

5°A la surveillance, à la veille et à la sécurité sanitaires, en développant l'observation de l'état de santé des populations, l'évaluation et la production d'indicateurs relatifs à l'état de santé de la population et l'analyse de leur variation dans le temps et dans l'espace, la détection d'événements de santé inhabituels pouvant représenter une menace pour la santé publique et l'évaluation de leurs liens éventuels avec des facteurs d'exposition et l'évaluation d'actions de santé publique ;
6°A la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale. »

[445] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

Cour des comptes elle-même a formulé de nombreuses critiques sur son fonctionnement[446]. La pérennité de ce mécanisme permet de penser que des améliorations ont été apportées afin de prendre en compte les commentaires et observations qui ont été faits depuis sa création. De plus, si les accès permanents aux données de santé, qui sont des exceptions radicales au principe d'interdiction d'accès aux données de santé[447], continuent d'exister, il est nécessaire d'y déceler une détermination concrète de l'Etat à tirer le meilleur parti des opportunités offertes.

175. L'objet de ce chapitre est donc multiple. Il s'agit, dans un premier temps, de décrypter les incompréhensions suscitées par la mise en place des accès permanents depuis le premier arrêté SNIIRAM[448]. Nous commencerons par évoquer la légitimité d'un processus de choix des bénéficiaires de l'accès permanent qui, comme nous l'avons abordé dans le premier titre[449], a été ponctuée de quelques fragilités, étroitement liées à l'argument de la sécurisation des données de santé mises entre les mains des acteurs publics titulaires de cet accès (Chapitre 1). La question hautement importante de l'utilisation effective des données de santé par les dépositaires de l'accès permanent sera abordée dans un second temps, en lien avec l'étude des réponses apportées, ou éludées, par les auteurs du décret créant le nouveau système[450] (Chapitre 2).

[446] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*,

[447] *Supra* n° 60.

[448] Arrêté du 11 avril 2002, *op. cit*.

[449] V. Partie I, Titre I.

[450] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

CHAPITRE I
L'IDENTIFICATION DES LIMITES VACCILLANTES DE L'ACCÈS PERMANENT

176. Il est difficile de parler de contestation au sens premier du terme lorsque l'on évoque les arguments qui iraient à l'encontre de l'accès permanent aux données de santé. Il n'y a pas eu de grande mobilisation citoyenne, pas de tribunes publiées par voie de presse ni de polémiques initiées par certains acteurs publics déçus de ne pas avoir d'accès permanent. Ici, il est plutôt question de mettre dans la balance la justification de la création de cet accès face aux modalités de choix et d'habilitation des bénéficiaires qui revêt une apparence arbitraire (Section 1), et la sécurité des données qui ne semble pas forcément plus assurée que dans les mains d'autres acteurs (Section 2).

SECTION 1 : L'APPARENCE ARBITRAIRE DU CHOIX DES BÉNÉFICIAIRES DE L'ACCÈS PERMANENT

177. Depuis la délivrance des premiers accès permanents aux données de santé du SNIIRAM, les divers arrêtés et décrets se sont succédé[451] sans que le cheminement ayant mené à la décision finale ne soit vraiment connu. Si l'on ne peut pas réellement qualifier cette situation d'opaque, la méthode utilisée est propice au questionnement tant en amont du choix des bénéficiaires que dans la justification ultérieure de ce choix. Aussi, nous nous efforcerons de détailler les arguments qui sont de nature à mettre à l'épreuve les fondements de cet accès (Paragraphe 1). Puis nous questionnerons la maîtrise des conséquences qui découlent de l'accès permanent (Paragraphe 2).

Paragraphe 1 : Le processus méconnu du choix des bénéficiaires

178. Le premier arrêté[452] créant l'accès permanent découle de la loi de financement de la sécurité sociale pour 1999[453] qui est à l'origine de la création du SNIIRAM. Une année et demi s'est donc écoulée entre la loi et le premier arrêté du 11 avril 2002[454]. Dès lors, il est légitime

[451] *Supra* n° 104 à 113.

[452] Arrêté du 11 avril 2002, *op. cit.*

[453] Loi n° 98-1194 du 23 décembre 1998 *op. cit.*

[454] Arrêté du 11 avril 2002, *op. cit*.

de penser que, aussi bien les professionnels que la doctrine attendaient avec impatience la parution du texte comprenant la description formelle du fonctionnement des divers types d'accès permanents aux données de santé. En effet, ce texte constituait l'officialisation de la création de la plus grande base de données de santé en France : il était parfaitement légitime que les questions et réflexions sur le sujet soient nombreuses aussi bien avant la publication de l'arrêté, qu'après. Pourtant, et c'est bien cela qui étonne, il est aujourd'hui très ardu de retrouver de la documentation, de la doctrine, des notes, relatives aux attentes mais aussi à l'analyse de cet arrêté fondateur de l'accès permanent. Tout au plus retrouvons-nous un ouvrage sur l'adéquation de la recherche médicale avec les principes de la loi relative à l'informatique et aux libertés[455] en 2001, et une étude sur la protection des données de santé à caractère personnel[456] en 2003. En revanche, tout écrit ou commentaire précisément lié à la mise en œuvre des premiers accès permanents est tout à fait absent. Si nous prenons la peine de soulever ce point dans une sous-partie consacrée à la légitimité du choix des bénéficiaires des accès permanents c'est que plusieurs remarques peuvent en être tirées.

179. En premier lieu, cela permet de prendre conscience de la difficulté de l'ensemble de la classe politique, intellectuelle ou scientifique, à se saisir pleinement du sujet à une époque où la technologisation du monde est en plein essor. Les bases de données se développaient, le géant Google, aujourd'hui incontournable, commençait à peine à conquérir la planète. Dans ce contexte, où les mots « *bases de données* », « *données massives* » et « *données ouvertes* » étaient encore sibyllins pour la majorité des personnes, la question de l'accès permanent à une nouvelle base de données de santé en France pouvait paraître distante contrairement à ce qui peut être observé actuellement avec l'omniprésence de sujets liés à la protection de la vie privée et des données à caractère personnel.

180. En second lieu, la réflexion qui peut être apportée vise directement l'absence d'analyse postérieurement à la publication de l'arrêté. Il aurait été plutôt logique de retrouver des études du contenu du texte, autant pour la liste qu'il propose, que pour les types de données accessibles,

[455] de LAMBERTERIE I. et LUCAS H.-J., « Informatique, libertés et recherche médicale », *CNRS Editions*, 2001, 283 p.

[456] CHEMTOB-CONCE M.-C., « La protection des données de santé à caractère personnel », *RGDM*, 01/06/2003, n° 10, p. 111-126.

ou pour les objectifs visés par la mise en œuvre du SNIIRAM[457]. Ce travail n'a, semble-t-il, pas été réalisé au début des années 2000. Tout cela est intrigant car, comme nous l'avons observé dans le premier chapitre[458], beaucoup d'observations pouvaient être formulées dès le premier arrêté. Est-ce un signe d'un désintéressement pour le sujet à cet instant précis ? Ce postulat est plutôt difficile à croire, pourtant les faits semblent nous pousser dans cette direction.

181. Le constat d'une doctrine rare entourant le premier arrêté[459] ne fait pas obstacle à nos considérations. Si l'arrêté de 2002 avait été analysé à sa publication, les auteurs auraient probablement souligné que le choix des bénéficiaires de l'accès permanent semblait parfois hasardeux. En effet, des agents du ministère de l'agriculture se voyaient octroyer un accès permanent à des données de santé alors que ceux du ministère de la santé et d'organismes placés sous son autorité, comme l'InVS (devenu Santé Publique France[460]) en étaient interdits d'accès. Cette simple observation suffit à se demander comment les bénéficiaires des accès permanents étaient choisis. On peut penser que, dans leur sagesse, les autorités à l'origine de la création du SNIIRAM et de sa mise en œuvre ont procédé à la réalisation d'études préalables pour détecter les acteurs chargés d'une mission de service public les plus susceptibles d'avoir besoin de recourir aux données mises à disposition. Pourtant, l'absence des agents du ministère de la santé, qui sera heureusement corrigée en 2005[461], tout comme celle d'autres agences sanitaires[462], nous conduit à nourrir de sérieux doutes quant à la méthode employée pour sélectionner ceux qui obtiennent le droit de récupérer de manière permanente des données de santé.

182. Nos doutes se confirment malheureusement lorsque, malgré nos recherches, il se trouve qu'aucun des arrêtés relatifs à la modification de la liste des bénéficiaires de l'accès permanent aux données de santé n'a fait l'objet d'un commentaire ou d'une analyse critique (qu'elle soit bonne ou mauvaise). Le sujet, certes très technique, et pourtant hautement sensible, ne s'est pas montré digne d'intérêt avant que les autorités françaises ne décident de réfléchir sérieusement

[457] Ce travail a été réalisé dans le titre I de la partie I de cette étude, dédié à l'étude des bénéficiaires de l'accès permanent et aux données proposées dans le cadre de cet accès.

[458] *Ibid.*

[459] Arrêté du 11 avril 2002, *op. cit.*

[460] Ordonnance n° 2016-462 du 14 avril 2016, *op. cit.*

[461] Arrêté du 20 juin 2005, *op. cit.*

[462] *Supra* n° 104 à 113.

aux interrogations soulevées par l'insuffisance de l'accès aux données de santé[463]. Tout au plus, pouvons-nous retrouver les arrêtés publiés dans les revues doctrinales[464] sans aucun commentaire annexé. Même l'arrêté pris le 19 juillet 2013[465] qui a entièrement réécrit la liste des bénéficiaires de l'accès permanent ainsi que celles des données faisant l'objet de cet accès n'a fait l'objet d'aucun article dans les revues spécialisées, alors même qu'il a été publié au moment où la réflexion de nouvelles modalités d'accès à la base de données de santé étaient en pleine ébullition.

183. Un autre élément est de nature à attiser notre curiosité : d'après nos recherches, le processus de sélection des acteurs bénéficiant de l'accès permanent ne semble pas être décrit dans un document officiel directement accessible[466]. Ce manque de transparence, qui s'est estompé avec le temps et la démocratisation des données ouvertes, était prégnant au début du XXI^{e} siècle. Cela ne serait pas problématique si l'ouverture des différents accès avait été fluide et bien échelonnée dans le temps. Or, nous l'avons vu[467], chaque arrêté, ou presque, publié pour donner la liste exhaustive des bénéficiaires de l'accès permanent contenait son lot d'approximations ou d'oublis. Rappelons que tous les « prestataires de soins » bénéficiaient dès 2002 d'un accès permanent à certaines données de santé alors qu'aucune définition précise de cette notion n'était donnée : seuls deux exemples figuraient dans l'arrêté, les professions médicales et les pharmaciens. Sachant cela, le fait que ces professionnels médicaux aient eu un accès permanent avant les agents du ministère de la santé, qui ne l'ont obtenu qu'en 2005, demeure un mystère que nous ne pouvons résoudre.

La principale question qui émerge de ce constat est la suivante : comment les bénéficiaires de l'accès permanent aux données de santé étaient-ils sélectionnés ? Si c'était pour leur mission

---

[463] V. GOLDBERG M., *Rapport du Haut Conseil de la Santé publique de mars 2012, op. cit. ;* BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit. ;* GORCE G. et PILLET F., Rapport d'information au Sénat, *La protection des données personnelles dans l'open data : une exigence et une opportunité, op. cit. ;* BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé, op. cit.*

[464] Assurance maladie, « Mise en œuvre du système national d'information interrégimes – Texte non codifié », *JCP S*, n° 13, 20/09/2005.

[465] Arrêté du 19 juillet 2013, *op. cit.*

[466] Le rapport de la Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, précise, p. 54, que le premier protocole de 2001 relatif au SNIIRAM aurait donné au COPIIR (Comité d'Orientation et de Pilotage d'Information Inter-Régimes) le soin de définir les conditions d'accès aux données du SNIIRAM. Cette mission lui aurait été retirée en 2008, pourtant, le COPIIR aurait continué d'avoir ce type de questions prévues à son ordre du jour.

[467] *Supra* n° 104 à 113.

de service public, comment se fait-il que les agents du ministère de la santé en 2002 ne se sont pas vu accorder d'accès permanent ? On peut reconnaître que le ministère du travail d'alors avait pour dénomination « Ministère des Affaires sociales, du Travail et de la Solidarité ». Contrairement à ce que certains voudraient penser, ceci n'est pas qu'affaire de sémantique c'est bien pour cette raison que l'arrêté de 2005[468] a précisé dans le texte que les « *agents du ministère chargé de l'assurance maladie, de la santé, de l'action sociale des personnes handicapées et de la dépendance* » devaient impérativement avoir leur accès permanent.

L'autre critère qui aurait pu être retenu par les acteurs[469] à l'origine des différents protocoles transformés en arrêtés est celui de la capacité à protéger les données rendues accessibles. En effet, c'est la protection de la vie privée des individus qui devrait prévaloir à toute délivrance d'accès permanent : il ne faut pas oublier que l'accès aux données de santé à caractère personnel est interdit par principe[470] et que toute exception doit être justifiée par la garantie que la protection de la vie privée des individus est respectée. Cette hypothèse paraît acceptable à première vue, toutefois, nous le décrypterons ultérieurement[471], l'argument de la sécurité des données de santé reste débattu.

184. Il ressort de ces développements que les modalités de choix des bénéficiaires de l'accès permanent aux données de santé depuis la création du SNIIRAM demeurent un mystère. Le nouveau SNDS aurait pu apporter un éclaircissement bienvenu à cette opacité pourtant préjudiciable. Cela n'est, à l'heure actuelle, pas tout à fait le cas[472]. Le sentiment d'iniquité ressenti par les acteurs qui ne pouvaient pas accéder facilement aux données de santé avant la réforme de 2016 était donc palpable, ce qui est d'autant plus flagrant avec l'analyse de l'effectivité relativement tardive de l'accès permanent, prochaine étape de notre étude.

[468] Arrêté du 20 juin 2005, *op. cit.*

[469] Le contenu des arrêtés est défini par un Comité d'Orientation et de Pilotage d'Information Inter-Régimes (COPIIR) composé des 3 principaux régimes d'assurance maladie obligatoire, de l'Etat, des représentants des professionnels de santé. V. Institut des données de santé, « Processus d'élaboration de l'arrêté permettant l'utilisation des données anonymisées de l'assurance maladie obligatoire ».

[470] *Supra* n° 60.

[471] *Infra* n° 191 à 199.

[472] *Infra* n° 219 à 228.

Paragraphe 2 : Le manque de maîtrise de l'accès permanent

185. L'existence de l'accès permanent aux données de santé a parfois donné l'impression d'échapper à tout contrôle raisonnable. La délivrance de ce type d'accès a pour objectif initial d'améliorer les missions de service public[473] des bénéficiaires en leur donnant les moyens d'analyser toutes les informations mises à leur disposition dans un cadre sécurisé. Dès lors, il serait tout à fait normal d'attendre de cet accès qu'il soit délivré de manière maîtrisée, immédiatement effectif et que son impact soit directement favorable à l'amélioration des missions incombant aux bénéficiaires. Pourtant certaines situations sont de nature à montrer que la possibilité offerte d'obtenir et décrypter ces mines d'informations n'a pas nécessairement eu les effets concrets escomptés.

186. Certains événements remettent directement en cause le raisonnement conduisant à penser que l'accès permanent aux données de santé implique que toutes les actions des acteurs qui peuvent l'utiliser s'en trouvent directement améliorées. Le plus emblématique d'entre eux est le scandale sanitaire du Mediator[474] qui, malgré la disponibilité des données de santé, n'a pas été révélé par les autorités sanitaires françaises mais par I. FRACHON, une pneumologue exerçant au CHU de Brest. Or, au moment même où cette affaire occupait le devant de la scène, nombreux furent celles et ceux qui se sont demandé si tout cela n'aurait pas pu être détecté plus tôt et évité en partie grâce à l'utilisation des données de santé contenues dans le SNIIRAM. Ainsi, le collectif Initiative Transparence Santé a obtenu[475] que les informations relatives à la consommation de ce médicament entre l'année de création du SNIIRAM par la loi de 1998[476] et l'année de suspension de l'autorisation de mise sur le marché (AMM) du médicament en 2009, lui soient communiquées[477].

---

[473] V. Partie 1, Titre 1, Chapitre 1.

[474] V. notamment ARBBOUSSET H., « Mediator et indemnisation des victimes : retour sur une affaire d'Etat », *JCP A*, 12/12/2011, n° 50 ; ROTOULLIE J. C., « Responsabilité de la puissance publique – Mediator : responsabilité de l'Etat à partir de 1999 et faute des laboratoires Servier – Veille », *JCP G*, 21/11/2016, n° 47 ; Conseil d'Etat, « Affaire du médiator : portée de la responsabilité de l'Etat », *Recueil Dalloz*, 24/11/2016, n° 40.

[475] LAUDE A., « Démocratie sanitaire, open data et Médiator », *Journal du droit de la santé et de l'Assurance maladie (JDSAM)*, Chronique 2, Droits des malades et bioéthique, n° 1 de 2014, p. 58 à 61.

[476] Loi n° 98-1194 du 23 décembre 1998 *de financement de la sécurité sociale pour 1999, op. cit.*

[477] Les données de santé finalement extraites et traitées ont été mises en ligne sur le site gouvernemental data.gouv.fr à l'adresse suivante : https://www.data.gouv.fr/fr/datasets/donnees-de-consommation-du-medicament-mediator/

Cette initiative cristallise à elle seule toute la défiance qui a, peu à peu, émergé face aux capacités des autorités sanitaires à se saisir des opportunités offertes par l'accès permanent pour améliorer, notamment, la veille sanitaire. En effet, bien qu'une étude menée en 2009 par la CNAMTS elle-même confirme le lien entre la consommation du médicament et le développement de valvulopathies et d'hypertension artérielle pulmonaire[478], le collectif a voulu savoir si l'accès permanent, utilisé avec toutes les diligences, aurait permis de détecter plus tôt les anomalies dues à la prescription du médicament en dehors de son AMM. Cela signifie que les agences chargées de la veille sanitaire n'auraient pas cru bon d'utiliser pleinement leur possibilité d'analyser les informations qu'elles seules sont habilitées à consulter. Par extension, c'est l'intégrité de tous les bénéficiaires de l'accès permanent qui est en jeu : malgré la promesse d'une utilisation bénéfique des données de santé pour le bien commun, cette situation conduit les citoyens à se questionner sur la légitimité et l'utilité de l'accès permanent s'il ne permet pas d'éviter ce type d'incident. En effet, pourquoi créer un accès permanent si ceux qui devraient en avoir besoin n'estiment pas utile de s'en servir ? Ceci est bien l'une des composantes du problème qui accentue l'impression de choix arbitraire et s'ajoute au processus méconnu de sélection des bénéficiaires[479] évoqué précédemment.

187. L'apparent manque de contrôle de la délivrance et de l'effectivité de l'accès permanent ressort également de l'écart qui existe entre la création dudit accès, et son officialisation, puis sa mise en œuvre. Le cas le plus parlant est celui, déjà évoqué[480], des ARS. Celles-ci ont obtenu leur accès par la promulgation d'une loi le 21 juillet 2009[481], mais l'arrêté officialisant sa création n'est paru que plus de deux années plus tard, le 22 janvier 2012. Cette situation semble opposer deux réalités qui ne sont pas nécessairement inconciliables. D'un côté il y a la volonté du législateur de renforcer rapidement l'action des ARS en accroissant leur capacité de connaissance et d'analyse : cette réalité pratique est tout à fait logique et paraît même être de bon sens. De l'autre se tient la réalité pragmatique et juridique qui impose, volontairement ou non, son lent tempo à l'entrée en application de cet accès permanent.

[478] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 67.

[479] *Supra* n° 178 à 184.

[480] *Supra* n° 106.

[481] Loi n° 2009-879 du 21 juillet 2009, *op. cit.*

Cette dualité a tendance à affaiblir et essouffler la portée de l'accès permanent aux données de santé. Il est légitime de se demander pourquoi cet accès est présenté comme essentiel pour renforcer l'action de ses bénéficiaires alors même qu'aucune mesure n'est prise pour vérifier qu'il soit rapidement décidé et mis en œuvre. A quoi bon donner accès aux données de santé à un organisme si c'est pour que celui-ci ne puisse l'appliquer que deux années plus tard ? Cette question fait partie des nombreuses autres qui pourraient être posées sur le sujet. Tous les commentaires se rejoignent finalement en une considération globale : le fonctionnement de la délivrance et de la mise en œuvre de l'accès permanent depuis 2002 et la parution du premier arrêté[482], jusqu'à la réforme de 2016[483], donne une apparence non coordonnée à l'ensemble. D'autres exemples similaires peuvent d'ailleurs être donnés. Ainsi, nous pouvons évoquer le cas de l'AFSSAPS (devenue ANSM) qui a dû attendre plus de deux ans après la délivrance des premiers accès permanents[484] pour enfin figurer dans le second arrêté SNIIRAM[485].

188. S'il est un acteur qui a recours aux données de santé de manière importante et ce, depuis plusieurs années, c'est la DREES. L'analyse de sa situation est intéressante car elle est symptomatique de l'instabilité du processus de gestion des acteurs qui bénéficient de l'accès permanent. Il est nécessaire de commencer par apporter une précision : cette direction qui dépend de l'administration centrale des ministères sanitaires et sociaux n'est citée directement parmi les acteurs disposant de l'accès permanent que depuis l'arrêté paru en 2016[486]. Pourtant, la Cour des comptes considère que les agents de la DREES ont accès aux données du SNIIRAM en permanence depuis le second arrêté paru en 2005[487]. Cela amène un commentaire liminaire, il est probable que la Cour assimile la DREES aux « *agents du ministère chargé de l'assurance maladie, de la santé, de l'action sociale des personnes handicapées et de la dépendance ou de ses services déconcentrés* », formule présente dans l'arrêté de 2005. D'ailleurs, c'est potentiellement pour clarifier le propos que la DREES a finalement été précisément désignée,

[482] Arrêté du 11 avril 2002, *op. cit.*

[483] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[484] Rapport de P.-L. Bras, *op. cit.*, p. 34.

[485] *Supra* n° 106.

[486] Arrêté du 6 octobre 2016, *op. cit.*

[487] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 76.

signe de l'aveu des membres du Comité d'Orientation et de Pilotage d'Information Inter-Régimes (COPIIR[488]) qui admettent l'incertitude provoquée par les formules trop vagues.

Bien que les agents de cette direction hautement importante aient un accès aux données depuis 2005, la Cour des comptes indique, sans toutefois s'en émouvoir, que ce n'est que depuis 2010 que la DREES exploite les informations disponibles. Cette information est pourtant remarquable car elle vient s'ajouter aux cas de l'ANSM et des ARS qui, elles, ont dû se montrer patientes avant que leur accès permanent annoncé ne devienne effectif. Du côté de la DREES, cinq années se sont écoulées[489] sans faire usage d'informations présentées comme essentielles à l'amélioration des missions de service public dans le domaine sanitaire.

189. Cette succession d'exemples illustre l'apparence désordonnée du processus de délivrance et de contrôle des accès permanents. Ceux qui ont un accès en raison de leur mission ne sont pas tous disposés à s'en servir, débouchant parfois sur de graves problèmes de veille sanitaire. A l'opposé, ceux qui voudraient un accès et qui devraient l'obtenir doivent attendre plusieurs années avant de pouvoir profiter pleinement du précieux sésame. L'ensemble donne une image plutôt négative du dispositif que le nouveau SNDS est supposé réparer[490].

Il est utile de rappeler que l'exclusivité de l'accès permanent à certains acteurs spécifiquement nommés par arrêté procède avant tout d'une volonté de protéger la vie privée des individus. Pourtant, au regard de la confusion qui règne sur ce type d'accès, qu'il s'agisse des modalités de choix des bénéficiaires, ou bien de la mise en œuvre de ces accès, il est permis de douter de la réelle protection conférée aux données. Certains seront d'ailleurs tentés de faire un parallèle entre l'incertitude qui plane autour des modalités de contrôle de la bonne mise en œuvre des accès permanents et la vérification de la bonne sécurité des données de santé. Sur ce point, il ne faut pas oublier que c'est avant tout la CNIL qui est la gardienne de la sécurité des données : son activité s'exerce indépendamment de l'évolution des acteurs titulaires de l'accès permanent.

[488] Le COPIIR est le Comité d'Orientation et de Pilotage d'Information Inter-Régimes, v. Institut des données de santé, « Processus d'élaboration de l'arrêté permettant l'utilisation des données anonymisées de l'assurance maladie obligatoire ».

[489] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 76 : le rapport ne donne aucune explication sur les raisons qui ont poussé la DREES à reporter l'utilisation de l'accès permanent à 2010 alors qu'elle en bénéficiait dès 2005.

[490] *Infra* n° 226 à 228.

190. Nous venons donc de constater que la sélection des personnes morales autorisées à accéder au SNIIRAM en permanence soulève des interrogations tant elle comporte des incohérences qu'il est difficile d'expliquer. L'absence de doctrine à cet égard est particulièrement problématique car elle accentue le sentiment que les autorités à l'origine de la délivrance des accès ont agi en toute discrétion, bien heureuses que personne ne souligne les éventuels manques de cohésion des textes publiés. Le choix final des bénéficiaires ne repose évidemment pas sur l'arbitraire des décisionnaires mais répond forcément à une logique précise : pourtant, l'absence d'explication de cette logique sème le doute. Si nous sommes tentés de nous raccrocher à l'explication tenant à la meilleure capacité des acteurs choisis à assurer la protection des données consultées[491], nous allons voir que cette justification n'est pas non plus la moins contestable.

SECTION 2 : L'ARGUMENT FRAGILISÉ DE LA SÉCURITÉ DES DONNÉES EN ACCÈS PERMANENT

191. Le principe essentiel qui enveloppe l'ensemble du mécanisme d'accès aux données de santé est la protection de la vie privée[492] des individus. Ce principe s'applique à travers la création d'un dispositif destiné à assurer la sécurité des données de santé contenues dans le SNIIRAM devenu SNDS. S'il est incontestable que la sécurité des données de santé à caractère personnel, qu'elles soient directement ou indirectement identifiantes, est primordiale, la méthode consistant à brandir systématiquement cet argument pour justifier que seuls quelques acteurs peuvent bénéficier de l'accès permanent est critiquable (Paragraphe 1). De cette volonté de mettre en avant la sécurité a même découlé certains effets directement, ou indirectement, contreproductifs pour les acteurs eux-mêmes bénéficiaires de l'accès permanent (Paragraphe 2).

Paragraphe 1 : L'insuffisance de l'argument sécuritaire

192. Les données de santé à caractère personnel sont, par principe, interdites d'accès par la loi Informatique et Libertés[493]. Leur collecte, mais surtout leur traitement sont prohibés comme

[491] *Supra* n° 183.

[492] *Supra* n° 4 et 54 à 62.

[493] Loi n° 78-17 du 6 janvier 1978, *op. cit.* art. 6.

nous l'avons vu en introduction[494]. Les autorités ont donc saisi l'opportunité de créer des exceptions à cette interdiction en créant le SNIIRAM en 1998[495] avec la possibilité pour les seuls acteurs spécialement nommés d'y avoir accès en permanence. L'une des premières explications de cette position tenue par l'Etat français est que ce dernier veut inspirer la confiance aux citoyens et professionnels dont les données de santé à caractère personnel sont stockées numériquement. En fermant la base de données et en limitant drastiquement l'accès permanent à une liste exhaustive de bénéficiaires, l'Etat s'impose comme le garant de la sécurité des informations de chacun. Le secret professionnel ainsi conservé, en apparence, par les autorités nationales est de nature à « *préserver la confiance du citoyen dans le système de santé et les technologies de l'information et de la communication auxquelles celui-ci a recours* » comme l'indiquait le Groupe européen d'éthique des sciences et des nouvelles technologies de la Commission européenne dans son avis rendu en 1999[496]. Le même Groupe considérait alors déjà que la sécurité dont devaient faire preuve les systèmes informatisés servant à stocker les données, et, par extension, les données elles-mêmes, constituait un « *impératif éthique* ». Cela s'expliquerait par le fait que la sécurité conférée aux données et bases de données informatisées « *conditionne le respect des droits et libertés de l'individu* ».

La création d'un accès permanent d'apparence extrêmement encadré et réglementé semble donc avoir deux objectifs : le premier est de garantir véritablement aux individus que leurs données sont protégées et accessibles seulement aux acteurs les plus vertueux. Le second est d'inspirer, par voie de conséquence, la confiance aux individus. Cependant, la sécurité qui entoure l'accès permanent aux données de santé en France reste discutable.

193. Si nous admettons que c'est la sécurité des données qui permet de justifier que l'accès permanent aux données de santé ait été réservé à une liste restreinte de bénéficiaires pendant quinze ans (du premier arrêté de 2002[497] à la mise en œuvre du SNDS en 2017[498]), l'analyse de son fonctionnement reste instructive. En effet, pendant ses premières années d'existence, l'accès permanent ne prévoyait pas de mesures plus contraignantes que celles qui étaient déjà

[494] *Supra* n° 60.

[495] Loi n° 98-1194 du 23 décembre 1998, *op. cit.*

[496] Commission européenne, *Avis n° 13 du 30 juillet 1999 : Aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information*, *op. cit*.

[497] Arrêté du 11 avril 2002, *op. cit*.

[498] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

imposées aux acteurs pouvant se voir accorder un accès ponctuel[499]. La principale mesure de sécurité prise par arrêté était l'établissement de la liste permettant d'identifier chaque individu pouvant accéder aux données[500]. L'autre caution de la sécurisation de l'accès permanent était bien entendu l'analyse du protocole, faisant l'objet d'une publication par arrêté, par la CNIL : il va de soi que l'avis rendu par les membres de cette Commission est de nature à garantir que tout est mis en œuvre pour assurer la meilleure protection possible des données.

Malgré cela, un élément important de la sécurisation de l'accès permanent est toujours absent : il s'agit du suivi *a posteriori* des utilisations que chaque acteur fait de son accès permanent. D'après ce que nous avons observé jusqu'ici, c'est davantage un contrôle *a priori* qui était réalisé, ce qui est encore insuffisamment sécurisant. Ce n'est qu'à partir de 2011[501] que des indications concrètes portant sur la traçabilité des usages de données sont proposées dans le texte des arrêtés. L'arrêté de 2013[502] reprendra le même type de précisions sur la sécurité apportée à l'accès permanent par le prisme du contrôle de l'activité des différents bénéficiaires. Il aura donc fallu attendre neuf ans entre la mise en application de l'accès permanent et la publication, bien que de manière sommaire et à titre informatif, des modalités d'anonymisation des informations[503]. Cette description s'est accompagnée de la création d'un « *annuaire sécurisé* […] *des personnes habilitées à accéder au Système national d'information interrégimes de l'assurance maladie* […] *établi pour contrôler toutes les autorisations d'accès.* »[504]. En plus de cela, « *des dispositifs de journalisation des interrogations sont mis en œuvre pour contrôler les accès au système. Des procédures d'exploitation systématique de ces journaux sont élaborées de manière à permettre l'audit des accès au système* »[505]. C'est ce type de mesure qui aurait dû être mis en œuvre dès la création de l'accès permanent, et non neuf ans plus tard, pour justifier que les données de santé n'étaient accessibles facilement et en permanence qu'à une liste limitée d'acteurs. La sécurité des données n'est pas acquise par sa simple annonce, il est nécessaire que des procédures détaillées soient officiellement publiées, connues, et appliquées pour que l'ensemble du dispositif et de l'argumentaire soit convaincant.

[499] V. Partie II, Titre I.

[500] *Supra* n° 126 à 131.

[501] Arrêté du 1er décembre 2011, *op. cit.*

[502] Arrêté du 19 juillet 2013, *op. cit.*

[503] Cette anonymisation s'effectue par chiffrement appelé FOIN, v. *supra* n° 139 à 142.

[504] Arrêté du 1er décembre 2011, *op. cit.*

[505] *Ibid.*

En l'espèce, le fait que le contrôle *a posteriori* de l'utilisation de l'accès permanent n'ait pas été prévu avant 2011[506] est de nature à remettre en question l'édifice argumentaire de la sécurité des données. Cela envoie même un signal négatif qui laisse penser que l'usage des données accessibles en permanence n'était pas totalement sous contrôle. Bien que ce constat ne signifie pas d'emblée que les données aient été utilisées de façon inappropriée, il témoigne du manque intrigant de clairvoyance et d'anticipation des autorités sur ce sujet sensible.

194. Un autre facteur peut être opposé à l'idée que l'accès permanent soit limité pour garantir la sécurité des données. C'est celui, bien plus factuel, du piratage quasi-inévitable des informations. Certains auteurs l'ont bien compris[507] en mettant en garde les responsables des bases de données, dont fait partie le SNIIRAM, aujourd'hui inclus dans le SNDS. Quelle qu'elle soit, la sécurité, aussi élevée soit-elle, ne peut pas être infaillible face à la volonté de certains individus de venir pirater et dérober les données de santé[508]. La promesse de l'inviolabilité des données mises à disposition en permanence qui semblait être délivrée par les autorités de 2002[509] jusqu'à la réforme de 2016[510] paraît alors inatteignable. Ce raisonnement ne signifie pas pour autant qu'il ne soit pas utile de protéger les données en y voyant là un acte superflu dès lors qu'elles sont susceptibles d'être subtilisées par un éventuel pirate. Bien au contraire, cette faille constante, à laquelle nul ne peut remédier, dans le dispositif de sécurité qui entoure les données, doit être perpétuellement prise en compte pour imaginer les meilleurs moyens de protéger les informations tout au long de leur parcours.

Garder à l'esprit l'existence de cette faille nous rappelle la vulnérabilité des systèmes informatisés et oblige les responsables des différentes bases à la plus grande vigilance. Par

---

[506] *Ibid.*

[507] MESSI P., « Big Brother : la surveillance de la population », *Les Tribunes de la santé*, 2010/4, n° 29, p. 69-74.

[508] C'est essentiellement aux Etats-Unis que les affaires de piratage de données de santé les plus médiatisées ont éclaté. Ainsi en 2016, une personne seule a réussi à prendre le contrôle de l'intégralité du système informatique du Hollywood Presbyterian Medical Center, maîtrisant ainsi toutes les données relatives aussi bien au personnel de l'établissement qu'aux patients y étant soignés, WINTON R., « Hollywood hospital pays $17,000 in bitcoin to hackers ; FBI investigating », *Los Angeles Times*, 18/02/2016. La même année, c'est un autre établissement, le York Hospital, qui a été victime du vol des données personnelles de ses 1 400 employés, incluant leur numéro de sécurité sociale., HOEY D., « York Hospital reports data breach affecting its employees », *Portland Press Herald*, 24/02/2016. Ces affaires ne sont que des exemples concrets de la vulnérabilité permanente des systèmes informatisés.

[509] Arrêté du 11 avril 2002, *op. cit.*

[510] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

extension, cela porte un coup à l'idée selon laquelle la sécurité des données de santé est assurée si elles ne sont accessibles qu'au plus petit nombre : le seul fait que ces données soient informatisées les fragilise. A la lumière de ces paramètres, l'accès permanent qui serait réservé à quelques bénéficiaires pour assurer l'intégrité des données et le respect de la vie privée des individus n'est que partiellement acceptable. Certes, la protection à réserver à ces informations est importante, mais la qualité de ladite protection depuis 2002 ne semble pas avoir toujours été à la hauteur des enjeux. Nous pourrions être tentés d'y voir là un prétexte avancé par les autorités pour ne pas modifier plus vite l'accès permanent tant les difficultés juridiques et techniques étaient, et sont encore, nombreuses.

195. La question de la sécurité des données de santé a eu des répercussions directes sur les acteurs eux-mêmes susceptibles de disposer de l'accès permanent, ou déjà titulaires dudit accès. Un sujet paradoxal lorsque l'on sait que, comme nous venons de le détailler, ces mesures de protection n'étaient peut-être pas tout à fait au point.

Paragraphe 2 : La sécurité au détriment des bénéficiaires

196. Avant d'amorcer notre raisonnement, commençons par rappeler une fois de plus que notre propos n'est pas de mettre en cause le fait que les données de santé à caractère personnel fassent l'objet d'une protection, conformément à la loi Informatique et Libertés[511]. En revanche, il est nécessaire de s'interroger sur les modalités d'application et sur l'efficacité du dispositif qui a été choisi pour assurer la protection de la vie privée des individus ; ce que nous faisons tout au long du présent chapitre. Cette sous-partie présente ainsi l'opportunité d'étudier l'impact parfois négatif du mécanisme sécuritaire sur le fonctionnement de l'accès permanent.

197. Nous en avons déjà évoqué le contenu : l'accès permanent aux données de santé diffère dans la variété des informations disponibles selon les acteurs qui peuvent en bénéficier[512]. Chaque arrêté successif a ainsi pu faire évoluer cette situation en proposant parfois d'élargir le champ des données mises à disposition. Cette ouverture a, malheureusement, été ralentie par des considérations juridiquement acceptables mais contestables dans leurs modalités de mise

[511] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[512] *Supra* n° 143.

en œuvre. Le cas de la DREES est tout à fait symbolique à cet égard[513]. La Cour des comptes considère que les agents de la DREES font partie des plus grands utilisateurs des données de santé[514] alors qu'ils n'ont pas accès aux données individuelles exhaustives (ces données sont proposées par le « *datamart* de consommation inter-régimes », ou DCIR[515], qui fait partie du SNIIRAM). Malgré leur productivité constatée et l'utilité incontestable du travail des différents agents, l'accès à plus d'informations ne leur a pas été accordé avant la réforme de la loi de modernisation de notre système de santé[516] et sa concrétisation dans le décret paru le 28 décembre 2016[517].

Or, cet accès aurait dû leur être accordé bien plus tôt, dès 2013 si la procédure avait été rapide et efficace. Le rapport de la Cour des comptes[518] signale bel et bien que le COPIIR avait délivré, dès le 18 avril 2013, un avis favorable à ce que les agents de la DREES accèdent aux données de santé individualisées du DCIR. En dépit de ce signe positif, il ne s'est rien passé avant plusieurs années. Si l'on en cherche la cause, il semblerait que c'est le processus de vérification des données qui ait retardé la prise de décision finale. Le projet d'arrêté destiné à élargir l'accès permanent de la DREES avait bien été transmis à la CNIL. Cependant, cette dernière a souhaité que la CNAMTS réalise, en amont de sa décision, deux études relatives à la sécurité des données de santé. Ces études n'ont jamais été produites, la proposition d'arrêté est donc restée suspendue pendant 3 ans, avant que la réforme de 2016[519] ne vienne dépoussiérer le dispositif.

Le cas de la DREES est un cas d'école des contradictions qui ont pu régir la gestion de l'accès permanent. L'action positive de cette direction était parfaitement connue et, alors que son expertise dans l'analyse et l'utilisation des données de santé était répandue, l'autorisation de consulter les données individualisées est restée dépendante de l'action, ou plutôt l'inaction, de la CNAMTS. Cette dernière, en ne réalisant pas le travail nécessaire sur la sécurité des données, a privé l'un des premiers utilisateurs de l'accès permanent d'élargir son potentiel.

---

[513] Concernant l'ouverture de l'accès permanent au bénéfice de la DREES, v. *supra* n° 188.

[514] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 76.

[515] Le DCIR est notamment défini à la page 32 du rapport de la Cour des comptes, *ibid*.

[516] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[517] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*.

[518] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 77.

[519] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

198. L'ATIH[520] s'est retrouvée, peu ou prou, dans le même cas de figure. Bien que son usage des données de santé ne soit pas aussi remarquable que celui de la DREES, le blocage que l'agence a subi dans l'ouverture de son accès permanent aux données individualisées ne peut être ignoré. C'est en 2008 que l'ATIH a obtenu son accès permanent aux données agrégées ainsi qu'à l'EGB[521]. Or, comme le souligne le rapport BRAS[522], les membres de l'agence étaient dans l'attente de la décision de la CNIL et de la publication d'un arrêté validant l'accès aux données individualisées en 2013.

Pour pousser le mimétisme jusqu'au bout, il se trouve que le décret paru en décembre 2016[523] a accordé à l'ATIH, tout comme pour la DREES, l'accès aux données individualisées. Il semblerait donc que pendant la période qui a séparé l'année 2013 de l'année 2016, les responsables de la gestion de l'accès permanent et notamment de l'aspect sécuritaire des données, CNIL et CNAMTS en tête, aient été frappés d'immobilisme patent. La problématique de la sécurité des données a servi de justification pour ne rien modifier dans l'accès permanent. Il y a pourtant tout lieu de penser, en demeurant dans le champ de l'hypothétique, que les études supplémentaires qui auraient été produites grâce aux nouvelles données individuelles accessibles auraient été bénéfiques à l'ensemble du système de santé : nous pouvons penser à une meilleure gestion des fonds des établissements de soins, la détection plus rapides d'anomalies dans le fonctionnement desdits établissements, ou encore une meilleure appréhension des tendances de consommation de soins conduisant à la mise en œuvre de mesures adéquates. Ces exemples sont l'illustration concrète de l'impact contreproductif que la sécurité des données a parfois eu sur l'accès permanent.

199. La sécurité et la protection des informations qui concernent les individus sont des notions qui ne relèvent pas que du droit. Outre le fait qu'une procédure prédéfinie et appliquée doit assurer le respect de la vie privée, certains auteurs voient dans cette quête de la protection des droits fondamentaux une excuse trop évidente pour ne pas travailler à trouver un moyen d'approfondir l'accès permanent. Parmi ces auteurs, nous retrouvons notamment D. SICARD, qui a été médecin, professeur de médecine à l'Université Paris Descartes, et président du Comité

[520] Agence technique de l'information sur l'hospitalisation, v. *supra* n° 23.

[521] *Supra* n° 148.

[522] Rapport de P.-L. Bras, *op. cit.*, p. 34.

[523] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*.

consultatif national d'éthique (CCNE) de 1999 à 2008, et J. de KERVASDOUE, économiste de la santé et professeur au Conservatoire national des arts et métiers (CNAM).

Ils ont tous deux publié une tribune dans le journal Le Monde le 16 janvier 2013 portant sur l'accès aux données de santé en France. A travers ce texte D. SICARD[524] soulève le fait que les résistances que l'Etat français montre face à l'accès aux données de santé trouvent leur origine « *dans la volonté de maintenir l'illusion que la santé des Français est gérée avec rigueur et discernement* ». Si l'on effectue le parallèle avec l'accès permanent, nous pouvons estimer que l'Etat a été aussi intransigeant pour les uns, frileux pour les autres, vis-à-vis de son développement en harmonie avec la sécurité des données, afin de répandre un sentiment de maîtrise et de bonne gestion du dispositif parmi les Français : il pourrait s'agir d'une portée philosophique attribuée au fonctionnement verrouillé de l'accès permanent. Les citoyens pouvaient bel et bien interpréter les difficultés des bénéficiaires de l'accès permanent à traiter plus de données comme une garantie de sécurité donnée par les autorités. La réalité modère cette impression, à l'image de l'empêchement subi par la DREES[525] : le fonctionnement initial des autorisations d'accès permanent repose bien sur la notion de protection des informations, mais, pour reprendre les termes de D. SICARD, « *l'illusion* » ne dure pas si l'on en connaît les détails.

Dans les différents exemples que nous venons d'aborder, la haute sécurisation des données associée à une procédure qui peut facilement générer des blocages sont la source d'une baisse de performance de la part des bénéficiaires de l'accès permanent. Si la recherche de la performance était auparavant souvent identifiée comme néfaste pour le respect des droits fondamentaux[526], nous verrons ultérieurement[527] que l'ambition du nouveau système est de trouver l'équilibre entre la sécurité des données d'une part, et les performances[528] des bénéficiaires d'autre part.

---

[524] Cité *in* DEBOST C., « Publication du rapport sur la gouvernance et l'utilisation des données de santé, la promesse d'un entrebâillement de l'Open data dans le secteur de la santé ? », *RDS*, janvier 2014, n° 57, p. 947 à 949.

[525] *Supra* n° 197.

[526] BOURRET R., DEBOST C., MARTINEZ E., VIALLA F., « Lorsque le respect des droits fondamentaux l'emporte [encore] sur la quête de la performance », *RDS*, 2014, n° 57, p. 864-868

[527] *Infra* n° 219 à 228.

[528] Par performance des bénéficiaires de l'accès permanent, nous pouvons notamment entendre l'optimisation accrue de leurs missions grâce à l'exploitation des données de santé, ou la production d'études plus nombreuses et plus précises utiles à leurs activités.

CONCLUSION DU CHAPITRE I

200. L'accès permanent aux données de santé contenues dans les bases médico-administratives repose sur un prédicat inégalitaire : seule une poignée d'acteurs nommés par arrêté, aujourd'hui par décret, sont les bénéficiaires privilégiés du droit d'accès, ceci afin de protéger le droit au respect de la vie privée des individus. A l'inverse, tous les acteurs absents de cette liste sont, par définition, obligés de se plier à la procédure d'accès sélectif pour demander l'accès à des données en vue de réaliser un traitement spécifique. Mais les piliers de l'accès permanent révèlent de sérieuses failles depuis sa création. En effet, pour rendre cette inégalité plus acceptable, il aurait été utile que la démarche amenant les autorités à choisir les bénéficiaires de l'accès permanent soit définie et expliquée. Or, malgré la réforme, ces informations ne sont toujours pas disponibles, ce qui peut avoir pour effet de provoquer un sentiment d'iniquité dans l'esprit des exclus de l'accès permanent.

201. L'absence de résultats mesurés et identifiés dans l'amélioration des missions de service public des bénéficiaires de l'accès permanent aux données de santé est aussi de nature à renforcer la défiance à l'égard du dispositif. La survenance de scandales sanitaires tels que l'affaire du Mediator a d'ailleurs mis en lumière l'absence de maîtrise et de connaissance de données de santé pourtant disponibles et accessibles aux acteurs les mieux placés pour agir.

202. L'idée selon laquelle la sécurité des données de santé est mieux préservée dans le cadre de l'accès permanent est aussi fragilisée. Pendant près de dix ans, les bénéficiaires de cet accès ont pu traiter les données accessibles sans aucun rapport officiel de suivi permettant d'avoir une connaissance de la manière dont les données ont été exploitées. Dans le même temps, une promesse d'inviolabilité des données de santé mises à disposition dans le cadre de l'accès permanent était délivrée alors que le risque de piratage peut difficilement être écarté. En d'autres termes, l'argument selon lequel les données de santé étaient mieux protégées au sein de l'accès permanent qu'au sein de l'accès sélectif est difficilement défendable avec nos connaissances actuelles. L'argument de la sécurité des données est d'autant plus affaibli par ses conséquences sur certains bénéficiaires de l'accès permanent. En effet, en raison des procédures de contrôle, certains acteurs n'ont pu accéder à des données de santé essentielles à leur activité que plusieurs années après en avoir formulé le besoin.

203. L'argumentaire qui entoure l'édifice de l'accès permanent a un objectif louable qui est la protection de la vie privée, mais sa mise en œuvre révèle plusieurs zones d'ombre. C'est le manque de communication, de pédagogie et de transparence sur le sujet qui conduit, dans la pratique, à ce que l'on ne sache plus clairement qui peut être sélectionné pour accéder en permanence aux données de santé, comment et dans quel but. C'est face à cette forme de défiance grandissante devant un système parfois teinté d'opacité, que des études ont été menées sur l'utilisation réelle de l'accès permanent afin que celui-ci soit mieux optimisé dans le cadre de la réforme du 26 janvier 2016[529].

[529] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

CHAPITRE II
LE DÉPASSEMENT BIENVENU DES LIMITES À L'ACCÈS PERMANENT

204. Il aura fallu attendre quatorze ans[530] pour qu'une étude précise soit publiée au sujet de l'accès permanent aux données de santé et de l'utilisation qu'en font les bénéficiaires. Remarquons que ce thème reste très confidentiel et ne semble toujours pas de nature à conduire à la production de davantage de notes et d'analyses malgré des bénéfices attendus, ou espérés, non négligeables pour la santé publique. Le document produit par la Cour des comptes[531] s'attache aux faits et décrypte, sur la durée, les utilisations par les différents acteurs de l'accès permanent. Il en ressort un diagnostic sévère. Hormis quelques exceptions[532], les données de santé accessibles en permanence sont sous-exploitées (Section 1), ce qui devrait changer avec la mise en œuvre du nouveau système national des données de santé (Section 2).

SECTION 1 : LA SOUS-EXPLOITATION DOMMAGEABLE DE L'ACCÈS PERMANENT

205. Nous avons précédemment[533] abordé les différents éléments qui conduisent à penser que l'accès permanent a été organisé avec trop peu de considération pour l'impact positif qu'il peut avoir dans le cas d'une exploitation complète et vertueuse. Il est maintenant nécessaire d'étudier le rapport de la Cour des comptes pour comprendre comment les trop rares usages de l'accès permanent (Paragraphe 1) ont conduit à une difficulté d'en quantifier les résultats potentiels qui auraient pu justifier l'existence d'un tel accès (Paragraphe 2).

[530] Cet écart part de la publication du premier arrêté SNIIRAM le 11 avril 2002, *op. cit.*, et va jusqu'à la parution du document de la Cour des comptes de mars 2016 sur « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*

[531] *Ibid.*

[532] L'utilisation que fait la DREES de l'accès permanent fait partie de ces exceptions, v. *supra* n° 197.

[533] *Supra* n° 176 à 203.

Paragraphe 1 : L'insuffisance d'utilisation de l'accès permanent

206. C'est par une lettre du 3 décembre 2014[534] que la commission des affaires sociales de l'Assemblée nationale, alors présidée par C. LEMORTON, a demandé au Premier président de la Cour des comptes, D. MIGAUD, de réaliser notamment « un rapport d'enquête sur les données médicales personnelles inter-régimes détenues par l'assurance maladie » pour la fin du premier trimestre 2016. Coïncidant avec la réforme du système d'accès aux données de santé[535], ce rapport avait pour ambition de détecter les différentes failles et dysfonctionnements du dispositif afin de proposer des pistes d'améliorations pour la construction du nouveau SNDS. Finalement remis et publié en mars 2016, le document est très instructif et apporte de nombreux exemples concrets du manque d'engagement des bénéficiaires de l'accès permanent[536].

207. La CNAMTS est la première utilisatrice de l'accès permanent avec, en septembre 2015, plus des trois quarts des habilitations délivrées à l'ensemble des organismes disposant d'une autorisation. A cette date, 281 personnes[537] de cet organisme étaient habilitées à accéder aux données de santé contenues dans le SNIIRAM. Malgré ce nombre important de potentiels accédants aux données, la Cour souligne qu'au regard de l'étendue considérable des missions de la CNAMTS, l'accès permanent n'a été utilisé que de manière diffuse et partielle dans chacun des domaines d'action. Ainsi, l'activité de lutte contre les abus et les fraudes à la sécurité sociale n'a pas assez tiré profit du potentiel offert par l'accès permanent. Si le nombre de requêtes opérées par les services de la CNAMTS est passé de 146 en 2012 à 392 en 2014[538], la Cour estime que c'est encore insuffisant. A l'échelle des directions régionales de service médical (DRSM) le constat est plus variable avec certaines régions bien plus utilisatrices du SNIIRAM pour détecter les fraudes (20 589 requêtes réalisées en Île-de-France et 12 998 en

[534] V. Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, Annexe I, p. 121.

[535] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *op. cit.*

[536] Le manque d'engagement des acteurs ayant un accès permanent aux données de santé se traduit par un nombre très faible de requêtes effectuées sur les bases de données pour obtenir des données. La Cour des comptes souligne que l'accès est encore insuffisamment utilisé par l'Assurance maladie tandis que des agences comme l'ANSM, l'INSERM ou la HAS ont un taux d'utilisation de l'accès permanent qui reste trop marginal. V. *infra* n° 207 à 211.

[537] V. Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, encadré p. 65.

[538] *Idem*, p. 70.

Midi-Pyrénées entre 2012 et le 30 juin 2015) que d'autres (309 requêtes effectuées en Franche-Comté et 703 dans le Limousin entre 2012 et le 30 juin 2015)[539].

Le constat de la Cour des comptes est important en ce qu'il met en lumière le fait que même la CNAMTS, composante centrale du système de santé français, n'utilise pas assez l'accès permanent aux données de santé qui lui est offert. L'insuffisance d'utilisation s'entend aussi bien au sens de la fréquence des requêtes, trop peu nombreuses et hétérogènes selon les régions, qu'au sens de la finalité des utilisations qui sont trop limitées s'agissant de la gestion des risques sanitaires, des études sur la santé publique[540].

Pour tenter d'apporter des explications à cette utilisation trop résiduelle, les auteurs du rapport s'intéressent à la question des moyens alloués à l'exploitation des données concernant les abus et les fraudes. Ces moyens peuvent être affectés à deux pôles bien précis : le premier concerne le pilotage du projet, le second a trait à la concrétisation des actions qui doivent découler des constats réalisés grâce aux données.

208. La première problématique, celle du pilotage, exige que des personnes suffisamment compétentes soient affectées aux postes opérationnels. Or, bien que bénéficiant de l'accès permanent dès 2002[541], la CNAMTS ne semble s'être réellement saisie de cette question qu'en 2006 avec la création de la « *direction du contrôle contentieux et de la répression des fraudes* ». Cette direction, appelée aujourd'hui direction de l'audit, du contrôle contentieux et de la répression des fraudes, ne comptait que 25 agents en 2007, puis 35 au 30 septembre 2015. Parmi ces agents, seulement 7 sont véritablement habilités à utiliser le SNIIRAM. Ces informations

[539] Ces données sont à mettre en perspective avec la population présente dans chacune des régions prises en considération. Ainsi, au 1er janvier 2015, d'après l'Insee, la région Île-de-France comptait 12 millions d'habitants, la région Midi-Pyrénées en comptait 3 millions, la région Franche-Comté en comptait 1,1 million, et la région Limousin n'en comptait que 733 mille. Si l'on rapporte le nombre de requêtes des DRSM pour détecter les fraudes au nombre d'habitants de chaque région cela donne environ : 1 requête par tranche de 583 habitants en Île-de-France, 1 requête par tranche de 231 habitants en Midi-Pyrénées, 1 requête par tranche de 3 560 habitants en Franche-Comté, et 1 requête par tranche de 1 043 habitants dans le Limousin. Nous constatons que la mise à l'échelle du nombre de requêtes effectuées selon le nombre d'habitants d'une région confirme que les DRSM de Franche-Comté et du Limousin ont bien moins sollicité les données de santé disponibles en accès permanent que celles de Midi-Pyrénées et d'Île-de-France. V. Insee, « Tableaux de l'économie française », Collection Insee Références, édition 2016.

[540] Depuis l'étude réalisée par une équipe de la CNAMTS sur le Médiator en 2009, seulement une dizaine d'études de cette nature ont été réalisées, Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 67.

[541] Arrêté du 11 avril 2002, *op. cit.*

relatives au nombre d'agents ne portent que sur les effectifs du siège de la CNAMTS, comme le déplorent les auteurs du rapport. Aucune donnée officielle et vérifiable ne permettrait de savoir, avec exactitude, combien de personnes sont affectées à ces missions dans les DRSM. La situation est telle que l'Etat n'a pas les moyens de connaître la part d'utilisation de l'accès permanent par les différentes CPAM dans le cadre du contrôle des abus et des fraudes.

209. Le second enjeu tient aux moyens mis à disposition pour donner suite aux fraudes et abus détectés grâce à l'usage de l'accès permanent aux données de santé. Comme la CNAMTS l'a précisé à la Cour des comptes, « *augmenter de façon conséquente la détection d'atypies grâce au SNIIRAM n'a un sens que dans la mesure où l'assurance maladie a les moyens de mener les investigations correspondantes et nécessaires* »[542]. Or, il semblerait que la CNAMTS a plutôt eu tendance à réduire ses effectifs de praticiens-conseils au fil des ans[543], ce qui a eu un impact direct sur les capacités à faire aboutir les enquêtes permises par l'exploitation de l'accès permanent.

Nous pouvons déduire de ces éléments que si les ambitions de l'accès permanent sont connues, les bénéficiaires ne se donnent pas les moyens d'atteindre leurs objectifs. Malheureusement, ce qui est observé chez le principal acteur de l'accès permanent, la CNAMTS, l'est également chez les autres.

210. La CNAMTS n'est pas le seul acteur à disposer d'un accès permanent très large aux données de santé depuis la création du système. Les autres régimes de sécurité sociale aussi disposent d'un accès égal mais n'en font qu'une utilisation très légère. La Cour des comptes indique à ce titre[544] que, entre septembre 2014 et août 2015, le Régime social des indépendants (RSI, devenu Sécurité Sociale des Indépendants) n'a accédé que 2 171 fois aux données du SNIIRAM, sans même penser à se servir de l'EGB ou du PMSI[545]. Dans le même temps, la Caisse centrale de la Mutualité sociale agricole (CCMSA) a effectué bien plus de requêtes avec

[542] V. Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 73.

[543] *Ibid.*, les auteurs du rapport ne dévoilent pas de données chiffrées tout en affirmant que le nombre de praticiens-conseils de la CNAMTS n'a cessé de se réduire.

[544] *Idem*, encadré p. 74.

[545] Rappelons qu'en 2015 le RSI comptait 2,8 millions de cotisants. V. « L'essentiel du RSI », *Edition 2016 – Données 2015*, septembre 2016.

1 231 visant des données agrégées, et 10 126 visant des données individuelles[546]. Le nombre de requêtes peut paraître important et laisser penser que ces deux acteurs savent tirer profit de leur accès permanent. Mais en réalité, ces usages sont trop peu fréquents pour que ces organismes développent une réelle expertise dans le traitement des données de santé.

211. Outre les grands acteurs de l'Assurance maladie, nous savons que beaucoup d'autres structures sont titulaires d'un accès permanent depuis 2002[547]. Les agents des ministères sociaux peuvent ainsi être habilités à accéder aux données agrégées et à l'EGB. Seulement, de septembre 2014 à août 2015, moins de 1 200 accès aux données agrégées ont été effectués, et seulement 662 requêtes sur l'EGB ont été faites. En sachant que les termes « *agents des ministères sociaux* » incluent toutes les directions de ces ministères (DSS[548], DREES[549], DGOS[550], DGS[551], DGCS[552]) on comprend bien vite que le nombre de requêtes sur une année est faible. La DREES est en tête des acteurs, hors assurance maladie, à utiliser l'accès permanent au SNIIRAM : malgré son accès restreint[553], les 12 agents habilités ont su exploiter les données de l'EGB pour réaliser de nombreuses études. Face à cela, la DSS n'utilise que très peu l'accès permanent, et les autres directions ne l'utilisent même pas du tout. Du côté des ARS, les consultations sont un peu plus nombreuses avec 7 762 accès aux données agrégées et une moyenne de 125 requêtes par mois sur l'EGB entre septembre 2014 et août 2015[554]. Une fois de plus, les auteurs du rapport relativisent l'apparence volumineuse de ces accès qui pourraient être beaucoup plus nombreux.

Ce constat est surprenant et, bien qu'il soit réalisé tardivement[555], permet de prendre conscience du travail, presque pédagogique, qui doit être mené auprès des différents bénéficiaires de l'accès permanent pour qu'ils apprennent à en tirer le meilleur parti.

---

[546] Pour sa part, la MSA comptait 5,6 millions de ressortissants au régime agricole au 1er janvier 2016.

[547] *Supra* n° 104 à 113.

[548] La DSS est la Direction de la Sécurité Sociale.

[549] La DREES est la Direction de la Recherche, des Etudes, de l'Evaluation et des Statistiques.

[550] La DGOS est la Direction Générale de l'Offre de Soins.

[551] La DGS est la Direction Générale de la Santé.

[552] La DGCS est la Direction Générale de la Cohésion Sociale.

[553] *Supra* n° 197.

[554] V. Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 78.

[555] Ce constat a été officialisé et publié en 2016, après 14 ans de mise en service de l'accès permanent.

Au-delà d'une exploitation par l'Etat ou les régimes d'assurance maladie, plusieurs agences, autorités sanitaires, chercheurs en santé publique, disposent de l'accès permanent. Nous pouvons citer l'ANSM, l'InVS, devenu Santé Publique France, l'INSERM ou encore la HAS. Toutes ces entités recourent à des utilisations de leur accès permanent qui « *restent marginales* ».

212. A travers ces chiffrages, plus ou moins précis, du nombre de requêtes effectuées, la Cour des comptes nous interpelle sur l'absence de coordination entre les bénéficiaires de l'accès permanent et les usages qui peuvent en être potentiellement faits. Etonnamment, la question de la sécurité des données de santé traitées par le biais de l'accès permanent n'est pas étudiée. Seul l'enjeu de la bonne exploitation du système semble préoccuper les auteurs du rapport. Ce qui ressort de l'analyse des pratiques depuis la mise en œuvre des premiers accès permanents, c'est qu'aucune politique d'action commune ne semble avoir été définie pour améliorer le service public. Chaque acteur paraît livré à sa propre gestion de son accès permanent, d'où il découle un certain flottement et le sentiment que l'accès permanent est, pour quelques bénéficiaires, tombé en désuétude. Ceci nous amène à devoir étudier les difficultés à évaluer les bienfaits, ou non, de l'accès permanent au regard du désintéressement dont il a fait l'objet pendant de si longues années.

Paragraphe 2 : L'insuffisance d'évaluation de l'accès permanent

213. L'un des principaux enseignements que nous pouvons retirer de l'étude détaillée effectuée par les auteurs du rapport de la Cour des comptes[556] est le suivant : très peu de données chiffrées sur les résultats concrets de l'accès permanent sont disponibles. Nous pouvons reconnaître que des informations statistiques précises sont proposées sur les taux d'utilisation de l'accès permanent[557], mais les finalités de ces usages demeurent floues. Nous entendons par les termes « *résultats concrets* », la production de données chiffrées sur l'impact, autant fonctionnel (telle la réduction des délais de traitement de certaines demandes, de la réalisation de certaines études), sanitaire (comme l'amélioration des pratiques liées à la pharmacovigilance) que financier (par exemple l'optimisation des moyens dont disposent les différents acteurs) sur les

[556] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*

[557] *Supra* n° 206 à 212.

missions de service public. Un premier point nous intéressera ici, il s'agit de l'absence d'informations relatives à l'accès permanent dans ses premières années d'existence. Puis notre analyse portera sur les difficultés à quantifier les avantages nouveaux procurés par ce type d'accès. Ces deux éléments sont de nature à alimenter les arguments tendant à contester l'existence de l'accès permanant dans sa forme antérieure à la loi relative à la modernisation de notre système de santé[558].

214. De prime abord, on peut signaler que nous n'avons que très peu, voire pas du tout, d'informations quant à la fréquence de recours aux données de santé dans le cadre de l'accès permanent avant l'année 2009. En effet, l'entrée en activité du système a eu lieu en 2002 et les premières statistiques d'utilisation citées par le rapport remontent au plus tôt à 2007, la majorité d'entre elles commençant à courir en 2009. Pourquoi une collecte aussi tardive des informations qui permettent de suivre la bonne tenue de l'accès permanent aux données de santé ? Aucune réponse directe n'est à notre portée au moment d'écrire ces lignes. Peut-être est-ce à cause de l'inexistence de l'Institut des données de santé, ou IDS[559], qui n'a commencé à produire des rapports sur l'accès aux données de santé qu'en 2008. Cette première observation n'est pas neutre : elle indique soit, première hypothèse, que pendant les cinq premières années de mise en fonction de l'accès permanent, les statistiques d'utilisation de l'accès permanent n'ont, ni été récoltées et stockées, ni analysées ; soit, seconde hypothèse, que ces statistiques étaient tellement faibles, éparses, ou imprécises, que les auteurs du rapport de la Cour des comptes ont préféré s'abstenir d'y faire référence. La seconde hypothèse n'est pas impossible étant donné le peu d'intérêt que la majorité des acteurs figurant dans les premiers arrêtés portaient à l'accès permanent.

215. La première hypothèse, en revanche, est plus intéressante. Cela signifierait que pendant les premières années d'existence de l'accès permanent, les autorités françaises se seraient focalisées uniquement sur la sécurisation, en amont, des données et sur le choix des acteurs bénéficiaires. Cette concentration des efforts sur le processus de construction de l'accès permanent est compréhensible, tant l'enjeu de la protection des données personnelles de santé, qui doit combiner les normes juridiques et la création de techniques informatiques suffisamment

[558] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[559] L'IDS a été créé par la loi n° 2004-810 du 13 août 2004 et n'est entré en fonction qu'après la publication de l'arrêté d'approbation du 30 avril 2007, v. *supra* n° 165.

sécurisées, est primordial. Toutefois, le fait que l'IDS, notamment chargé de proposer un rapport annuel sur son activité et de recueillir des informations sur les accès effectués et autorisés, n'ait été créé qu'en 2004 pour être installé en 2007, nous interpelle. Il est difficile d'admettre qu'aucun système de centralisation et de recueil des informations relatives à l'accès permanent (nombre de requêtes, type de requêtes, études réalisées, objectifs visés et éventuellement atteints, impact sur l'activité de l'acteur bénéficiaire), n'ait été pensé plus tôt : cela rend difficile, voire impossible, la quantification des bénéfices éventuellement apportés à la réalisation des missions de service public.

216. Avec le recul que nous possédons aujourd'hui, la mise en œuvre de ce système n'a pas vraiment de sens si nous ne pouvons en mesurer les avantages et inconvénients avec des données concrètes sur les taux d'utilisation, les objectifs et les résultats envisagés et obtenus. La production du rapport de la Cour des comptes[560], au moment de la réforme[561] du SNDS n'est d'ailleurs pas étrangère à cela : le document permet d'avoir un regard global sur l'utilisation de l'accès permanent depuis les années 2007-2009 (en fonction des acteurs). Mais comme nous venons de l'appréhender, une part non négligeable d'informations est manquante. Certains détracteurs du fonctionnement de l'accès permanent ont pu se nourrir de cette absence de suivi en l'analysant comme la preuve d'un désintérêt pour ce mécanisme dont l'utilisation serait laissée au bon vouloir des bénéficiaires désignés par arrêté. Le double discours consistant, d'une part, à affirmer que les données sont accessibles en permanence pour des missions de service public hautement importantes[562], d'autre part, à ne pas s'assurer que lesdites missions de service public bénéficient bien de ce système, participe de la remise en cause de l'existence même de l'accès permanent.

217. Maintenant que la problématique de l'absence d'informations suffisantes sur les usages effectués par les acteurs bénéficiaires entre 2002 et 2007 a été traitée, il paraît opportun de faire basculer notre réflexion en direction des informations qui ont été récoltées ultérieurement ainsi que sur les indications qu'elles nous procurent en termes d'amélioration des missions de service public.

---

[560] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*

[561] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[562] *Supra* n° 99 à 101.

Le chapitre II du rapport de la Cour des comptes[563] est hautement instructif quant aux usages qui ont pu être faits de l'accès permanent à partir des années 2007-2009. Il analyse, pour chaque type d'acteurs, en commençant par l'Assurance maladie, si le recours aux données de santé est fréquent, dans quel but ces données sont utilisées et, fort malheureusement, cela s'arrête là. Le travail des auteurs du rapport n'a, semble-t-il, pas permis de collecter des informations détaillées sur les résultats concrets potentiellement obtenus.

En l'occurrence, les informations délivrées par le rapport sont plutôt d'ordre négatif, c'est-à-dire que ce sont les impacts insuffisants qui sont signalés sans que nous ne sachions quels sont leurs résultats. Nous pouvons citer, à titre d'exemple, l'exploitation « *trop marginale en santé publique* » : le rapport nous rappelle que l'accès permanent aux données de santé devrait être utile aux missions de santé publique en pointant du doigt le fait qu'il n'est pas encore assez mis à profit en ce sens. S'agissant de la pharmacovigilance, nous apprenons que l'implication des différents acteurs est très hétérogène avec de fortes difficultés à évaluer les conséquences financières d'une pharmacovigilance efficace[564]. Du côté de l'amélioration de la qualité des soins, le document révèle que la contribution de l'accès permanent aux données de santé est « *encore très limitée* »[565]. Tout le raisonnement tend à mettre en lumière les insuffisances de l'accès permanent. Cette méthode, probablement volontaire, vise à favoriser l'amélioration du dispositif en dressant la liste de tous les dysfonctionnements, non recours, et pratiques à consolider. N'oublions pas que le rapport a été rendu dans le cadre de la création du nouveau SNDS. Les observations et recommandations formulées dans ce document avaient pour principal objectif d'aider à trouver un moyen de corriger les défauts détectés.

Cependant, le fait que les résultats et apports de cet accès permanent, après 14 ans d'existence au moment de la publication du rapport, ne soient pas davantage documentés pose nécessairement question. Comment se fait-il qu'un tel mécanisme ait été installé sans qu'une procédure de suivi des usages par les bénéficiaires et sans que des résultats, qu'ils soient à court ou long terme, n'aient été définis et attendus ? A n'en pas douter, organiser cela aurait probablement été ardu, mais se limiter à s'assurer de la sécurité des données accessibles en

[563] V. Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p.65 à 91.

[564] *Ibid.*, p. 84.

[565] *Ibid.*, p. 88.

permanence sans réellement se préoccuper de l'usage, ou plutôt du non usage, de ces données est critiquable.

218. La réforme menée par M. TOURAINE avec la loi de modernisation de notre système de santé[566] a été pensée afin de réviser l'ensemble du système d'accès aux données de santé, incluant l'accès permanent, pour le proposer dans un nouveau cadre destiné à optimiser son utilisation vertueuse.

SECTION 2 : POUR UNE EXPLOITATION AMÉLIORÉE DE L'ACCÈS PERMANENT

219. La refonte du système d'accès aux données de santé par la loi du 26 janvier 2016[567] a pris en compte un certain nombre de remarques et critiques formulées à l'égard de l'accès permanent. Ses imperfections tendent à être corrigées par les nouvelles dispositions en vigueur avec la création d'un cadre destiné à mieux suivre les usages des différents acteurs bénéficiaires (§1). En dépit de toute la bonne volonté du gouvernement à l'origine de la réforme, des zones d'ombre demeurent néanmoins (§2).

Paragraphe 1 : L'amélioration justifiée de l'encadrement de l'accès permanent

220. Le nouveau dispositif d'accès permanent aux données de santé a été entièrement réécrit dans le décret paru le 26 décembre 2016[568]. Ce décret était prévu par le III de l'article L. 1461-3 du code de la santé publique nouvellement créé par la réforme. L'objectif du décret est de « *fixe*[r] *la liste des services de l'Etat, des établissements publics ou des organismes chargés d'une mission de service public autorisés à traiter des données à caractère personnel du système national des données de santé pour les besoins de leurs missions* » et « *précise*[r], *pour chacun de ces services, établissements ou organismes, l'étendue de cette autorisation, les conditions d'accès aux données et celles de la gestion des accès* ». Nous l'avons déjà observé en amont de notre étude[569], le texte du décret crée les articles R. 1461-11 à R. 1461-19 du code

[566] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[567] *Ibidem.*

[568] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

[569] *Supra* n° 114 à 120.

de la santé publique. Il dresse la liste exhaustive des bénéficiaires en précisant, pour chacun d'eux, l'étendue des données auxquelles il peut accéder en permanence.

Le décret va plus loin que ces simples considérations car il répond, en partie seulement[570], aux différentes critiques formulées à l'encontre de l'ancien fonctionnement de l'accès permanent. Dans les développements à suivre, nous nous intéresserons uniquement contenu du décret susmentionné que nous pouvons interpréter comme une réponse aux observations parfois négatives que nous avons évoquées plus tôt.

221. Nous parlions dans le paragraphe précédent de l'instabilité apparente du choix des acteurs bénéficiaires de l'accès permanent. Certains acteurs qui nous semblent importants ont dû attendre quelques années avant d'obtenir leur précieux accès[571] quand d'autres, titulaires de l'accès dès la première année, ne se sont pas beaucoup servi du trésor d'informations qu'ils avaient à leur disposition[572]. Les rédacteurs du décret semblent avoir entendu le message qui leur était adressé. La liste exhaustive des bénéficiaires de l'accès permanent est détaillée et place même la DREES, première utilisatrice, en tête. Les acteurs sont plus variés qu'ils ne l'étaient auparavant avec l'Institut national d'études démographiques, l'Observatoire français des drogues et toxicomanies ou encore l'Institut de radioprotection et de sûreté nucléaire. Le décret a pour ambition de faire oublier les errements constatés depuis 2002 pour repartir sur de meilleures bases et fixer la liste la plus complète possible. Tous les acteurs cités bénéficient, au même moment, de l'accès permanent selon les modalités spécifiques qui les concernent.

Cette façon de remettre tous les bénéficiaires de l'accès permanent sur un même pied d'égalité est louable. Chacun sait à quelles données de santé il peut avoir accès et dans quelles conditions, sans que des considérations de délais d'autorisations ou de parution de textes juridiques supplémentaires ne viennent déséquilibrer le dispositif.

222. Les auteurs de la réforme ont bien assimilé le fait que certains bénéficiaires de l'accès permanent peuvent avoir besoin d'accéder à des données qui ne rentrent pas dans le champ de

[570] *Infra* n° 226 à 228.

[571] A titre d'exemple, les chercheurs de l'Inserm ont attendu l'arrêté de 2005 pour obtenir un accès permanent. Ceux de la Drees ont attendu l'arrêté de 2016 pour être nommément cités pour bénéficier de cet accès. V. *supra* n° 104 à 113.

[572] C'était le cas de certains régimes de sécurité sociale, v. *supra* n° 206 à 212.

l'autorisation qui leur a été attribué. Afin d'optimiser les opportunités offertes aux acteurs investis d'une mission de service public concernés par l'accès permanent, le décret[573] crée donc l'article R. 1461-15 du code de la santé publique. Cet article dispose que si les bénéficiaires de l'accès permanent ont besoin, dans le cadre d'un traitement, d'accéder à des données auxquelles ils n'ont pas accès de manière permanente, ils peuvent soumettre une demande d'autorisation directement à la CNIL dans les conditions prévues par le chapitre IX de la loi relative à l'informatique et aux libertés[574]. Cette procédure est la même que celle par laquelle doivent passer tous les demandeurs qui ne disposent pas d'un accès permanent[575]. Deux enseignements sont à en tirer : en premier lieu, la volonté de promouvoir l'utilisation, la plus large possible, du SNDS par les acteurs publics est mise en avant, cela démontre que les critiques émises au sujet du désintérêt[576] qui ressortait du fonctionnement de l'ancien système d'accès permanent ont été entendues. Deuxièmement, nous pouvons constater que la procédure que doivent suivre les bénéficiaires de l'accès permanent est identique à celle qui doit être suivie par tous les autres demandeurs.

Nous pouvons interpréter cette égalité de traitement comme une réponse des autorités au fait que les acteurs ayant accès en permanence aux données de santé seraient privilégiés ou se verraient accorder une confiance aveugle. Le fait qu'ils soient soumis, pour accéder à des données supplémentaires, à la procédure « *classique* » permettant de vérifier le bien-fondé de l'étude envisagée et la sécurité des fichiers recueillis, démontre que leur activité reste contrôlée et surveillée.

223. La sécurité est aussi très importante quand il s'agit de celle des données de santé. Elle prend d'ailleurs une large place dans le décret relatif au SNDS[577]. Trois articles destinés à prouver le soin qui est apporté pour assurer cette sécurité dans le cadre de l'accès permanent ont alors été créés.

---

[573] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

[574] Loi n° 78-17 du 6 janvier 1978, *op. cit.,* modifiée par la loi n° 2016-41 du 26 janvier 2016, *op. cit*., art. 53 à 61. Ces articles ont été modifiés pour devenir les articles 64 à 77 depuis l'ordonnance n° 2018-1125 du 12 décembre 2018 *prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel*, *JORF*, n° 0288, 13/12/2018.

[575] Cette procédure est détaillée dans la Partie II de l'étude.

[576] *Supra* n° 206 à 212.

[577] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

L'article R. 1461-16 du code de la santé publique précise que chaque bénéficiaire de l'accès permanent habilite, sous sa responsabilité, des personnes nommément désignées pour accéder au SNDS. Ces utilisateurs officiellement autorisés ne peuvent user de leur habilitation que dans le cadre qui est strictement utile au traitement autorisé et prévu. Enfin, ces individus doivent avoir été spécifiquement formés pour accomplir ces missions. Tout cela n'existait pas auparavant : les bénéficiaires de l'accès permanent sont aujourd'hui directement responsabilisés pour maîtriser l'usage qui est fait dudit accès. Cet article a deux objectifs directs : d'abord, il permet d'avoir un suivi strict des individus susceptibles d'accéder aux données du SNDS. Ensuite, il donne une place plus importante aux acteurs qui doivent véritablement s'impliquer dans la gestion et le contrôle de l'accès qui leur a été conféré. C'est un moyen, parmi d'autres, de pousser tous les acteurs figurant sur la liste de l'article R. 1461-12 du code de la santé publique à se mobiliser pour que les données de santé soient mieux exploitées, dans le respect des normes de sécurité, pour améliorer les missions de service public.

L'article R. 1461-17 du même code poursuit la mise en place de nouvelles mesures de sécurité. Chaque acteur doit ainsi désigner un correspondant informatique et liberté (CIL)[578]. Il a pour mission de tenir à jour la liste de tous les traitements, et leurs caractéristiques portant sur les données individuelles du SNDS et mis en œuvre dans le cadre de l'accès permanent. Cette liste est ensuite rendue publique sur le site internet du SNDS tout en étant transmise chaque année au comité stratégique[579] créé par le ministre chargé des affaires sociales et de la santé ainsi qu'à la CNIL. Le modèle de présentation des caractéristiques de traitement a, par ailleurs, fait l'objet de la publication d'un arrêté paru le 15 avril 2017 au Journal officiel[580]. Tout l'intérêt de cette disposition nouvelle, inexistante jusqu'alors, figure dans la transparence de l'action publique qu'elle promeut. Grâce à ces mesures de publicité de la liste des études réalisées grâce à l'accès

[578] Le correspondant à la protection des données, ou correspondant informatique et liberté (CIL) est une fonction qui a été créée par le Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Le CIL est ainsi le référent sur les questions de protection des données personnelles. Il est important de souligner que le Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016, *op. cit.*, a créé la fonction du délégué à la protection des données dont les missions sont similaires à celles du CIL. Le délégué à la protection des données remplace officiellement le CIL depuis le 1er mai 2018.

[579] Ce comité est prévu par l'article R. 1461-10 I du code de la santé publique : il fixe les orientations de développement du SNDS et réunit des représentants des organismes responsables des bases de données alimentant le SNDS, le président de l'IDS et une personnalité qualifiée. L'arrêté ministériel fixant sa composition n'est pas encore paru au moment de l'écriture de ces lignes.

[580] Arrêté du 6 avril 2017 portant fixation du modèle décrivant les caractéristiques des traitements portant sur des données individuelles du système national de santé, JORF n° 0090 du 15/04/2017.

permanent aux données de santé, le sentiment d'opacité qui pouvait être éprouvé jusqu'à la réforme[581] devrait rapidement se dissiper. L'autre apport de cet article est le contrôle des listes de ces études par deux autorités distinctes : bien que l'une d'elle ait une composition et un fonctionnement encore inconnu, cette initiative augure d'une meilleure connaissance des usages qui seront faits par les bénéficiaires de l'accès permanent aux données de santé. L'efficience de cette procédure devra toutefois se vérifier dans la pratique.

Sur la question de la sécurité des données de santé, l'article R. 1461-18 du code de la santé publique contraint les bénéficiaires de l'accès permanent à tenir la liste, à jour, des personnes compétentes en leur sein pour délivrer des accès au SNDS, des personnes qui reçoivent cette habilitation, de l'ensemble du mécanisme interne permettant de contrôler les modalités d'attribution, de gestion et de contrôle desdites habilitations. Cette liste doit aussi être rendue publique sur le site du SNDS et son modèle, établi par le ministère chargé de la santé et de la sécurité sociale, a été publié le 15 avril 2017[582]. L'ambition de cette mesure est la même que celle qui porte la constitution de la liste des études réalisées dans le cadre de l'accès permanent. La tenue d'un document à jour favorise le suivi et la connaissance des individus qui peuvent accéder au SNDS en permanence. Mais ce qui fait la force de cet article du code de la santé publique, ainsi que du précédent, c'est la publication de toutes ces informations. L'action de porter à la connaissance du public les traitements réalisés sur les données, l'identité des individus titulaires d'un accès permanent, et les modalités de gestion et de contrôle de cet accès, constitue un moyen efficace pour créer un lien de confiance entre les citoyens, l'ensemble des acteurs publics ou privés, et les acteurs bénéficiaires de l'accès permanent.

224. Le décret ne s'arrête pas à ces mesures et va plus loin en demandant à chacun des bénéficiaires figurant à l'article R. 1461-12 du code de la santé publique de produire un « *rapport d'évaluation de l'étendue de l'autorisation au regard de ses missions* »[583] dans un délai maximum de trois ans à compter du 1er avril 2017. Cette ultime précision est intéressante. Elle montre que l'accès permanent n'est pas délivré dans une totale indifférence en laissant aux bénéficiaires la tâche de s'en accommoder, quitte à le délaisser comme cela a été le cas par le passé. Ici, les auteurs de la réforme entendent bien suivre sa mise en place en s'assurant que les

[581] *Supra* n° 213 à 218.

[582] Arrêté du 6 avril 2017 portant fixation du modèle décrivant les informations concernant les habilitations à accéder aux données du système national de santé, JORF n° 0090 du 15/04/2017.

[583] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*, art. 2, II.

acteurs disposant de l'accès permanent soient entièrement impliqués dans sa mise en œuvre, son amélioration et son développement. Tous les rapports devraient donc être délivrés à la CNIL avant le 1er avril 2020. Cette ultime mesure est, une fois de plus destinée à responsabiliser les acteurs publics qui peuvent accéder en permanence au SNDS.

225. Les apports de la réforme sur le fonctionnement de l'accès permanent sont finalement de deux ordres : le plus visible est l'encadrement des usages par le renforcement du contrôle et du suivi des accès et des études réalisées, l'autre apport majeur est la publication systématique des documents permettant de connaître les activités réalisées par les acteurs dans le cadre de leur accès permanent. Nul doute que cette nouvelle course à la transparence de l'action publique concourra à la satisfaction des personnes les plus critiques à l'égard du modèle de ce type d'accès. Plusieurs sujets ont toutefois été mis de côté par la réforme.

Paragraphe 2 : Les lacunes de la réforme de l'accès permanent

226. La refonte du système de mise à disposition permanente des données de santé à des acteurs présélectionnés sert, nous l'avons vu[584], à renouer la confiance avec les citoyens en créant un dispositif permettant à tous de savoir qui peut avoir accès aux données, à quelles fins et sous quelles conditions de sécurité. Mais quelques éléments critiquables de l'accès permanent, tel qu'il existe depuis le premier arrêté du 11 avril 2002[585], n'ont pas été clarifiés : les auteurs du décret du 26 décembre 2016[586] donnent l'impression fâcheuse de s'être contentés de répondre aux questions, certes primordiales, directement liées à la sûreté et à l'utilisation des données, alors que certaines considérations, toutes aussi importantes, ont été mises de côté.

227. Le premier sujet, grand absent de la réforme, est celui de la procédure de sélection des bénéficiaires de l'accès permanent. Ce point, que nous pensons être très important pour asseoir la légitimité de tout le dispositif, est parfaitement introuvable à travers les textes publiés dans le cadre de la réforme du SNDS. Nous en avons pourtant étudié la problématique[587] : le fait de ne pas pouvoir connaître les modalités de choix des acteurs qui peuvent obtenir leur précieux

[584] *Supra* n° 220 à 225.

[585] Arrêté du 11 avril 2002, *op. cit*.

[586] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

[587] *Supra* n° 178 à 184.

accès permanent aux données de santé impacte directement la perception que les autres acteurs, et les citoyens, ont de ce mécanisme.

La réforme représentait une occasion idéale de clarifier l'intégralité du processus afin de savoir qui sont les décideurs, quels sont les critères de sélection et comment la liste finale des bénéficiaires de l'accès permanent est fixée. Jusqu'à aujourd'hui, l'un des seuls documents accessibles était une maigre publication[588] de l'Institut des données de santé (devenu Institut national des données de santé dans le nouveau système) faisant référence uniquement à l'organisation mise en œuvre à l'issue du projet de loi de financement de la sécurité sociale pour 1999[589]. Ce texte désigne le COPIIR comme l'organe chargé de définir « *les organismes pouvant utiliser les données du SNIIRAM, et quelles données ils peuvent utiliser* ». Pourtant, la Cour des comptes rappelle[590] que cette mission ne fait plus partie des attributions du COPIIR depuis 2008, la gestion des accès étant uniquement fixée par le biais des arrêtés. Dans le même temps, la Cour souligne « *l'indétermination de la procédure d'instruction des droits d'accès permanents* » qui, de notre point de vue, est préjudiciable à la compréhension et à l'acceptation du système d'accès permanent. Nous en revenons à l'idée que les acteurs sont sélectionnés après un cheminement opaque et hasardeux[591] que les décisionnaires eux-mêmes ne semblent pas maîtriser. Nous sommes en face d'un vide juridique que seule la réforme aurait pu combler. Malheureusement, le décret relatif à l'accès permanent[592] ne propose aucun détail sur les modalités de choix des acteurs et il est étonnant de constater que rien n'a été publié, sur le site du SNDS ou de la DREES par exemple, sur le sujet par ailleurs.

Le manque de pédagogie des auteurs de la réforme ne peut être qu'à déplorer. Nous ne pouvons que nous demander pourquoi un document officiel détaillant les modalités de sélection des bénéficiaires de l'accès permanent n'a pas été publié alors que, dans le même temps, la transparence semble être le mot d'ordre à propos de la sécurité des données ou des usages qui en sont faits. Ce sujet sensible est pourtant l'un des points clefs qui, s'il était expliqué publiquement, ôterait tous les doutes susceptibles de persister chez les détracteurs de l'accès

[588] Loi n° 98-1194 du 23 décembre 1998 *de financement de la sécurité sociale pour 1999, op. cit.*

[589] Institut des données de santé, « Processus d'élaboration de l'arrêté permettant l'utilisation des données anonymisées de l'assurance maladie obligatoire ».

[590] V. Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p.54.

[591] *Supra* n° 178 à 184.

[592] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

permanent qui dénoncent notamment un fonctionnement trop méconnu. Peut-être que les prochaines années seront l'occasion pour les pouvoirs publics de travailler à proposer un règlement de sélection des bénéficiaires de l'accès permanent qui soit consultable par tous. Il n'en demeure pas moins que le décret du 26 décembre 2016[593] peut être perçu comme une occasion manquée de faire toute la lumière sur l'intégralité du dispositif. La parution, le 1er décembre 2018, d'un décret[594] complétant la liste initiale des bénéficiaires de l'accès permanent n'a malheureusement pas apporté plus d'éléments de réponse sur ce sujet.

228. Le second sujet qui aurait pu, dans une moindre mesure, apporter une réponse à certaines critiques émises dans la section précédente[595], est celui des objectifs et résultats attendus. Nous ne parlons pas nécessairement de la préparation d'une liste exhaustive d'améliorations chiffrées à atteindre qui serait attribuée à chaque acteur, mais de la présentation de l'esprit de chaque accès permanent délivré. Cette question est traitée en partie par l'obligation fixée par le II de l'article 2 du décret[596] qui impose à chaque bénéficiaire de délivrer un rapport d'évaluation, avant le 1er avril 2020, relatif à l'étendue de l'autorisation au regard de ses missions. Il s'agit d'un premier pas vers le suivi des besoins et utilisations des données de santé qui sont propres à chaque acteur. Ce premier pas aurait pourtant gagné à être complété par un rappel de ce qui est attendu de la mise en œuvre de l'accès permanent au bénéfice de certains acteurs ayant une mission de service public : l'amélioration aussi bien qualitative que quantitative de ces missions, couplée à une optimisation des coûts potentiellement générés lorsque l'accès permanent n'était pas mis en œuvre. Il n'aurait pas été inutile de proposer ce rappel pour indiquer, aussi bien à l'ensemble des français, qu'aux bénéficiaires de l'accès permanent, la voie à suivre. Bien entendu, il revient à chacun des acteurs de déterminer, en leur sein, qui peut accéder aux données de santé, comment en tirer le meilleur parti et à quelle fin les utiliser. Mais nous ne pouvons que regretter que les auteurs du décret n'aient pas fixé un cap général plus appuyé à suivre.

---

[593] *Ibid.*

[594] Décret n° 2018-1056 du 29 novembre 2018 *complétant le décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »*, JORF, n° 0278, 01/12/2018.

[595] *Supra* n° 206 à 218.

[596] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

Si nous nous reportons au rapport de la Cour des comptes[597], nous savons que beaucoup de bénéficiaires[598] de l'accès permanent ont un travail très important à fournir pour rattraper leur retard dans la maîtrise des données de santé et dans leur exploitation. La seule obligation de fournir un rapport, avant une date donnée, sur les opportunités offertes par l'accès aux données de santé dans le cadre de leur mission de service public n'est pas de nature à pousser ces acteurs à utiliser davantage leur accès permanent.

La réforme de l'accès permanent reste donc à parachever s'agissant de l'incitation des acteurs à favoriser un usage vertueux de l'opportunité qui leur est donnée de traiter des données de santé particulièrement protégées. Malgré les quelques oublis de la réforme que nous venons d'évoquer, celle-ci a pour principale qualité d'éclaircir de nombreux points qui faisaient, jusqu'alors, l'objet de nombreuses critiques : les personnels sont mieux formés et sensibilisés aux questions inhérentes à la protection de la vie privée, tout citoyen peut désormais savoir qui sont les responsables des traitements de données de santé au sein des structures ayant un accès permanent, à quelles données ils accèdent, comment ils les traitent, et pour quelle finalité. Le fait que les documents déclaratifs soient destinés à être rendus publics permet de rétablir un lien de confiance et de s'assurer que les règles de sécurité entourant les traitements de données soient respectées.

[597] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*

[598] Nous pouvons notamment citer les régimes de sécurité sociale autres que le régime général, les ministères et les ARS, *supra* n° 206 à 212 et *ibid.* p. 74 à 90.

CONCLUSION DU CHAPITRE II

229. Le diagnostic opéré par la Cour des comptes[599] en vue de la réforme de l'accès aux données de santé des bases médico-administratives est salutaire. Le document permet de poser, pour la première fois, une analyse objective du fonctionnement de l'accès permanent. Le constat appelle indéniablement à une réforme qui implique un suivi et une maîtrise des traitements effectués dans le cadre de l'accès permanent. Le document révèle effectivement que l'accès permanent a été sous-utilisé par ses bénéficiaires, y compris par la CNAMTS, malgré le potentiel identifié d'amélioration des missions de service public. Cette sous-exploitation implique que ces acteurs n'ont pas su développer leur maîtrise des données de santé. De plus, le contenu du rapport souligne le manque d'indicateurs de suivi des usages de l'accès permanent : les indicateurs les plus fournis sont ceux qui concernent l'insuffisance d'utilisation des données pour des missions qui auraient pourtant dû en bénéficier.

230. La réforme du 26 janvier 2016[600] a été préparée en parallèle de la rédaction de ce rapport de la Cour des comptes[601] et répond, en partie, aux critiques qui s'y trouvent. Le nouvel accès permanent existe pour être utilisé et véritablement mis à profit par ses bénéficiaires pour l'amélioration de leurs missions. Cette ouverture n'est pas dénuée de garanties concernant la sécurité des données avec la mise en œuvre d'un suivi officiel des accès réalisés et des traitements effectués. Signalons malgré tout l'absence de visibilité sur les attentes de la réforme : aucun objectif chiffré n'a été fixé. Cela aurait pourtant été une solution pour encourager les bénéficiaires de l'accès permanent à développer leur expertise dans l'obtention et le traitement des données de santé.

[599] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit*

[600] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[601] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit*

CONCLUSION DU TITRE II

231. Le dispositif d'accès permanent aux données de santé a dû attendre quinze années avant de vraiment faire l'objet d'une réforme structurante et bénéfique pour son bon fonctionnement. Les utilisations, trop variables et dispersées d'un acteur à l'autre, n'ont été suivies que tardivement. Il en va de même pour le mécanisme de choix des acteurs pouvant se voir attribuer un accès. Ce sont ces dysfonctionnements constatés dans un système qui a peut-être été mis en place trop tôt et trop rapidement, qui ont conduit les autorités françaises à le redéfinir. La protection de la vie privée est au cœur de cette réforme avec le contrôle étroit de tout le personnel susceptible d'accéder aux données de santé. La publicité et la communication envisagées sont aussi un signe fort de la volonté de proposer un accès permanent qui soit maîtrisé et connu de tous. Mais certaines inconnues demeurent, comme la procédure de sélection des bénéficiaires, et ne devraient pas manquer d'être rappelées par les éventuels opposants à l'accès permanent.

232. La réforme proposée par la loi de modernisation de notre système de santé apporte toutefois un nouveau souffle, accompagné de ses quelques imperfections, lequel devrait, vraisemblablement, permettre aux bénéficiaires de l'accès permanent aux données de santé d'en tirer le meilleur parti. N'oublions pas que c'est à des fins de protection de la vie privée que cet accès réservé à certains acteurs existe : c'est d'ailleurs pour cette raison qu'il contient des mesures strictes de suivi des différents traitements réalisés. Un autre système, davantage contrôlé et sévère dans sa mise en œuvre, permet aussi aux nombreux exclus de l'accès permanent d'avoir accès à des données de santé sur demande, à condition que cela ne puisse pas porter atteinte à cette protection de la vie privée. Cette procédure d'autorisation préalable peut être présentée comme la procédure commune d'accès aux données de santé : elle a également fait l'objet de nombreuses modifications depuis sa création et sa mise en œuvre a parfois été difficile. Cela d'ailleurs fait l'objet du prochain chapitre de cette étude.

CONCLUSION DE LA PARTIE I

233. L'accès permanent aux données de santé est, pour des raisons de sécurité liées à la protection de la vie privée, très encadré par les textes depuis sa création[602]. Il conserve encore aujourd'hui son caractère exclusif que le premier arrêté relatif à la mise en œuvre du SNIIRAM[603] lui a conféré. Cet accès reste ainsi réservé à des acteurs spécifiquement autorisés par arrêté ou par décret dans un objectif d'intérêt général[604]. Cette notion d'intérêt général imprègne le mécanisme d'accès permanent depuis sa création avec trois finalités[605] : l'amélioration de la qualité des soins ; la contribution à une meilleure gestion de l'assurance maladie ; la transmission aux prestataires de soins des informations pertinentes relatives à leur activité, à leurs recettes et, s'il y a lieu, à leurs prescriptions. Aujourd'hui, cet accès permanent répond à six finalités précisées par décret[606] : l'information sur la santé et notamment l'offre de soins ; 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 de l'assurance maladie et des dépenses médicosociales ; l'information des professionnels de santé, des structures et des établissements de santé ou médico-sociaux sur leur activité ; la surveillance, la veille et la sécurité sanitaires ; et la recherche, les études, l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale.

234. Pour limiter, *de facto*, l'étendue de l'accès permanent, il a été décidé de le réserver aux acteurs participant à l'organisation du service public. Le nombre réduit de bénéficiaires permet en principe de maîtriser plus facilement les usages et de détecter rapidement les éventuelles dérives pouvant violer le droit au respect de la vie privée des individus. Les textes se sont donc efforcés de dresser une liste exhaustive des bénéficiaires de l'accès permanent en prévoyant, pour chacun d'eux, le type de données qu'ils peuvent exploiter. Mais l'instabilité de ces textes

[602] Arrêté du 11 avril 2002, *op. cit.*

[603] *Ibid.*

[604] La notion d'utilisation des données de santé est évoquée dès 1998 dans BRAIBANT G., Données personnelles et société de l'information : transposition en droit français de la directive n° 95-46 / rapport au Premier Ministre, *op. cit.*

[605] Arrêté du 11 avril 2002, *op. cit.*, v. *supra* n° 104.

[606] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*, v. *supra* n° 172.

au fil des années[607], est le signe d'une désorganisation manifeste du dispositif. Cela n'a pas empêché l'accès permanent aux données de santé d'être élargi à un nombre croissant d'acteurs pour atteindre une liste de vingt-cinq catégories différentes aujourd'hui[608]. Cette ouverture à de nouveaux bénéficiaires s'est déroulée sur plusieurs années afin de penser, dans le même temps, à la meilleure sécurisation des données de santé qui est au cœur de l'accès permanent. La réforme mettant en œuvre le nouveau SNDS[609] a par ailleurs été préparée dans ce sens.

235. Ce que nous pourrions qualifier de « point faible » du mécanisme de l'accès permanent aux données de santé consiste dans l'absence de contrôle de son bon fonctionnement. Depuis 2002, un seul rapport complet sur l'utilisation de l'accès permanent a été réalisé et il date de 2016[610]. Dès lors, la légitimité de l'accès permanent peut être remise en cause car il est supposé améliorer le fonctionnement du service public. Mais l'absence de dispositif permettant de mesurer son impact concret sur les missions des différents bénéficiaires va à l'encontre de l'objectif fixé.

236. La réforme proposée le 26 janvier 2016[611] est, à ce titre, bienvenue. Elle a permis de faire un bilan de l'accès permanent aux données de santé et de proposer une actualisation qui s'avérait nécessaire. La liste des acteurs disposant de l'accès permanent est désormais clairement connue, les mesures de sécurité sont nettement exposées, avec notamment un contrôle individualisé et une publication prévue des personnes disposant de l'accès permanent[612]. Des imperfections demeurent toutefois car les modalités précises de sélection des bénéficiaires de l'accès permanent aux données de santé restent inconnues.

237. L'accès permanent n'est finalement qu'un type très particulier d'accès aux données de santé. Le second type d'accès, qui est le plus important, est l'accès ponctuel, aussi appelé accès sélectif, dont peuvent bénéficier de nombreux acteurs exclus de l'accès permanent. Il s'effectue après l'obtention d'une autorisation préalable et doit répondre à de nombreux prérequis afin de

[607] Nous pouvons compter sept arrêtés relatifs au SNIIRAM modifiant significativement la liste des bénéficiaires entre 2002 et 2016. V. *supra* n° 105.

[608] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*., v. *supra* n° 116.

[609] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[610] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*

[611] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[612] *Supra* n° 220 à 225.

s’assurer que le respect de la vie privée des individus à l’origine des données ne soit, à aucun moment, en péril.

PARTIE II

LA TRANSPARENCE SÉLECTIVE DES DONNÉES DE SANTÉ AU BÉNÉFICE DES ACTEURS PUBLICS ORDINAIRES ET PRIVÉS À BUT NON LUCRATIF

238. La mise en place d'un système d'information destiné à recueillir des milliards de données de santé[613] place nécessairement la problématique de la protection de la vie privée au cœur de la réflexion. La combinaison des questions juridiques aux considérations techniques et pratiques n'a pas rendu la tâche du législateur aisée. Il fallait réussir à permettre un accès aux données de santé à des fins de recherche, d'analyse des activités de soins et de prévention[614] tout en garantissant l'inviolabilité du droit au respect de la vie privée des individus. Or, les connaissances techniques relatives aux systèmes informatiques étaient, et sont encore dans une moindre mesure, en pleine évolution. La difficulté à appréhender l'intégralité du faisceau d'enjeux planant sur l'accès aux données de santé contenues dans le SNIIRAM était bien réelle au moment de sa mise en œuvre[615].

239. La base de données de santé SNIIRAM n'est devenue opérationnelle qu'après la création de deux finalités autorisant l'accès sélectif : l'accès à des fins de recherche dans le domaine de la santé, et l'accès à des fins d'évaluation ou d'analyse des activités de soins et de prévention. Dès lors, les acteurs potentiellement bénéficiaires de l'accès sélectif aux données de santé étaient tous les acteurs exclus du mécanisme de l'accès permanent. La situation n'était pourtant pas aussi simple et le premier arrêté[616] relatif à la mise en œuvre du SNIIRAM a immédiatement

[613] Comme nous l'avons déjà vu, *supra* n° 93, d'après P.-L. BRAS, le SNIIRAM contient *a minima* perpétuellement les informations provenant d'1,2 milliard de feuilles de soins, de 500 millions d'actes médicaux, ou encore de 11 millions de séjours hospitaliers. V. BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.*, p. 21.

[614] Dès la loi n° 94-548 du 1 juillet 1994 *relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, JORF n° 152, 02/07/1994, le traitement de données de santé a été rendu possible sous certaines conditions.

[615] Rappelons que le SNIIRAM a été créé par la loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale pour 1999, *op. cit*.

[616] Arrêté du 11 avril 2002, *op. cit*.

prévu des exceptions à cet accès sélectif. Ainsi, les acteurs historiquement bénéficiaires de l'accès sélectif sont, d'une part, tous les acteurs publics qui sont exclus de l'accès permanent, que nous pouvons nommer acteurs publics ordinaires, et, d'autre part, les acteurs privés à but non lucratif. La situation des acteurs privés à but lucratif, longtemps mis à l'écart de l'accès sélectif[617], est plus complexe et sera l'objet de notre prochaine partie.

240. En amont de la définition des acteurs bénéficiaires de l'accès sélectif et de leurs conditions d'accès, G. BRAIBANT est parvenu à rassembler dans son rapport[618] les préoccupations qui entouraient la création de la nouvelle base de données de santé de l'assurance maladie française. Il avait ainsi détecté les risques liés au recueil et au traitement systématique des informations relatives aux individus tout en reconnaissant le potentiel bénéfique des traitements. La condition posée d'emblée pour que les traitements des données personnelles soient acceptés et acceptables est donc qu'ils demeurent limités à leur finalité initiale. Par une simple phrase, l'auteur établit le rapport ambigu qui existe entre d'une part la tentation de traiter des données de façon industrialisée, sans limites, et d'autre part le respect de la vie privée : « *les bénéfices, directs ou indirects, de ces traitements sont incontestables, dès lors qu'ils restent dans le cadre de finalités expressément définies* »[619]. Il recensait alors seulement trois finalités s'agissant du traitement des données de santé[620] : la santé, la recherche et l'assurance maladie. Nous savons aujourd'hui que le traitement des données de santé peut avoir des finalités plus précises qui ont été autorisées à travers les lois successives[621].

241. Le législateur n'a pas attendu la mise en œuvre du SNIIRAM[622] pour édifier l'encadrement de l'accès aux données de santé. Dès 1994[623], un mécanisme de demande d'accès aux données

[617] Les acteurs privés à but lucratif sont légalement admis à solliciter un accès aux données de santé du SNDS (incluant le SNIIRAM) depuis l'entrée en vigueur de la loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[618] BRAIBANT G., Données personnelles et société de l'information : transposition en droit français de la directive n° 95-46, rapport au Premier Ministre, *op. cit.*

[619] *Ibid.* p. 6.

[620] *Supra* n° 95.

[621] *Infra* n° 273 à 282.

[622] Le SNIIRAM a été mis en œuvre par l'arrêté du 11 avril 2002 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, *op. cit.*

[623] Loi n° 94-548 du 1 juillet 1994 *op. cit.*

de santé a été inséré au cœur de la loi relative à l'informatique et aux libertés[624]. Ce premier pas vers l'utilisation des données de santé était alors retranscrit au chapitre V-bis de la loi relative à l'informatique et aux libertés[625]. Le traitement des données était alors limité à des finalités de recherche dans le domaine de la santé. Signalons toutefois que le chapitre était alors nommé « *Traitements automatisés de données nominatives ayant pour fin la recherche dans le domaine de la santé* ». Nous reviendrons ultérieurement[626] sur l'utilisation des termes « *données nominatives* » dont le traitement éventuel est, *de facto*, en totale opposition avec le respect de la vie privée des individus. La modification intervenue en 1994 marque aussi l'acte fondateur de l'un des acteurs essentiels du dispositif de demande d'accès aux données de santé : le comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé, ou CCTIRS[627], remplacé en 2016 par le comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé, ou CEREES[628]. Ce dernier est appelé à devenir le comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé, ou CESREES, lorsque le projet de loi relatif à l'organisation et à la transformation du système de santé sera appliqué[629]. Ce comité avait pour mission d'évaluer les demandes d'accès aux données de santé déposés dans le cadre de recherches, préalablement à leur examen par la CNIL.

242. Par la suite, avant la mise en place du SNIIRAM, de nouvelles finalités permettant l'accès aux données de santé et leur traitement ont été introduites par le législateur. Il s'agit des finalités d'évaluation ou d'analyse des activités de soins et de prévention qui ont été intégrées au chapitre V-ter de la loi relative à l'informatique et aux libertés[630]. On ne le sait que trop peu,

---

[624] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[625] *Ibid.* dans sa version modifiée par la loi n° 94-548 du 1 juillet 1994 *op. cit.*

[626] *Infra* n° 273.

[627] Le CCTIRS avait pour mission d'émettre un avis sur la méthodologie de la recherche au regard des dispositions de la loi relative à l'informatique et aux libertés, la nécessité du recours à des données nominatives et la pertinence de celles-ci par rapport à l'objectif de la recherche, préalablement à la saisine de la Commission nationale de l'informatique et des libertés. La loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *op. cit*., l'a remplacé par le CEREES.

[628] Le CEREES a été créé par la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *op. cit.*, et remplace le CCTIRS. Il a pour mission de rendre « *un avis sur la méthodologie retenue, sur la nécessité du recours à des données à caractère personnel, sur la pertinence de celles-ci par rapport à la finalité du traitement et, s'il y a lieu, sur la qualité scientifique du projet* ».

[629] Projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019.

[630] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

c'est par l'article 41 de la loi portant création d'une couverture maladie universelle[631] que ces nouveaux objectifs de traitement des données de santé ont vu le jour. Nous pourrions d'ailleurs nous interroger sur la légitimité d'une telle disposition dans un texte de loi portant sur la création d'une couverture maladie. Il s'agissait probablement d'une mesure d'opportunité car le titre V de ladite loi est entièrement dédié à la « *modernisation sanitaire et sociale* » et contient d'autres dispositions qui n'ont aucun lien direct avec le sujet principal de la couverture maladie universelle.

243. L'ensemble des mesures prévues par le législateur pour garantir le respect de la vie privée dans le cadre du traitement des données de santé s'est ainsi développé à partir de l'année 1994[632] et cette situation s'est prolongée sans grand bouleversement jusqu'à la réforme du 26 janvier 2016[633]. Cette dernière a permis de réaliser un audit complet du système d'accès aux données de santé du SNIIRAM en évaluant, point par point, l'efficience du dispositif. Les différents rapports, études et réflexions[634] parus sur ce sujet épineux ont mis en exergue aussi bien les éléments essentiels et fonctionnels de l'accès sélectif, que ses lacunes et dysfonctionnements. L'objectif de la réforme est ainsi de parvenir à concilier le besoin d'accéder, de façon claire et rapide, à des données de santé avec l'obligation de tout mettre en œuvre pour que l'usage desdites données ne présente aucun risque d'atteinte à la vie privée.

244. Il nous semble donc primordial de dresser une analyse juridique et pratique du mécanisme d'accès sélectif aux données de santé depuis sa création en 1994[635], jusqu'à sa nouvelle mouture

---

[631] Loi n° 99-641 du 27 juillet 1999 *portant création d'une couverture maladie universelle*, JORF n° 0172 du 28/07/1999.

[632] Loi n° 94-548 du 1 juillet 1994, *op. cit.*, qui a créé les premières modalités d'accès sur autorisation à des fins de recherche dans le domaine de la santé.

[633] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[634] Nous pouvons citer notamment : BOSSI J., « Comment organiser aujourd'hui en France la protection des données de santé », *op. cit.* ; BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.* ; BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé*, *op. cit.* ; DEBOST C., « Quand les traitements de données relatives à l'état de santé sont légitimes par les plus hautes institutions françaises », *RDS*, 2015, n° 63, p. 128-129 ; DUCROS D., NICOULES V., CHEHOUD H., BAYLE A., SOUCHE A., TANGUY M., VALIERE J.-P., CAYLA F., GROSCLAUDE P., « Les bases médico-administratives pour mesurer les inégalités sociales en santé », *op. cit.* ; GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *Pour une meilleure utilisation des bases de données administratives et médico-administratives nationales pour la santé publique et la recherche*, *op. cit.* ; GORCE G. et PILLET F., Rapport d'information au Sénat, *La protection des données personnelles dans l'open data : une exigence et une opportunité*, *op. cit.* ; LAUDE A., « De quelques problématiques relatives à l'ouverture des bases de données en santé », *op. cit.* ; PECHILLON E., « L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ? », *op. cit.*

[635] Loi n° 94-548 du 1 juillet 1994, *op. cit.*

issue de la loi du 26 janvier 2016[636] en mettant en lumière l'équilibre, ou le déséquilibre, entre la possibilité d'accéder aux données et la protection de la vie privée, ainsi que les influences du droit communautaire et européen sur chacune des évolutions constatées (Titre I). Puis nous proposerons une analyse des imperfections de l'accès sélectif aux données de santé qui ont conduit à la création du nouveau SNDS que nous connaissons aujourd'hui (Titre II).

[636] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

TITRE I

L'ACCÈS SÉLECTIF AUX DONNÉES DE SANTÉ JUSTIFIÉ PAR LA PROTECTION DE LA VIE PRIVÉE

245. L'ambition qui imprègne la création du SNIIRAM, dès 1998[637], est de permettre aux données de santé d'être mises à disposition afin d'être utilisées pour améliorer la qualité des soins, contribuer à une meilleure gestion de l'assurance maladie ou encore favoriser une meilleure communication avec les prestataires de soins[638]. La priorité a, toutefois, été donnée à la mise en place d'un premier accès permanent à ces données, réservé à des acteurs désignés par arrêté, et participant à une mission de service public[639]. En effet, il est nécessaire de rappeler que, depuis sa création, la base de données de santé SNIIRAM est gouvernée par un principe fondamental : les données de santé qui y sont conservées sont inaccessibles. *A contrario*, l'accès à ces données reste l'exception. Ce prédicat est compréhensible étant donné la sensibilité des informations proposées[640] et le risque avéré ou potentiel pour la protection de la vie privée. Pourtant, ce n'est pas avant la loi du 6 août 2004[641], transposant la directive 95/46/CE[642], que la loi relative à l'informatique et les libertés[643] est venue poser sans ambiguïté l'interdiction de principe de collecter et traiter les données à caractère personnel de santé[644]. Avant cela, la protection des données personnelles de santé semblait reposer sur l'application implicite de

[637] Loi n° 98-1194 du 23 décembre 1998 *de financement de la sécurité sociale pour 1999, op. cit.*

[638] Ces objectifs sont les premiers à être fixés par l'arrêté du 11 avril 2002, *op. cit.*

[639] V. Partie I, Titre I.

[640] *Supra* n° 27 à 39.

[641] 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.*

[642] Directive 95/46/CE 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*.

[643] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, art. 8 dans sa version modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit*.

[644] Signalons le retard de transposition de la directive 95/46/CE dans le droit français lorsque l'on sait que des Etats voisins, comme la Belgique, l'ont transposée dès 1999. V. de BROUWER F., « Protection des données à caractère personnel : un nouveau cadre légal belge », *Revue de droit des affaires internationales*, 01/03/1999, p. 181-206.

ladite directive[645]. Aujourd'hui encore, l'interdiction de principe est en vigueur[646] et inscrite à l'article 6 de la loi relative à l'informatique et aux libertés[647].

246. Aux débuts du système d'accès aux données de l'assurance maladie, le seul moyen offert aux acteurs non concernés par l'accès permanent pour accéder aux données de santé du SNIIRAM était de déposer une demande d'autorisation auprès de la CNIL[648] selon des modalités prévues par la loi relative à l'informatique et aux libertés[649]. Désormais, ces demandes sont régies par la section 3 du chapitre III du Titre 2 de ladite loi[650]. Toute la procédure d'autorisation préalable au traitement de données personnelles de santé a, comme nous le verrons ultérieurement[651], peu évolué jusqu'à la réforme du 26 janvier 2016[652]. L'intérêt de l'encadrement strict de l'accès sur demande aux données est le suivant : cela permet aux autorités compétentes de vérifier la conformité des traitements envisagés avec la législation en vigueur afin de garantir qu'ils ne mettront pas en péril la protection de la vie privée des individus. C'est l'essence même de ce mécanisme qui nous amène à identifier cette procédure comme étant un accès sélectif.

247. L'accès sélectif aux données de santé demeure le seul moyen, depuis le premier arrêté relatif à la mise en œuvre du SNIIRAM[653], pour les non-bénéficiaires de l'accès permanent, d'accéder à des données de santé en vue d'un traitement. Si sa forme a évolué au fil des années, son fonctionnement est longtemps resté le même et a fait couler beaucoup d'encre[654] : c'est la

---

[645] *Ibid.*

[646] Supra n° 60.

[647] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, art. 6 modifié par l'ordonnance n° 2018-1125 du 12 décembre 2018 *prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel*, JORF, n° 0288, 13/12/2018.

[648] L'arrêté du 11 avril 2002, *op. cit.*, indique que « *toute autre demande d'accès à des données individuelles relatives aux bénéficiaires devra faire l'objet d'une demande d'autorisation auprès de la CNIL dans les conditions prévues aux articles 40-11 à 40-15 de la loi du 6 janvier 1978 susvisée* ».

[649] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[650] *Ibid.*, articles 64 à 77.

[651] *Infra* n° 302 à 310.

[652] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[653] Arrêté du 11 avril 2002, *op. cit.*

[654] V. notamment BRECHAT P.-H., BRIOT P., FOURY C., TEIL A., BRECHAT N., « Remporter les défis des systèmes de santé et d'Assurance maladie au XXIe siècle : l'expérience de la France et de l'Utah des Etats-Unis d'Amérique », *Journal de droit de la santé*, 01/01/2014, p. 19-30 ; CASTETS-RENARD C., « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data », Revue Lamy de Droit

raison pour laquelle la loi de modernisation de notre système de santé[655] est venue proposer une mise-à-jour dont nous analyserons les impacts potentiels ultérieurement[656].

248. Le présent chapitre représente l'opportunité de revenir sur les fondements de l'accès sélectif aux données de santé et sur le fonctionnement d'un mécanisme destiné à assurer la protection de la vie privée (Chapitre 2). Mais avant d'aborder ce point, il apparaît primordial de connaître l'identité des bénéficiaires de cet accès sélectif, qui sont nombreux à vouloir obtenir une autorisation d'accès et de traitement, ainsi que les dispositions prises à leur égard (Chapitre 1).

de l'Immatériel, 01/10/2014, supplément au n° 108, p. 38-45 ; DEBOST C., « Publication du rapport sur la gouvernance et l'utilisation des données de santé, la promesse d'un entrebâillement de l'Open data dans le secteur de la santé ? », *RDS*, janvier 2014, n° 57, p. 947 à 949 ; DESMARAIS P., « Open data santé, un rapport décevant pour un retard de transposition certain ? », *JCP A*, 08/09/2014, n° 36, 716 ; DESMARAIS P., « La réforme de l'open data suppose une approche globale ! », *JCP G*, 05/05/2014, n° 18, 528 ; ENCINAS de MUNAGORRI R., « Santé et nouvelles technologies en Europe, synthèse et perspectives. Quelles recompositions du droit pour le XXIe siècle ? », *Revue Lamy droit de l'immatériel*, 01/12/2014, n° 110, p. 40-42 ; JOB J.-M., « La loi "Informatique et libertés" et les données de santé », *Revue Lamy droit de l'immatériel*, 01/01/2008, n° 34, p. 86-94 ; KHODOSS H., « L'exploitation des données de santé », *RGDM*, 30/09/2004, n° 4, p. 65-76 ; de LAMBERTERIE I., « Protection de la vie privée et traitement des données relatives à la santé à l'heure européenne », *Médecine et droit*, 01/09/1996, n° 20, p. 6-12 ; LAVERDET C., « Données personnelles : bilan de 1995 et réforme de 2014 ? », *Revue Lamy du Droit de l'immatériel*, 01/05/2014, n° 104, p. 96 à 99 ; PECHILLON E., « L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ? », *L'information psychiatrique*, 8/2015, volume 91, p. 645-649 **;** RICHARD J., « Le numérique et les données personnelles : quels risques, quelles potentialités ? », *RDP*, 01/01/2016, n° 1, p. 87-100 ; SAOUT C., « La crise de confiance dans le système de santé », *Les Tribunes de la santé*, 1/2009, n° 22, p. 119-132 ; SAURET J., « Economie des nouveaux systèmes d'information en santé », *Les Tribunes de la santé*, 2010/4, n° 29, p. 59-68 ; TABUTEAU D., « Le secret médical et l'évolution du système de santé », *D.*, 12/11/2009, n° 39, p. 2629-2633.

[655] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[656] *Infra* n° 393 à 440.

CHAPITRE I
L'ACCÈS SÉLECTIF OUVERT À DES ACTEURS STRICTEMENT CONTRÔLÉS

249. Eu égard à la nature hautement sensible[657] des données rendues accessibles dans le cadre de l'accès sélectif, le législateur a prévu, dès la fondation du SNIIRAM, un véritable arsenal juridique permettant de savoir qui peut demander et obtenir un accès (Section 1), mais surtout, comment cet accès est contrôlé *a posteriori* afin d'éviter que des dérives se produisent (Section 2).

SECTION 1 : L'OUVERTURE DÉLIMITÉE DE L'ACCÈS SÉLECTIF

250. Pour accompagner l'existence de l'accès permanent ouvert à certains acteurs[658], le pouvoir réglementaire s'est permis d'ajouter, en quelques mots seulement[659], l'accès sélectif soumis à autorisation préalable. Cette nouvelle possibilité d'obtenir des données personnelles de santé avait, dès sa création, un champ d'application très vaste (§1), nécessitant la création de normes destinées à assurer le respect des règles relatives à la protection de la vie privée (§2).

Paragraphe 1 : Les bénéficiaires variés de l'accès sélectif

251. En France, deux lois majeures sont à l'origine de l'accès sélectif aux données de l'assurance maladie. La première est la loi de financement de la sécurité sociale pour 1999[660] qui a créé le SNIIRAM, regroupant toutes les données de soins de ville puis, au sens large, toutes les données de soins hospitaliers. La seconde est la loi portant création d'une couverture maladie universelle[661] qui a inséré dans la loi relative à l'informatique et aux libertés[662] les dispositions permettant un accès, sur autorisation préalable, aux données contenues dans le SNIIRAM. C'est ainsi que le chapitre V ter de ladite loi, intitulé « *traitement de données*

[657] *Supra* n° 60.

[658] V. Partie I.

[659] L'arrêté du 11 avril 2002, *op. cit.*, dispose que « toute autre demande d'accès à des données individuelles relatives aux bénéficiaires devra faire l'objet d'une demande d'autorisation auprès de la CNIL ».

[660] Loi n° 98-1194 du 23 décembre 1998, *op. cit.*

[661] Loi n° 99-641 du 27 juillet 1999, *op. cit.*

[662] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

personnelles de santé à des fins d'évaluation ou d'analyse des activités de soins et de prévention », est né. Nous ne pouvons nous empêcher de remarquer que ces nouvelles opportunités de traitement des données personnelles de santé en France sont apparues dans les délais de transposition de la directive de 1995[663] alors même que la loi de transposition n'est entrée en vigueur que bien des années plus tard[664].

252. A la suite de l'entrée en vigueur de ces deux lois fondatrices, c'est par le premier arrêté[665] relatif au SNIIRAM que l'accès sélectif a véritablement été mis en œuvre, dévoilant ainsi l'identité de ses potentiels bénéficiaires. Remarquons d'emblée que les acteurs pouvant prétendre à l'accès sélectif ne sont désignés que par un mécanisme d'exclusion : au lieu de définir précisément qui peut ou ne peut pas déposer une demande d'accès aux données personnelles de santé, l'arrêté se contente d'indiquer que toutes les demandes qui ne rentrent pas dans le cadre de l'accès permanent doivent nécessairement passer par la procédure d'accès sélectif. Dans ce cadre, d'après la lecture du premier arrêté, tous les acteurs non concernés par l'accès permanent en 2002 avaient, en théorie, la possibilité de déposer une demande dans les conditions prévues à l'ancien chapitre V ter de la loi relative à l'informatique et aux libertés[666] : cela inclut les acteurs privés à but lucratif. Cette formule très évasive, et au champ d'application extrêmement large, témoigne des balbutiements dont faisait l'objet, au début des années 2000, le sujet de l'ouverture contrôlée de l'accès aux données personnelles de santé.

253. A titre de rappel, il est nécessaire d'avoir à l'esprit que, lors de l'élaboration du SNIIRAM, il n'était pas directement prévu de rendre possible l'extraction et la mise à disposition des données. En effet, la loi du 23 décembre 1998[667] ne prévoyait que deux missions dévolues à ce système, et aucune n'indiquait de procédure spécifique d'autorisation d'accès ouverte à tous. Nous pouvons comprendre la prudence du texte car le risque principal qui existait alors est,

---

[663] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[664] *Infra* n° 254.

[665] Arrêté du 11 avril 2002, *op. cit*.

[666] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 94-548 du 1 juillet 1994 *op. cit.*

[667] Loi n° 98-1194 du 23 décembre 1998, *op. cit.*, art. 21 : « *Il est créé un système national d'information interrégimes de l'assurance maladie qui contribue :*

1° A la connaissance des dépenses de l'ensemble des régimes d'assurance maladie par circonscription géographique, par nature de dépenses, par catégorie de professionnels responsables de ces dépenses et par professionnel ou établissement ;

2° A la transmission en retour aux prestataires de soins d'informations pertinentes relatives à leur activité et leurs recettes, et s'il y a lieu à leurs prescriptions. »

aujourd'hui encore, d'actualité : il s'agit du risque de réidentification[668] des individus pouvant entrainer une violation directe du respect de leur vie privée. Cependant, l'arrêté de 2002 est venu prévoir la possibilité d'accéder aux données du SNIIRAM en renvoyant aux dispositions légales en vigueur. Avant la loi du 6 août 2004[669], l'accès sélectif était donc offert à tous les acteurs exclus de l'accès permanent. Dans ce cadre, seules des données présentées « *sous la forme de statistiques agrégées ou de données par patient constituées de telle sorte que les personnes concernées ne puissent être identifiées* » pouvaient être communiquées. Cette précision a son importance[670] car cela signifie que les acteurs éligibles à l'accès sélectif ne pouvaient accéder qu'à des données qui nécessitaient un traitement préalable destiné à assurer l'absence de risque de réidentification, et donc à éradiquer, ou tout du moins limiter fortement, les dangers pesant sur la protection de la vie privée.

254. Cette première définition des bénéficiaires de l'accès sélectif n'a subsisté que quelques années avant d'être remaniée par la transposition de la directive européenne de 1995[671] en droit français par la loi du 6 août 2004[672]. Le délai de transposition, près de dix ans, ne fut pas vain car ladite loi a intégralement révisé le contenu de la loi relative à l'informatique et aux libertés[673]. Dans le sillage de cette réforme, l'arrêté relatif à la mise en œuvre du SNIIRAM de 2002[674] a, lui aussi, été mis à jour par arrêté du 20 juin 2005[675].

255. La prise en compte de la réforme du 6 août 2004[676] par l'arrêté relatif au SNIIRAM de 2005[677] est venue affiner le champ des acteurs pouvant déposer une demande dans le cadre de l'accès sélectif. Le texte a ajouté plusieurs éléments de nature à nous indiquer qui peut prétendre obtenir un accès aux données de santé. En premier lieu, une distinction nous est proposée en fonction de l'activité des demandeurs : il ne peut s'agir que d'un « *organisme de recherche,*

---

[668] V. *supra* n° 53 à 62 et notamment BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 26.

[669] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[670] V. *infra* n° 374 à 376 l'impact du traitement préalable des données sur l'effectivité de l'accès sélectif.

[671] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[672] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[673] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[674] Arrêté du 11 avril 2002, *op. cit*.

[675] Arrêté du 20 juin 2005, *op. cit*.

[676] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[677] Arrêté du 20 juin 2005, *op. cit*.

[d'] *universités, écoles ou autres structures d'enseignement liés à la recherche* ». L'interprétation stricte de cette première distinction indique que tous les organismes qui n'ont pas d'activité liée à la recherche sont totalement exclus de l'accès sélectif : la légitimité d'une telle exclusion est compréhensible mais discutable[678]. Le deuxième élément distinctif, le plus important car le plus discriminant, vise l'objet de l'activité du demandeur : toute structure « *poursuivant un but lucratif ne peut accéder aux informations* » mises à dispositions dans le cadre du SNIIRAM[679]. Ainsi, c'est toute une partie des acteurs potentiellement intéressés par l'accès aux données de santé qui se trouve exclue du dispositif d'accès sélectif. Ce principe a soulevé de nombreux débats relatifs notamment à l'impact négatif sur l'utilité de l'accès sélectif qui n'est pas accessible à une frange importante des potentiels bénéficiaires[680].

256. Ce principe d'exclusion catégorique des acteurs à but lucratif du bénéfice de l'accès sélectif est resté en vigueur jusqu'à la réforme de la loi de modernisation de notre système de santé[681] qui a ouvert l'accès à tous les acteurs privés, publics, à but lucratif ou non. Cependant, comme nous le verrons ultérieurement[682], certains organismes à but lucratifs, tels que des laboratoires[683], n'ont pas attendu la réforme pour obtenir le droit d'accéder à des données de santé à caractère personnel pour effectuer des traitements, dans le respect du cadre protecteur de la vie privée.

257. Une subtilité se glisse dans l'articulation de l'accès sélectif avec l'accès permanent aux données personnelles de santé. Comme cela a déjà été développé au sein de cette étude[684], certains acteurs bénéficient d'un accès permanent aux données. Cet accès est ouvert à une liste limitée de personnes, définie par arrêté[685] et dernièrement par décret[686]. L'une des

---

[678] *Infra* n° 462.

[679] Pour l'analyse de l'accès des acteurs privés à but lucratif, v. Partie III.

[680] Sur les débats entourant l'encadrement de l'accès sélectif, v. Partie II ; Titre II.

[681] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*, v. art. L. 1461-3 du code de la santé publique.

[682] *Infra* n° 489 à 492.

[683] Sur ce sujet, nous pouvons citer deux arrêts emblématiques du Conseil d'Etat impliquant tous deux la société Celtipharm : Conseil d'Etat, 10e et 9e sous-sections réunies, 26 mai 2014, n° 354903, recueil Lebon, Société IMS Health c/ CNIL et Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, recueil Lebon, Celtipharm.

[684] V. Partie I.

[685] Depuis l'arrêté du 11 avril 2002, *op. cit.*, jusqu'à l'arrêté du 6 octobre 2016, *op. cit.*, la liste des bénéficiaires de l'accès permanent et l'étendue des données accessibles a régulièrement évolué.

[686] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

caractéristiques majeures de l'accès permanent est aussi qu'il n'est pas ouvert à la même étendue de données selon la nature de l'acteur concerné : ainsi en 2005, les médecins-conseils des caisses d'assurance maladie avaient accès à l'ensemble des données du SNIIRAM, tandis que les agents du ministère chargé de la santé n'avaient accès qu'à ces données sous forme de statistiques agrégées. Aujourd'hui encore, la réforme a maintenu ces distinctions éventuelles afin que le personnel accomplissant les missions de service public visées n'ait accès qu'aux données qui leur sont utiles.

258. Cependant, nous pouvons nous demander si les acteurs dont la sollicitation de données excède le champ de leur accès permanent sont contraints de se plier au mécanisme de l'accès sélectif. Nous aurions pu penser que la procédure d'accès sélectif pouvait leur être destinée : et nous aurions eu à la fois tort et raison. En effet, le premier arrêté de 2002[687] précisait bien, à l'issue de la liste des bénéficiaires de l'accès permanent, que « *toute autre demande d'accès à des données individuelles relatives aux bénéficiaires* [devait] *faire l'objet d'une demande d'autorisation auprès de la CNIL dans les conditions prévues aux articles 40-11 à 40-15 de la loi du 6 janvier 1978* » : les acteurs ayant un accès permanent étaient donc directement invités à se soumettre à l'accès sélectif pour les données qui ne leur étaient pas ouvertes. Mais avec la mise en œuvre de l'Institut national des données de santé (IDS) en 2005[688], un véritable dispositif, propre à l'accès sélectif, était proposé : l'IDS avait pour mission d'approuver les traitements de données envisagés avant de transmettre les dossiers à la CNIL à travers la procédure prévue par le chapitre X de la loi relative à l'informatique et aux libertés[689]. Cependant, les arrêtés successifs n'ouvraient cette procédure qu'à « *tout autre organisme* […] *ou autres structures* […] *que ceux mentionnés au paragraphe précédent* »[690] : les acteurs soumis à l'examen préalable de leur demande par l'IDS n'étaient donc que des acteurs qui ne faisaient pas partie de la liste des bénéficiaires de l'accès permanent. Cette exclusion d'office de l'accès sélectif, pour les acteurs ayant un accès permanent est étonnant car il semble évident que rien n'interdisait auxdits acteurs de solliciter la CNIL, à travers le chapitre X de la loi

[687] Arrêté du 11 avril 2002, *op. cit.*

[688] L'Institut des données de santé (IDS) a été défini par l'arrêté du 20 juin 2005, *op. cit.*

[689] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[690] Cette formule apparaît pour la première fois dans l'arrêté du 20 juin 2005, *op. cit.*, et se retrouve dans tous les arrêtés réformant la mise en œuvre du SNIIRAM jusqu'à celui du 19 juillet 2013, *op. cit.*

relative à l'informatique et aux libertés[691] auquel la procédure d'accès sélectif renvoyait systématiquement.

259. Depuis la réforme du 26 janvier 2016[692] et la parution du décret du 26 décembre 2016[693], cette légère incohérence est réparée comme le soulignait M. GIRARD[694]. Les dispositions propres à l'accès permanent prévoient désormais officiellement que « *lorsque les besoins d'un traitement particulier ou d'une catégorie de traitements de données du système national des données de santé excèdent l'étendue de l'autorisation dont bénéficie, sur le fondement des dispositions* [relatives à l'accès permanent]*, le service de l'Etat, l'établissement ou l'organisme qui entend le mettre en œuvre, ce dernier soumet à la Commission nationale de l'informatique et des libertés une demande d'autorisation dans les conditions mentionnées au II de l'article L. 1461-3* [du code de la santé publique] »[695]. Cet article du code de la santé publique auquel le décret renvoie indique que tout traitement à des fins de recherche, d'étude, ou d'évaluation doit être autorisé selon la procédure définie à la section 3 du chapitre III du Titre 2 de la loi relative à l'informatique et libertés[696] qui est aujourd'hui la référence en matière d'accès sélectif aux données de santé.

260. Aujourd'hui, tous les acteurs qui souhaitent traiter des données aux fins qui sont strictement définies par la loi[697] relèvent donc du même mécanisme, peu importe qu'il s'agisse d'un acteur public « ordinaire » ou privé ou d'un bénéficiaire de l'accès permanent qui souhaite accéder à des données qui n'entrent pas dans son autorisation initiale. Maintenant que le champ des bénéficiaires potentiels de l'accès sélectif à travers les années est bien appréhendé, il est important de connaître qui, au sein des différentes structures, est autorisé à être en contact avec les données mises à dispositions et quels types d'obligations pèsent sur ces personnes.

---

[691] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit*.

[692] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[693] Décret n° 2016-1871 du 26 décembre 2016, *op. cit*.

[694] GIRARD M., cheffe de la mission accès aux données de santé à la DREES, a proposé un bilan des premiers mois de fonctionnement du nouvel accès sélectif à l'occasion du colloque « Santé et protection des données », *Cycle Conseil d'Etat en droit social*, 01/12/2017.

[695] Article R. 1461-15 du code de la santé publique créé par le décret n° 2016-1871 du 26 décembre 2016, *op. cit*.

[696] Loi n° 78-17 du 6 janvier 1978, *op. cit*. Depuis l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit*., les dispositions du chapitre IX initialement visé par le II de l'article L. 1461-3 du code de la santé publique ont été complétées et déplacées à la section 3 du chapitre III du Titre 2 de la loi. Pour l'étude de la procédure d'accès sélectif découlant de la réforme du 26 janvier 2016, v. *infra* n° 330 à 336.

[697] Pour l'étude des finalités autorisées dans le cadre de l'accès sélectif, v. *infra* n° 273 à 282.

Paragraphe 2 : Le contrôle individuel renforcé de l'accès sélectif

261. Entre la mise en place du premier accès sélectif et le système tel qu'il existe aujourd'hui, les acteurs bénéficiaires ont rarement été entièrement libres de conférer, en interne, la jouissance de l'autorisation de traitement aux personnes de leur choix. Pourquoi « rarement » ? Tout simplement parce qu'avant la transposition en droit français de la directive européenne du 24 octobre 1995[698], la notion de responsable de traitement n'existait pas encore en droit français. La seule mention d'une personne physique potentiellement responsable pouvait être trouvée à l'article 19, alinéa 2, de la loi relative à l'informatique et libertés[699] qui disposait que « *la demande d'avis ou la déclaration* [effectuée auprès de la CNIL] *doit préciser : la personne qui présente la demande et celle qui a pouvoir de décider la création du traitement* ». La loi ne ciblait pas directement de personne physique chargée de veiller à la bonne mise en œuvre du traitement de données personnelles de santé en faisant peser sur elle des obligations qui leur étaient propres. Rappelons malgré tout que des dispositions pénales étaient déjà prévues aux articles 226-16 à 226-24 du code pénal. Mais ces mesures ne s'adressaient qu'aux personnes physiques ou morales recueillant, détenant ou traitant des données nominatives, ce qui excluait par principe les bénéficiaires de l'accès sélectif qui ne pouvaient, à aucun moment, se voir communiquer des données de santé nominatives ou identifiantes.

262. Ce n'est donc pas avant la loi du 6 août 2004[700] transposant la directive européenne susmentionnée, que les bénéficiaires de l'accès sélectif, et par extension tous les acteurs ayant l'ambition de mettre en œuvre un traitement de données personnelles, ont eu l'obligation d'avoir, en leur sein, un individu identifié, en charge du traitement autorisé par la CNIL : le responsable de traitement. Depuis lors, tous les traitements de données personnelles doivent être chapeautés par une personne physique identifiée. Ce responsable de traitement a notamment l'obligation personnelle de « *prendre toutes précautions utiles* […] *pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou*

[698] Directive 95/46/CE du 24 octobre 1995, *op. cit.* Pour une étude du contenu de la directive, v. de LAMBERTERIE I., « Protection de la vie privée et traitement des données relatives à la santé à l'heure européenne », *Médecine et droit*, 01/09/1996, n° 20, p. 6-12.

[699] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version antérieure à la loi n° 2004-801 du 6 août 2004, *op. cit*.

[700] Loi n° 2004-801 du 6 août 2004, *op. cit*.

que des tiers non autorisés y aient accès »[701]. Il est également précisé que le responsable de traitement est, seul, habilité à autoriser un sous-traitant, ou une personne agissant sous son autorité, à traiter des données personnelles.

263. Au regard de la complexité des dispositions entourant les traitements de données personnelles, de surcroît lorsqu'elles s'ancrent dans le domaine de la santé, il a été proposé aux acteurs, dès 2005[702], la possibilité de nommer une personne chargée de construire une relation vertueuse avec la CNIL : le correspondant à la protection des données à caractère personnel, longtemps appelé correspondant informatique et libertés (CIL) en France. Celui-ci a pour mission « *d'assurer, d'une manière indépendante, le respect des obligations prévues dans la* [loi relative à l'informatique et aux libertés] »[703]. A ce titre, il « *ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions* »[704], ce qui lui permet en principe d'agir en toute indépendance. Cette faculté, offerte par la transposition de la directive européenne de 1995[705], permet au responsable de traitement de nommer un CIL dans des conditions définies par décret[706]. Toutes les informations transmises à la Commission doivent permettre à cette dernière d'identifier le CIL, de connaître son périmètre d'intervention sur le ou les traitements, de comprendre quels sont ses liens avec l'acteur auprès duquel il intervient, d'apprécier ses qualifications ou références professionnelles, et enfin de savoir quelles mesures protectrices des données ont été prises par le responsable de traitement pour l'accomplissement des missions du correspondant. Les textes sont sans ambiguïté sur ce point, la responsabilité des individus mettant en œuvre des traitements pour le compte de personnes morales, notamment dans le cadre de l'accès sélectif, témoigne de la volonté des autorités nationales d'impliquer tous les acteurs dans une spirale d'utilisation vertueuse des données personnelles dans le respect complet de la vie privée.

---

[701] Les obligations du responsable de traitement étaient alors détaillées aux articles 32 à 37 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiées par la loi n° 2004-801 du 6 août 2004, *op. cit.* Aujourd'hui ces obligations sont prévues par le Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*.

[702] Décret n° 2005-1309 du 20 octobre 2005 *pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*.

[703] *Ibid.*, art. 49.

[704] Art. 22, III, alinéa 3 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*

[705] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[706] Décret n° 2005-1309 du 20 octobre 2005, *op. cit.*, v. son Titre III.

Les années 2004 et 2005 ont finalement été une période de mutation pour l'accès sélectif aux données de santé, mais aussi pour les traitements de données personnelles dans leur ensemble. L'imposition d'un responsable de traitement et la possibilité de nommer un correspondant à la protection des données à caractère personnel permet de faire peser une responsabilité accrue sur les individus mettant en œuvre des traitements mais aussi de tisser un lien de confiance, voire de collaboration entre eux et la CNIL. Le Règlement général relatif à la protection des données[707] a remplacé cette faculté de désigner un CIL par une forte incitation, voire parfois une obligation[708], qui n'existait pas jusqu'alors pour tous les acteurs réalisant un traitement de données de santé à caractère personnel. Cette nouvelle obligation a un impact très important en pratique : celle de nommer un délégué à la protection des données ou DPO (*data protection officer*) qui pèse sur tous les candidats à l'obtention de données de santé à caractère personnel. Comme nous allons le découvrir dans les prochains développements, le DPO, prévu par les articles 37 à 39 du Règlement européen, s'impose comme la version augmentée du Correspondant informatique et libertés, ou CIL, que nous connaissions depuis la loi du 6 août 2004[709].

264. Dans quels cas la nomination d'un délégué à la protection des données est-elle obligatoire ? D'une part, toute autorité publique ou organisme public effectuant un traitement de données à caractère personnel a l'obligation de désigner une personne à cette fonction[710]. Les acteurs publics disposant d'un accès permanent ou ayant obtenu un accès sélectif au SNDS doivent donc nommer un DPO. D'autre part, tout acteur ayant pour activité de base le traitement à grande échelle de catégorie particulières de données visées à l'article 9 (dont font partie les données concernant la santé) est également obligé de nommer un DPO[711]. Cette nouvelle contrainte qui s'ajoute à toute la procédure d'accès au SNDS produit nécessairement des effets sur la pratique. Nous pouvons d'ores et déjà nous interroger sur la notion de « *traitement à grande échelle* » de données de santé à caractère personnel rendant obligatoire la désignation d'un DPO. Aucune indication n'est donnée sur un ordre de grandeur permettant de savoir à

[707] Règlement 2016/679, *op. cit.*

[708] *Infra* n° 266 et 267.

[709] 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.

[710] Règlement 2016/679, *op. cit.*, art. 37, point 1, a).

[711] *Ibid.*, art. 37, point 1, c).

partir de combien de données un traitement devient « *à grande échelle* ». Pourtant, cette précision mériterait d'être donnée car un traitement de données de santé qui ne serait pas effectué « *à grande échelle* » n'impose pas la désignation d'un DPO. Dans le cas de l'accès aux données du SNDS, il est fort probable que les informations demandées par les acteurs publics ou privés soient très nombreuses, mais tant que le seuil de quantité de données à dépasser, pour faire basculer un traitement dans la catégorie des traitements à grande échelle, ne sera pas défini, un doute persistera. En tout état de cause, l'acteur souhaitant obtenir des données de santé du SNDS a tout intérêt à désigner un DPO : cela « *démontre la bonne gouvernance interne et instaure la confiance* »[712], cela ne peut jouer qu'un rôle positif dans l'examen du dossier déposé à l'INDS et examiné par le CEREES et la CNIL.

265. Nous pouvons légitimement nous poser la question de savoir qui sont les personnes susceptibles d'être désignées correspondant à la protection des données à caractère personnel. Initialement, la loi ne prévoyait qu'une obligation de compétences, dont l'appréciation reste très subjective, en indiquant que « *le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions* »[713]. Le CIL pouvait alors être une personne physique ou morale, sans condition de connaissances particulières dans le domaine de la protection de la vie privée ou des bases de données. Ainsi, les acteurs disposaient d'une grande liberté dans la désignation de la personne de leur choix qui pouvait simplement être un juriste ou un technicien informatique, mais aussi un directeur du système d'information et de l'organisation ou un directeur de service juridique. Le correspondant à la protection des données à caractère personnel est donc bien souvent un salarié dont l'employeur juge les compétences suffisamment développées pour mener à bien les missions qui lui sont confiées dans le cadre de la loi relative à l'informatique et aux libertés[714]. Cependant, l'absence de précision dans la définition des qualifications requises est une source potentielle d'insécurité juridique concernant le degré d'appréciation desdites qualifications.

Désormais, les acteurs qui souhaitent déposer un dossier auprès de l'INDS en vue d'obtenir des données de santé doivent avoir désigné une personne physique ou morale[715] ayant des qualités

[712] FAUVARQUE-COSSON B., « Protection des données personnelles », *op. cit.*

[713] V. art. 22, III, alinéa 3 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*

[714] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[715] Le texte du Règlement 2016/679, *op. cit.*, ne précise jamais la nature du DPO, plusieurs indices permettent de conclure qu'il peut être une personne physique aussi bien que morale : par exemple au lieu d'évoquer les nom et

bien particulières. En effet, le nouveau Règlement européen apporte une clarification concernant les modalités de choix du correspondant à la protection des données à caractère personnel, désormais appelé délégué à la protection des données.

D'abord, celui-ci doit être désigné « *sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions* »[716] qui lui sont confiées. Cette contrainte supplémentaire demande à l'acteur qui souhaite obtenir des données de santé provenant du SNDS de bien sélectionner son DPO sur des critères objectifs : la personne choisie doit être suffisamment compétente pour être immédiatement opérationnelle dans ses fonctions.

Ensuite, afin de proposer une solution alternative à un recrutement direct qui peut parfois s'avérer extrêmement chronophage et même infructueux, le Règlement européen a prévu que le « *délégué à la protection des données peut* […] *exercer ses missions sur la base d'un contrat de service* »[717]. Autrement dit, la fonction de DPO peut être externalisée auprès d'un prestataire de services. Cette solution est potentiellement plus favorable aux petites structures qui font de la recherche dans le domaine de la santé, encore faut-il être en mesure de trouver un prestataire de services fiable, capable de remplir la mission de DPO. A ce titre, la CNIL a mis en place un certificat de délégué à la protection des données dont le projet de référentiel a fait l'objet d'une consultation publique du 23 mai 2018 au 22 juin 2018. Les modalités de certification ont finalement été approuvées par deux délibérations distinctes de la CNIL en date du 20 septembre 2018. La première[718] est relative aux critères du référentiel d'agrément d'organismes de certification dont la mission est de certifier les compétences du DPO. La seconde[719] vise la définition des critères du référentiel de certification des compétences du DPO. Les acteurs n'ayant pas les ressources suffisantes pour recruter, ou désigner en interne, un DPO ont donc la faculté de recourir à un tiers : cette solution est probablement moins onéreuse qu'une création de poste, et cela permet notamment à celui qui demande l'accès à des données de santé de

prénom du DPO, le texte renvoie à ses « *coordonnées* ». Le fait que le DPO puisse être externalisé laisse également penser que la fonction peut être déléguée à une personne morale.

[716] V. art. 37 du Règlement 2016/679, *op. cit.*

[717] *Ibid.*, art. 37, point 6.

[718] Délibération n° 2018-317 du 20 septembre 2018 portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPO).

[719] Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPO).

déléguer la tâche sereinement. Malgré tout, cette solution offerte par le droit européen d'externaliser le DPO est appréciable à cet égard. Cependant, elle comporte un inconvénient majeur souligné par V. LANGLET : « *le DPO n'aura pas écho des « conversations à la machine à café » ni même la connaissance fine de l'environnement de travail* »[720]. Cela peut impacter négativement les actions menées par le DPO externalisé qui n'a pas toutes les cartes en main pour bien appréhender les problématiques de l'acteur qui traite, ou qui souhaite traiter, des données de santé à caractère personnel provenant du SNDS.

266. L'obligation de désigner un DPO prévue par le droit européen, dans le cas où des données de santé à caractère personnel sont traitées à grande échelle, peut être vécue comme une contrainte supplémentaire importante par les acteurs qui traitent des données de santé à caractère personnel. La création de cette exigence repose avant toute chose sur l'objectif de protection des données traitées et de la vie privée des individus dont elles sont issues. En effet, les missions du DPO[721] consistent notamment à informer et conseiller le responsable de traitement ou le sous-traitant de leurs obligations prévues par le droit ; à contrôler le bon respect des dispositions légales et réglementaires par le responsable de traitement ou le sous-traitant en matière de protection des données ; à prodiguer des conseils concernant l'analyse d'impact ; à coopérer avec la CNIL tout en servant de point de contact avec celle-ci. Son rôle est, d'après les lignes directrices du groupe de travail européen sur la protection des données (ou G29)[722], de promouvoir « *une culture de la protection des données au sein de l'organisation et dans la mise en œuvre des éléments essentiels du* [Règlement général relatif à la protection des données] »[723]. Mais pour que ces missions soient correctement exercées, des garanties précises doivent être apportées[724]. Le DPO doit être indépendant et ne doit recevoir aucune instruction vis-à-vis de l'exercice de ses missions : l'organisme qui le désigne « *doit s'assurer d'une neutralité absolue* »[725]. D'une manière générale, le responsable du traitement ou le sous-traitant doit s'assurer que le DPO dispose de toutes les informations utiles et nécessaires, ainsi que de tous les moyens pour mener à bien ses missions.

---

[720] LANGLET V., « Nom de code : délégué à la protection des données », *Juris tourisme*, n° 207, 2018, p. 29.

[721] *Ibid.*, art. 39.

[722] Groupe de travail « Article 29 » sur la protection des données, « Lignes directrices concernant les délégués à la protection des données (DPD) », adoptées le 13 décembre 2016 et modifiées en dernier lieu le 5 avril 2017.

[723] FAUVARQUE-COSSON B., « Protection des données personnelles », *op. cit*.

[724] *Ibid.*, art. 38.

[725] LANGLET V., « Nom de code : délégué à la protection des données », *op. cit.*

Il découle de la définition de l'actuel délégué à la protection des données semble favoriser la désignation d'un juriste spécialisé en droit de la protection des données mais pas uniquement. Dans la pratique, un technicien informatique ayant des connaissances juridiques dans ce domaine pourrait aussi être apte à assumer ce rôle. Notons que, malgré la volonté du droit européen d'affiner les critères de désignation du délégué à la protection des données, une place importante est encore laissée à l'appréciation subjective des acteurs.

267. Cette nouvelle obligation de disposer, en interne ou *via* un prestataire externe, d'une personne chargée du respect du droit liée à la protection des données personnelles et de la vie privée est certes vertueuse en ce qu'elle responsabilise les acteurs dans leur démarche. En revanche, comme nous l'avons décrypté, le fait de choisir son DPO n'est pas un acte anodin et nécessite un travail supplémentaire important. Cette tâche s'ajoute inexorablement à toutes les autres mesures liées à la procédure d'accès sélectif aux données du SNDS, ce qui complexifie davantage l'ensemble du dispositif. Cela aurait-il pu, ou dû, être évité pour autant ? Il est difficile de répondre positivement à cette question tant la fonction du DPO semble primordiale dans l'assurance du respect du droit relatif à la protection des données et de la vie privée par l'acteur réalisant un traitement de données à caractère personnel. Ce nouvel intervenant s'apparente autant à une « *épine dans le pied* » du responsable du traitement ou du sous-traitant (car il lui indiquera tous les points à améliorer pour se conformer au droit), qu'à un gardien du temple chargé de veiller à la bonne réalisation du traitement de données en le maintenant dans les limites définies par le droit.

268. Cet accroissement de la responsabilité des bénéficiaires de l'accès sélectif a une autre conséquence : la contrepartie de cette autonomisation a notamment été la création de nouvelles sanctions, largement remaniées par l'adaptation de la loi relative à l'informatique et aux libertés au Règlement européen du 27 avril 2016[726] comme nous l'étudierons prochainement[727] : ainsi le responsable de traitement pouvait être déchargé de ses fonctions en cas de manquement constaté à l'un ou plusieurs de ses devoirs[728].

[726] Règlement 2016/679, *op. cit.*

[727] *Infra* n° 288 à 295.

[728] V. art. 22 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifié par la loi n° 2004-801 du 6 août 2004, *op. cit.*

269. Quelques enseignements peuvent être tirés des textes et de leurs évolutions proposées depuis la création de l'accès sélectif aux données de santé. Le principal enseignement touche à la grande variété d'acteurs potentiellement bénéficiaires dudit accès, qui a d'abord exclu les acteurs à but lucratif[729] avant de les réintégrer avec la réforme du 26 janvier 2016[730] pour les raisons que nous évoquerons plus loin[731]. Signalons également que ce potentiel de nombreux bénéficiaires de l'accès sélectif est probablement l'un des points fortement sensibles du mécanisme en raison de son obligation d'allier l'accessibilité des données avec le principe de sécurité de celles-ci. Cette nécessaire protection implique par ailleurs le contrôle individuel[732] des personnes exerçant au sein des structures qui jouissent d'une autorisation d'accès sélectif, ce qui peut avoir pour conséquence de peser encore plus sur la procédure. Le jeu d'équilibriste qui existe entre l'ouverture des données, le contrôle sur leur diffusion et leur utilisation vertueuse représente le cœur des dysfonctionnements qui ont pu émailler la vie de l'accès sélectif jusqu'à la dernière réforme : ces sujets seront traités dans le prochain titre[733].

270. A présent que nous connaissons l'étendue des bénéficiaires de l'accès sélectif et la façon dont la mise en place dudit accès doit être suivie en interne, il convient de nous intéresser aux prérequis imposés par la législation en vigueur ainsi qu'aux sanctions potentielles qui pèsent sur les acteurs.

SECTION 2 : LA SÉVÉRITÉ DE L'ENCADREMENT DE L'ACCÈS SÉLECTIF

271. Le bénéfice de l'accès sélectif peut être ouvert à une grande variation d'acteurs comme nous l'avons vu dans la section précédente[734]. Ce vaste champ d'application a immédiatement conduit le législateur à définir des conditions *sine qua non* imposées à tous les prétendants à une autorisation d'accès sélectif (Paragraphe 1). A ces prérequis viennent s'ajouter les éléments dissuasifs essentiels de l'arsenal juridique : il s'agit des sanctions qui pèsent sur les bénéficiaires

[729] *Supra* n° 255.

[730] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[731] V. Partie III.

[732] *Supra* n° 261 à 267.

[733] V. Partie II, Titre II.

[734] *Supra* n° 251 à 260.

de l'accès sélectif en cas de manquement au respect des dispositions légales et réglementaires (Paragraphe 2).

Paragraphe 1 : Les garanties préalables à l'accès sélectif

272. Plusieurs types de prérequis ont été mis en place pour déterminer les conditions d'autorisation de l'accès sélectif. Une distinction nette peut être opérée entre les finalités permises, d'une part (A), et les grands principes qui régissent cet accès aux données de santé (B).

A) Les finalités autorisant l'accès sélectif

273. En droit français, la première inscription dans la loi de la notion de traitement de données à caractère personnel potentiellement liées à la santé a été permise par la loi du 1er juillet 1994[735]. Comme évoqué en introduction du présent titre[736], cette loi a créé le chapitre V bis dans la loi relative à l'informatique et aux libertés[737] dénommé « *Traitements automatisés de données nominatives ayant pour fin la recherche dans le domaine de la santé* ». Il n'est pas clairement fait allusion aux données personnelles de santé mais nous pouvons déduire de la formule utilisée que les termes « *données nominatives* […] *dans le domaine de la santé* » font notamment référence à toutes les données personnelles relatives à la santé des individus. Il s'agit là des premières dispositions légales destinées à encadrer précisément le traitement des données personnelles de santé : tout traitement de données de santé était alors autorisé à la condition d'avoir pour finalité la recherche dans le domaine de la santé. Par opposition, toute autre finalité de traitement conduisait à un refus d'autorisation. Le législateur s'intéressait donc déjà à ce sujet, bien avant que des définitions de la donnée personnelle de santé ne soient proposées aussi bien en droit français qu'au niveau européen, ou que la base de données SNIIRAM ne soit créée. Nous pouvons d'ailleurs noter l'utilisation inadéquate de la notion de « *donnée nominative* » : en effet, une donnée peut ne pas être nominative et garder le caractère de donnée personnelle directement ou indirectement identifiante[738]. C'est-à-dire qu'une donnée

[735] Loi n° 94-548 du 1 juillet 1994 *op. cit.*

[736] *Supra* n° 16.

[737] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version modifiée par la loi n° 94-548 du 1 juillet 1994 *op. cit.*

[738] *Supra* n° 36 à 39.

qui permet d'identifier directement ou indirectement un individu sans jamais avoir de caractère nominatif fait partie du champ de la donnée personnelle.

274. Cette première procédure de traitement de données personnelles dans le domaine de la santé prévue par la loi du 1er juillet 1994[739] a posé les fondations[740] de ce qui deviendra le futur mécanisme d'accès aux données de santé du SNIIRAM. Un an après la prise de position claire du législateur français à l'égard de l'encadrement des traitements de données personnelles dans le domaine de la santé, la directive 95/46/CE du 24 octobre 1995[741] a apporté un socle européen commun au traitement des données personnelles dans leur ensemble. Son article 8 porte spécifiquement sur les traitements de données dites sensibles, incluant celles qui sont relatives à la santé. Si le traitement de telles données est en principe interdit, aussi bien par le droit européen que national[742], des exceptions sont permises et abondent dans le sens de la dérogation permise par la loi française. En effet, le paragraphe 4 de l'article 8 dispose que « *sous réserve de garanties appropriées, les Etats membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle* ». La directive admet donc que des traitements de données personnelles de santé puissent être réalisés à des conditions cumulatives : la création de garanties appropriées, permettant notamment de protéger la vie privée ; l'existence d'un motif d'intérêt public important ; l'autorisation de dérogation par la loi ou par une autorité de contrôle spécifique. Comme nous allons le constater, le législateur français a choisi de n'autoriser l'accès aux données personnelles de santé, et leur traitement, que dans le cadre de finalités prévues par la loi.

275. L'accès sélectif à des données personnelles de santé est nécessairement accompagné d'une série de contrepoids permettant de s'assurer de la protection adéquate des informations transmises, comme le requiert le droit européen depuis la directive de 1995[743]. Si la question de la suffisance de ces contrepoids et de la pertinence des exigences se pose[744], il est primordial de connaître leurs caractéristiques. Lorsque l'accès sélectif a été formellement créé en droit

[739] Loi n° 94-548 du 1 juillet 1994 *op. cit.*

[740] Pour une analyse du dispositif créé en 1994, v. *infra* n° 302 à 310.

[741] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[742] *Supra* n° 60.

[743] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[744] *Infra* n° 357 à 392.

français pour la première fois en 2002[745], c'est la procédure dictée par le chapitre V ter, évoqué précédemment[746], de la loi relative à l'informatique et aux libertés[747] qui faisait référence. Ce chapitre imposait d'emblée un prérequis de taille : les données ne pouvaient être accessibles qu'à la condition que la ou les finalités du traitement envisagé relèvent soit de l'évaluation, soit de l'analyse des activités de soins et de prévention. Toute autre finalité devait alors conduire au refus d'autorisation d'accéder aux données : la recherche ou l'identification des personnes étaient ainsi directement visées par cette exclusion à l'article 40-15 de la loi[748] ; devenu plus tard article 66[749].

276. Cette méthode consistant à limiter l'accès aux données personnelles de santé à certaines finalités déterminées est importante car elle joue le rôle de premier filtre parmi les demandeurs avant même le dépôt du dossier. C'est au demandeur de s'adapter aux finalités autorisées et non l'inverse. Ce procédé a également pour objectif de ne conduire à transmettre que des données pertinentes pour les finalités du traitement envisagé dans le cadre de l'accès sélectif. Ce principe d'autorisation découlant de la finalité du traitement provient directement de la directive européenne de 1995[750]. Bien que n'ayant pas encore été transposée en droit français au moment de la création du chapitre V ter susmentionné, l'esprit de l'article 20 du texte européen imprégnait déjà le mécanisme d'accès sélectif[751]. En effet, comme le notait I. de LAMBERTERIE[752], la directive prévoyait que les « *Etats membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre* ». L'auteure nous indique que l'expression « *risques particuliers* », bien qu'elle ne soit pas définie, vise notamment les finalités qui conduiraient à nuire aux droits d'un individu d'après le considérant 53 de ladite directive. Dès lors, c'est parce qu'un Etat identifie un risque qu'il peut mettre en place un système d'autorisation préalable pouvant notamment reposer sur le

[745] Arrêté du 11 avril 2002, *op. cit.*

[746] *Supra* n° 251.

[747] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version modifiée par la loi n° 94-548 du 1 juillet 1994 *op. cit.*

[748] *Ibid.* modifiée par la loi n° 99-641 du 27 juillet 1999, *op. cit.*

[749] *Ibid.* modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[750] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[751] V. *infra* n° 304 à 309 et 337 à 343 pour notre analyse de l'impact du droit européen sur l'accès sélectif aux données de santé.

[752] de LAMBERTERIE I., « Protection de la vie privée et traitement des données relatives à la santé à l'heure européenne », *Médecine et droit*, 01/09/1996, n° 20, p. 11.

contrôle de la ou des finalités du traitement envisagé. C'est précisément à partir de ce principe que le droit français de l'accès sélectif aux données de santé s'est développé.

277. La problématique de la finalité se pose également du point de vue de la personne dont les données personnelles de santé sont recueillies, stockées, puis traitées ultérieurement. En effet, l'individu dispose du droit à être informé de la ou des finalités du traitement auquel ses données sont destinées[753]. Les données personnelles ainsi récoltées ne peuvent servir à aucun autre traitement que celui qui a été initialement prévu. Cette condition présente un paradoxe intéressant, notamment mis en lumière par H. KHODOSS en 2004[754] : elle souligne que les données personnelles de santé sont avant tout collectées dans « *l'intérêt d'un malade singulier, dans le cadre d'une relation thérapeutique fondamentalement individuelle* » alors que l'objectif même des traitements de données de santé permis par l'accès sélectif relève de l'intérêt général[755]. Le législateur a décidé d'assouplir[756] ce principe afin de permettre la création d'une nouvelle finalité de traitement, ultérieure à la récolte des données, à condition que la personne auprès de laquelle les données personnelles de santé ont été recueillies, ou à propos de laquelle ces données ont été transmises, soit directement informée de ce changement.

Ce mécanisme permet, en théorie, de procéder à un traitement de données personnelles de santé pour une finalité qui n'avait pas été prévue initialement. Mais dans la pratique, l'information de la personne, parfois plusieurs mois, voire plusieurs années, après que celle-ci ait donné son consentement au recueil et au traitement de ses données, peut être de nature à causer des difficultés.

278. L'un des changements amenés par la transposition de la directive de 1995[757] que nous nous devons de souligner est aussi la fin de la possibilité de traiter des « *données nominatives* » à des fins de recherche dans le domaine de la santé. Le chapitre IX, ex-chapitre V bis, parle désormais de données à caractère personnel. Dans ce cadre, la seule possibilité de réaliser un traitement de données personnelles qui seraient identifiantes – soit pas nécessairement nominatives

[753] Directive 95/46/CE du 24 octobre 1995, *op. cit.*, art. 10 b) ;

[754] KHODOSS H., « L'exploitation des données de santé », *RGDM*, 30/09/2004, n° 4, p. 65-76.

[755] *Supra* n° 52.

[756] Article 57 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[757] La directive 95/46/CE du 24 octobre 1995, *op. cit.*, a été transposée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

comme cela a été décrypté précédemment[758] – est d'effectuer ledit traitement en association avec des études de pharmacovigilance ou des protocoles de recherche réalisés en lien avec des études coopératives nationales ou internationales, ou encore si une particularité de la recherche l'exige[759]. Tout traitement de données personnelles à des fins de recherche dans le domaine de la santé qui comporterait une demande de dérogation au principe de cryptage des données identifiantes doit alors apporter une justification scientifique et technique et doit également indiquer combien de temps la recherche prendra. Priorité est donnée, une fois de plus, au droit au respect de la vie privée. Soulignons que, comme ce fut le cas pour les demandes de traitements à des fins d'évaluations ou d'analyse des pratiques ou des activités de soins et de prévention, la procédure d'autorisation de traitement de données personnelles à des fins de recherche dans le domaine de la santé n'a pas non plus été bouleversée par la loi du 6 août 2004[760]. En effet, le texte du chapitre IX de la loi relative à l'informatique et aux libertés[761] est presque identique à celui de l'ancien chapitre V bis de cette même loi.

279. Pendant 14 ans (de 2002 à 2016) la possibilité d'obtenir un accès sélectif a été cantonnée aux finalités d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention jusqu'à la réforme du 26 janvier 2016[762] qui permet aujourd'hui de viser des finalités de recherche, d'étude ou d'évaluation dans le domaine de la santé. Cet élargissement des finalités potentielles de traitement ne signifie pas pour autant que toutes les finalités sont autorisées dans le cadre du nouvel accès sélectif qui s'appuie sur les données du SNDS. Effectivement, la refonte totale de l'accès sélectif par la loi du 26 janvier 2016[763] propose une redéfinition des prérequis à respecter pour pouvoir prétendre accéder aux données de santé du SNDS. Le nouveau système créé par la réforme a notamment inséré dans le code de la santé publique

[758] *Supra* n° 36 à 39.

[759] Art. 55 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version issue de la loi n° 2004-801 du 6 août 2004, *op. cit*.

[760] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[761] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version issue de la loi n° 2004-801 du 6 août 2004, *op. cit*.

[762] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[763] *Ibid.*

l'article L.1461-1 qui propose une liste exhaustive des finalités autorisées[764], ainsi qu'une liste courte mais sans ambiguïté de finalités interdites[765].

280. Bien plus complète qu'auparavant, la description des finalités autorisées vise avant tout à dresser l'éventail des possibilités offertes par les données contenues dans le SNDS. La nouvelle philosophie du système semble aujourd'hui définitivement liée à l'utilisation des données dans un objectif d'intérêt général et de participation active de l'ensemble de la population à la démocratie sanitaire avec, par exemple, la deuxième finalité consistant à contribuer « *à la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale* ». Cette idée prépondérante était déjà bien présente plusieurs années avant la réforme de 2016 : sa mise en œuvre est l'aboutissement des réflexions[766] menées afin de libérer les données de santé en les rendant exploitables par le plus grand nombre tout en préservant la vie privée des individus. Nous pouvons remarquer que certaines autres finalités font directement écho à l'accès sélectif, notamment celles qui sont liées à « *la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales* », à « *la surveillance, à la veille et à la sécurité sanitaires* », mais aussi « *à 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* ». L'intérêt sous-jacent de ces finalités étendues, qui peuvent toutes entrer dans le cadre de traitements à

[764] Article L. 1461-1 III du code de la santé publique :

« *Le système national des données de santé a pour finalité la mise à disposition des données, dans les conditions définies aux articles L. 1461-2 et L. 1461-3, pour contribuer :*
1° A l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité ;
2° A la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale ;
3° A la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales ;
4° A l'information des professionnels, des structures et des établissements de santé ou médico-sociaux sur leur activité ;
5° A la surveillance, à la veille et à la sécurité sanitaires ;
6° A la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale. »

[765] Article L. 1461-1 V du code de la santé publique :

« *Les données du système national des données de santé ne peuvent être traitées pour l'une des finalités suivantes :*
1° La promotion des produits mentionnés au II de l'article L. 5311-1 en direction des professionnels de santé ou d'établissements de santé ;
2° L'exclusion de garanties des contrats d'assurance et la modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque. »

[766] MARTIAL-BRAZ. N. *in* LAVERDET C., « Données personnelles : bilan de 1995 et réforme de 2014 ? », *Revue Lamy du Droit de l'immatériel*, 01/05/2014, n° 104, p. 96 à 99 : « *Les questions d'open data ont également été évoquées par Nathalie Martial-Braz qui a souligné la nécessité d'ouvrir* [les] *bases de données pour la prévention des scandales sanitaires, la mise en place de politiques de soins, ainsi que le contrôle des politiques publiques et notamment des dépenses publiques de soins* ».

des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé autorisés dans le cadre de l'accès sélectif, réside également dans le potentiel innovant et économique pour les entreprises françaises : il s'agissait d'ailleurs de l'un des objectifs portés par le gouvernement à l'initiative de la réforme[767]. L'esprit qui émane du nouveau mécanisme d'accès sélectif est donc de proposer une plus grande marge de manœuvre dans les finalités de traitement, mais cette liberté a toutefois des limites.

281. Deux finalités de traitement sont ainsi spécifiquement exclues du cadre de l'accès sélectif aux données de santé. Nous ne ferons qu'évoquer l'existence de ces finalités interdites et les acteurs qui s'en trouvent affectés car elles concernent directement certains acteurs à but lucratif : la Partie III de la présente étude est, à ce titre, consacrée à l'analyse du fonctionnement de l'accès des acteurs à but lucratif aux données personnelles de santé[768].

La première finalité interdite vise explicitement les laboratoires pharmaceutiques qui auraient pu être tentés d'utiliser l'analyse des informations portant sur les consommations de médicaments par établissement de soins, par région, par département ou même par ville, afin de faire la publicité de produits de santé directement corrélés aux résultats de ces analyses : la loi est formelle, tout traitement de données issues de l'accès sélectif au SNDS pour une promotion de ce type à destination des professionnels de santé ou d'établissements de santé est interdite.

La seconde concerne les organismes ayant une activité d'assurance. En effet, ceux-ci auraient pu avoir l'envie d'exclure certaines garanties, ou de tarifer leurs contrats en fonction d'un risque identifié chez un individu ou un groupe d'individus. Tout traitement ayant pour objectif de déterminer des risques pouvant amener un organisme d'assurance à discriminer ses clients en fonction de tels critères est donc prohibé.

Ces deux interdictions directement énoncées par la loi se rencontrent finalement dans un objectif commun : protéger les individus, les professionnels de santé et les établissements de soins par l'interdiction de l'utilisation de l'accès sélectif à des fins commerciales. Il s'agit là

[767] PELLERIN F. *in* DEBOST C., « Quand les traitements de données relatives à l'état de santé sont légitimés par les plus hautes institutions françaises », *op. cit.*

[768] V. Partie III.

d'une première étape dans la responsabilisation des bénéficiaires de l'accès sélectif. Le SNDS leur devient accessible, mais c'est sur leurs épaules que repose la responsabilité de respecter les limites imposées, sous peine d'être sanctionnés plus durement qu'auparavant[769].

282. Par-delà les finalités autorisées ou interdites, qui exercent une première barrière au bénéfice de l'accès sélectif, de grands principes généraux ont également été définis.

B) Les principes généraux de l'accès sélectif

283. Nous venons de l'aborder[770], la directive de 1995[771] prévoit un principe d'interdiction de collecte et de traitement de données personnelles de santé tout en proposant une liste de dérogations à cette interdiction. Mais ce texte ne s'est pas limité à cela, il rappelle également avec précision les principes qui doivent gouverner la mise en œuvre de tels traitements : loyauté, licéité, exactitude, finalité[772] et sécurité. Ces principes étaient déjà présents dans la loi relative à l'informatique et aux libertés comme le faisait remarquer I. de LAMBERTERIE en 1996[773]. De manière similaire, la directive confère aux personnes des droits spécifiques déjà prévus en droit français à l'image de l'obtention de leur consentement, de la mise en œuvre d'un droit de rectification ou même d'opposition. L'auteure remarque avec intérêt l'opportunité laissée par la directive aux Etats membres, et donc à la France, de proposer des exceptions à l'obligation d'information de l'individu producteur des données : tel est le cas des traitements ayant pour fin la recherche dans le domaine de la santé prévus en droit français dès la loi de 1994[774]. Dès lors, se posait déjà la question de savoir si le législateur allait profiter de cet aval du droit européen, communautaire en son temps, pour définir de nouvelles dérogations au principe d'information et de consentement. Une évolution de ce type ne pouvait toutefois se faire qu'à la condition de fournir un cadre juridique sûr et approprié afin d'assurer le respect de la vie

[769] *Infra* n° 292.

[770] *Supra* n° 274.

[771] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[772] *Supra* n° 273 à 282.

[773] de LAMBERTERIE I., « Protection de la vie privée et traitement des données relatives à la santé à l'heure européenne », *Médecine et droit*, 01/09/1996, n° 20, p. 6-12.

[774] Loi n° 94-548 du 1 juillet 1994 *op. cit.*

privée. C'est pour cette raison qu'I. de LAMBERTERIE s'exclamait « *si toutes les garanties sont réunies, il faut espérer que la transposition de la directive ira dans ce sens !* »[775].

284. La directive[776] devait être transposée par les Etats membres dans un délai de trois ans à compter de son adoption[777]. Il y avait donc tout lieu de penser que le législateur français était prêt à prendre les mesures nécessaires pour adapter la loi relative à l'informatique et aux libertés[778] avant le 24 octobre 1998. Pourtant, comme nous l'avons évoqué précédemment[779], ce n'est que près de neuf ans plus tard que ladite directive est finalement entrée en vigueur en France. Entre temps, une réflexion intense a été menée sur les possibilités offertes par les dérogations permises par le droit communautaire. Le Groupe européen d'éthique des sciences et des nouvelles technologies a ainsi émis un avis[780] sur les grands principes qui régissent le traitement de données personnelles de santé. Des chercheurs se sont également employés à décrypter[781] l'inépuisable question de la protection de ces données. Toute évocation d'un traitement de données personnelles de santé implique la mise en avant de la protection du droit au respect de la vie privée. Remarquons que sur la question des systèmes d'information permettant de traiter les données, le sujet crucial de leur sécurité est bien souvent directement lié à une problématique d'éthique car c'est d'abord cette sécurité qui permet d'assurer le respect de la vie privée. Si des dérogations à l'interdiction de traitement des données personnelles sont permises, le Groupe européen d'éthique des sciences et des nouvelles technologies souligne que des impératifs de cryptage des données, de spécialisation des réseaux de transmission de ces données, ou encore de surveillance constante de la fiabilité des systèmes et réseaux doivent prévaloir sur les traitements eux-mêmes. Le message est on ne peut plus clair : les Etats membres sont invités à la plus grande vigilance dans les autorisations de traitements de données personnelles de santé qu'ils accordent de manière dérogatoire.

---

[775] de LAMBERTERIE I., « Protection de la vie privée et traitement des données relatives à la santé à l'heure européenne », *op. cit.*, p. 10.

[776] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[777] *Ibid.* v. article 32, paragraphe 1.

[778] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[779] *Supra* n° 245.

[780] Commission européenne, « Avis n° 13 du 30 juillet 1999 : Aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information », *Journal international de bioéthique*, 2001/3, vol. 12, p. 113-117.

[781] MARLIAC-NEGRIER C., « La protection des données nominatives informatiques en matière de recherche médicale, Thèse de doctorat en Droit public soutenue en 1999 à Clermont Ferrand 1 », *Presses Universitaires d'Aix – Marseille*, 2001, 844 p.

285. La loi du 6 août 2004[782] a su tenir compte des apports européens mais aussi des débats et enjeux éthiques nés à l'orée des années 2000. Elle a ainsi modifié la loi relative à l'informatique et aux libertés[783] pour donner une liste complète des principes devant régir le traitement des données à caractère personnel. Nous y retrouvons des principes plus nombreux et développés que ceux de la directive : la collecte et le traitement loyaux et licites ; les finalités[784] déterminées, explicites et légitimes ; les caractères adéquat, pertinent et non excessif des données au regard des finalités de traitement ; l'exactitude des données ; et enfin les modalités de conservation des données. Ces grands principes doivent être respectés pour tout traitement de données à caractère personnel, de surcroît lorsqu'il s'agit de traitement de données sensibles effectuées dans le cadre de l'accès sélectif.

286. Cette définition des principes à respecter est restée la norme et n'a pas été modifiée par la réforme du 26 janvier 2016[785]. Cependant, des principes propres à l'accès sélectif dans le cadre du SNDS ont été créés à l'article L. 1461-1 IV du code de la santé publique[786] et doivent être impérativement respectés par les bénéficiaires dudit accès. Deux de ces principes sont particulièrement importants : le fait que les « *personnes responsables* [des traitements utilisant des données à caractère personnel issues du SNDS], *ainsi que celles les mettant en œuvre ou autorisées à accéder aux données à caractère personnel qui en sont issues, sont soumises au secret professionnel* » et celui selon lequel « *l'accès aux données s'effectue dans des conditions*

[782] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[783] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, art. 6., dans sa version issue de la loi n° 2004-801 du 6 août 2004, *op. cit.*

[784] *Supra* n° 273 à 282.

[785] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[786] Art. L. 1461-1 IV du code de la santé publique :

« *Pour le système national des données de santé et pour les traitements utilisant des données à caractère personnel issues de ce système :*
1° Aucune décision ne peut être prise à l'encontre d'une personne physique identifiée sur le fondement des données la concernant et figurant dans l'un de ces traitements ;
2° Les personnes responsables de ces traitements, ainsi que celles les mettant en œuvre ou autorisées à accéder aux données à caractère personnel qui en sont issues, sont soumises au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pénal ;
3° L'accès aux données s'effectue dans des conditions assurant la confidentialité et l'intégrité des données et la traçabilité des accès et des autres traitements, conformément à un référentiel défini par arrêté des ministres chargés de la santé, de la sécurité sociale et du numérique, pris après avis de la Commission nationale de l'informatique et des libertés ;
4° Les données individuelles du système national des données de santé sont conservées pour une durée maximale de vingt ans, sans préjudice de l'application du deuxième alinéa de l'article 36 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. »

assurant la confidentialité et l'intégrité des données et la traçabilité des accès et des autres traitements »[787]. Si ces précisions ne sont pas des nouveautés en termes de sécurisation des données de santé transmises, elles sont un indicateur clef de la place prépondérante de la protection de la vie privée parmi les fondements du nouvel accès sélectif. L'impact est immédiat sur les demandeurs d'accès aux données qui doivent se préparer, en amont de l'autorisation éventuelle, à la mise en œuvre de procédures adaptées afin de respecter la loi. Quelques illustrations de la mise en pratique de ces principes peuvent être donnés. Par exemple, dans le cas où le traitement de données issues du SNDS nécessiterait des appariements avec d'autres données de santé, le responsable de traitement doit apporter la preuve que lesdits appariements sont rendus « *strictement nécessaires par les finalités de la recherche, de l'étude ou de l'évaluation* »[788]. Qui plus est, tout demandeur de l'accès sélectif, sans distinction, est soumis à deux prérequis inévitables[789] avant d'obtenir un quelconque accès aux données personnelles de santé du SNDS. Le premier est la communication par le demandeur de plusieurs documents à l'Institut national des données de santé : il doit transmettre l'étude, ou l'évaluation, de l'autorisation délivrée par la CNIL ; il doit aussi faire part d'une déclaration de ses intérêts en lien avec l'objet du traitement ; et il doit transmettre le protocole d'analyse incluant la description des moyens mis en œuvre pour en évaluer la validité et les résultats. Le second prérequis est un engagement ferme du demandeur de communiquer à l'INDS les résultats de l'étude menée accompagnée des moyens d'en évaluer la validité. L'INDS est ensuite chargé de s'assurer de la publication de l'autorisation d'accès sélectif délivrée par la CNIL, de la déclaration d'intérêts et des résultats.

Soulignons que si tous les acteurs qui obtiennent un accès sélectif aux données de santé sont soumis à la loi relative à l'informatique et aux libertés et aux obligations qui en découlent[790], certaines catégories d'acteurs sont tenues d'apporter des garanties supplémentaires en renfort de leur dossier : ce point précis concerne certains acteurs à but lucratif dont les modalités d'accès aux données de santé à caractère personnel sont étudiées dans la Partie III de cette étude[791]. Mais le législateur français ne s'est pas limité à définir ces principes et prérequis, nous

[787] Art. L. 1461-1 IV 2° et 3° du code de la santé publique.

[788] Art. L. 1461-3 al. 4 du code de la santé publique.

[789] Art. L. 1461-3 al. 12 et 13 du code de la santé publique.

[790] *Infra* n° 311 à 321.

[791] V. Partie III.

verrons ultérieurement que des dispositions propres à la procédure du nouvel accès sélectif renforcent la protection de la vie privée[792].

287. Cette revue des exigences préalables à l'autorisation d'accès sélectif aux données de santé nous éclaire finalement sur l'équilibre fragile qui existe entre l'organisation qui met en œuvre le traitement de données personnelles de santé et l'autorité qui a donné son autorisation : bien qu'un lien de confiance soit tissé entre les bénéficiaires de l'accès et l'autorité, des sanctions sont prévues pour dissuader toute volonté de contrevenir à la loi.

Paragraphe 2 : Les sanctions pesant sur les bénéficiaires de l'accès sélectif

288. Toute personne qui obtient l'autorisation de traiter des données de santé à caractère personnel se trouve soumise à l'application de plusieurs types de sanctions : des sanctions prononcées par la CNIL, mais aussi des sanctions prévues directement par le code pénal. De plus, sont aussi bien visées les personnes physiques que les personnes morales.

289. Avant la loi du 1er juillet 1994[793], la loi relative à l'informatique et libertés reproduisait directement les dispositions pénales applicables[794] aux personnes reconnues coupables de violations des articles de ladite loi. Les peines encourues pouvaient aller, selon les faits, de deux à cinq ans d'emprisonnement, et de 2 000 à 2 000 000 de francs. La loi du 1er juillet 1994[795] a conservé ce rappel des sanctions pénales encourues, qui avaient été remaniées par la loi du 16 décembre 1992[796], tout en rappelant la soumission des personnes appelées à connaître des données personnelles au secret professionnel sous les peines prévues à l'article 226-13 du code pénal[797].

---

[792] *Infra* n° 302 à 310.

[793] Loi n° 94-548 du 1 juillet 1994 *op. cit.*

[794] V. Chapitre VI de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version initiale.

[795] Loi n° 94-548 du 1 juillet 1994 *op. cit.*

[796] Loi n° 92-1336 du 16 décembre 1992 *relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur*, JORF n° 0298 du 23/12/1992.

[797] V. art. 40-3, al. 5 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifié par la loi n° 94-548 du 1 juillet 1994, *op. cit*.

290. Il faut attendre la loi du 6 août 2004[798] pour que la définition des sanctions pesant sur les bénéficiaires de l'accès sélectif soient mises à jour. Cette réforme donne à la CNIL un arsenal juridique[799] lui permettant de prononcer elle-même des sanctions tout en conservant les sanctions pénales. Ces sanctions sont prises à l'encontre du responsable de traitement (qui peut être une personne physique ou morale) et peuvent être de deux natures : la première est une sanction pécuniaire pouvant aller jusqu'à 150 000 euros pour le premier manquement, puis 300 000 euros pour les manquements suivants (ou 5% du chiffre d'affaires hors taxe de la personne morale dans la limite de 300 000 euros). La seconde est une injonction de cesser le traitement. S'agissant de ce deuxième type de sanction, le législateur permet à la CNIL de décider d'interrompre un traitement et de verrouiller tout ou partie des données traitées : une telle décision ne peut être prise qu'en cas de violation caractérisée des droits et libertés défendus par la loi relative à l'informatique et aux libertés[800].

291. En complément de ces nouvelles prérogatives de la CNIL, des dispositions pénales sont toujours imposées aux bénéficiaires de l'accès sélectif. Ainsi, le chapitre VIII de la loi relative à l'informatique et aux libertés[801] renvoie en premier lieu aux articles 226-16 à 226-24 du code pénal[802], puis précise les sanctions pénales encourues en cas d'entrave à l'action de la Commission : la peine prévue dans ce cas est un an d'emprisonnement et 15 000 euros d'amende.

Nous pouvons souligner que la référence au traitement de « *données nominatives* » qui existait aux articles 226-16 à 224-24 du code pénal a également été supprimée et remplacée par la notion de « *données à caractère personnel* » grâce à la loi du 6 août 2004[803]. Comme le rappelle le rapport BRAS[804], ces dispositions sont mises à jour et peuvent pleinement s'appliquer aux

[798] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[799] V. chap. VII de la loi n° 78-17 du 6 janvier 1978, *op. cit.,* dans sa version issue de la loi n° 2004-801 du 6 août 2004, *op. cit*.

[800] Il s'agit des droits et liberté suivants : l'identité humaine, les droits de l'homme, la vie privée, les libertés individuelles ou publiques. V. art. 1 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*

[801] V. chap. VIII de la loi n° 78-17 du 6 janvier 1978, *op. cit.,* dans sa version issue de la loi n° 2004-801 du 6 août 2004, *op. cit*.

[802] Les articles 226-16 à 226-24 du code pénal constituent la Section 5 du Chapitre VI du Titre II du Livre II de la Partie législative intitulée « *Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques* ».

[803] Loi n° 2004-801 du 6 août 2004, *op. cit*

[804] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.,* p. 30.

traitements autorisés dans le cadre de l'accès sélectif. En effet, rappelons que l'accès sélectif ne peut en aucun cas être autorisé dans le cadre du traitement de données nominatives : ces données doivent nécessairement être pseudonymisées ou anonymisées. La conséquence majeure de cette nouveauté est que le responsable d'un traitement autorisé dans le cadre de l'accès sélectif se trouve directement concerné par les dispositions pénales : peuvent peser sur lui, pour chaque infraction avérée, une amende allant jusqu'à 300 000 euros couplée à une peine de prison maximale de cinq ans. Cela signifie que si le responsable de traitement est reconnu coupable de plusieurs infractions, les amendes et peines d'emprisonnement peuvent se cumuler.

Au-delà du chapitre VIII dédié aux dispositions pénales, la référence au respect du secret professionnel prévu par l'article 226-13 du code pénal est spécifiquement inscrite dans le chapitre X de la loi relative à l'informatique et aux libertés[805]. Rappelons que ce chapitre est justement celui qui fait référence dans le cadre de l'accès sélectif en vigueur avant la réforme du 26 janvier 2016.

292. Conscient que certains montants d'amende infligés par la CNIL pouvaient parfois être dérisoires[806] pour certains bénéficiaires de l'accès sélectif, le législateur a augmenté la peine prononçable par la Commission. Le changement n'est pas venu de la loi du 26 janvier 2016[807] mais de la loi du 7 octobre 2016 : elle a permis de réévaluer le montant maximum de l'amende qui est passé de 300 000 euros à 3 millions d'euros[808]. Cependant, il semble que cette amende maximale reste insuffisamment contraignante et une augmentation a, une fois de plus, été opérée. Cette modification est venue du droit européen qui, par le Règlement général relatif à la protection des données[809] signé en 2016 et entré en vigueur le 25 mai 2018, a élevé le montant maximum des amendes potentielles qui est passé de 3 millions d'euros à 10 millions d'euros, ou 2% du chiffre d'affaires mondial lorsqu'il s'agit d'une entreprise (le montant le plus élevé

[805] La référence à l'article 226-13 du code pénal est présente dans le chapitre X, art. 66 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version issue de la loi n° 2004-801 du 6 août 2004, *op. cit.* Aujourd'hui, cette référence est retrouvée à l'article 68 de la loi modifiée par loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[806] Le montant maximum d'amende de 300 000 euros reste très limité et peu dissuasif pour une personne morale, même si elle n'a pas un but lucratif.

[807] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[808] V. art. 47 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifié par la loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique*, JORF n° 0235 du 08/10/2016.

[809] Règlement 2016/679, *op. cit.*, art. 83.

étant retenu), et dans certains cas bien spécifiques, à 20 millions d'euros, ou 4% du chiffre d'affaires mondial lorsqu'il s'agit d'une entreprise[810] (le montant le plus élevé étant retenu).

293. Nous le comprenons, le bénéfice de l'accès sélectif est très loin de ressembler à une simple formalité administrative et impose de la part des acteurs, une prise de conscience de la responsabilité qui leur incombe : l'objectif essentiel des sanctions prévues par la loi demeure la protection de la vie privée des individus à travers l'assurance que la sécurité de leurs données de santé à caractère personnel ne sera pas violée. L'effectivité de ces mesures implique cependant que les moyens techniques et humains soient suffisamment importants pour parvenir à relever les infractions, les constater et instruire les dossiers jusqu'à leur terme. Ce prérequis est, malheureusement, l'une des failles de l'accès sélectif en raison des limites pratiques de l'application des sanctions[811] et, par extension, de l'ensemble des traitements de données personnelles, qui pourrait expliquer[812] la frilosité des autorités dans la facilitation de l'accès aux données de santé.

294. L'obtention de l'accès sélectif répond finalement à des contraintes importantes caractérisées par un encadrement strict des finalités envisagées, des principes à respecter, et des sanctions encourues en cas de non-respect de ces règles. Quelles que soient les obligations et sanctions qui pèsent sur le bénéficiaire de l'accès sélectif, ce sont l'intérêt général et la protection de la vie privée des individus qui demeurent au centre du dispositif : bien qu'un lien de confiance se tisse entre les demandeurs et les autorités, son fonctionnement ne saurait être bon qu'à la condition qu'un équilibre soit trouvé entre les opportunités offertes par le traitement des données de santé à caractère personnel, pouvant déboucher sur des abus, et le caractère dissuasif des sanctions. A ce titre, l'entrée en vigueur du nouveau Règlement européen[813] et l'application de la réforme du 26 janvier 2016[814] tentent de modifier ce rapport qui existe entre les demandeurs et les autorités en proposant un système plus permissif, dans la pratique, pour

[810] L'article 83, points 4 et 5 du Règlement 2016/679, *op. cit.*, propose une gradation de l'amende administrative encourue selon la nature de la violation caractérisée.

[811] *Infra* n° 434 et 435.

[812] Pour retrouver notre analyse du contrôle par les autorités administratives des traitements de données à caractère personnel, v. *infra* n° 311 à 321.

[813] Règlement 2016/679, *op. cit.*

[814] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

les bénéficiaires de l'accès sélectif[815]. La contrepartie prévue par cette responsabilisation est le durcissement des sanctions encourues.

295. La mise en œuvre de l'accès sélectif s'est donc développée depuis sa création en contrepartie de garanties fournies par les bénéficiaires afin de contrôler leur ambition dans le traitement des données de santé. L'étude du fonctionnement de l'accès sélectif serait toutefois incomplète si les procédures d'autorisation et de contrôle n'étaient pas abordées.

[815] Retrouvez l'analyse du nouveau paradigme mis en œuvre dans le cadre de l'accès sélectif aux données de santé *infra* n° 330 à 343.

CONCLUSION DU CHAPITRE I

296. La possibilité d'accéder aux données de santé des bases médico-administratives et de les traiter s'est construite très prudemment à partir du premier arrêté relatif au SNIIRAM de 2002[816]. Cette construction a surtout été divisée en deux grandes thématiques : d'un côté il est question de savoir qui peut bénéficier de l'accès permanent ; de l'autre ce sont les conditions d'accès aux données qui interrogent. La prudence repose avant tout sur la volonté d'empêcher tout risque d'atteinte au droit au respect de la vie privée des individus. Mais, nous l'avons vu, la définition de l'accès sélectif, tant dans sa démarche que dans les données auxquelles il permet d'accéder est marquée par une instabilité importante. Dès 2005[817], le champ des bénéficiaires potentiels de l'accès sélectif s'est ainsi rétréci pour n'inclure que les organismes de recherche ou toute structure d'enseignement liée à la recherche, à condition qu'ils n'aient pas de but lucratif. Ce principe est resté en vigueur jusqu'à la refonte du système d'accès aux données de santé en 2016[818].

297. Dans le même temps, pour garder un contrôle sur le parcours des données de santé et leur traitement dans le cadre de l'accès sélectif, chaque bénéficiaire est tenu, depuis la loi du 6 août 2004[819], de désigner un responsable de traitement chargé de la sécurité des données. Les bénéficiaires de l'accès sélectif sont également invités à désigner un CIL afin de faciliter les interactions avec la CNIL. Aujourd'hui cette fonction de CIL s'est transformée et renforcée en la personne du DPO, issu de l'application du Règlement général relatif à la protection des données[820]. Le législateur a donc créé un ensemble de mesures pour conserver un moyen de contrôler les acteurs qui entrent dans le cadre de l'accès sélectif : le fait d'avoir des interlocuteurs identifiés au sein de chaque structure est de nature à favoriser le dialogue et à prévenir les procédures éventuelles de vérification.

298. Au-delà de la restriction de l'accès sélectif par la sélection des acteurs qui peuvent en bénéficier, le respect des finalités autorisées de traitement et des principes régissant l'accès aux

[816] Arrêté du 11 avril 2002, *op. cit*.

[817] Arrêté du 20 juin 2005, *op. cit.*

[818] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[819] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[820] Règlement 2016/679, *op. cit.*

données de santé sont des éléments incontournables. Historiquement, l'accès aux données de santé des bases médico-administratives n'est autorisé qu'à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention dans le domaine de la santé. Ces finalités ont été élargies en 2016[821] à toutes les finalités de recherche, d'étude ou d'évaluation en santé présentant un caractère d'intérêt général. Cet élargissement a aussi donné lieu à la création de des finalités strictement interdites[822]. Aujourd'hui, la réforme dédiée à l'organisation et à la transformation du système de santé[823] ne conserve que le critère d'intérêt général : la finalité de recherche, pourtant perçue comme indispensable par les auteurs de la réforme de 2016, a disparu.

Les principes encadrant le traitement de données personnelles définis par le droit européen s'appliquent, eux, systématiquement aux données de santé. La loi du 26 janvier 2016[824] est toutefois venue apporter des principes propres aux traitements de données issues du SNDS : ces principes imposent notamment le respect du secret professionnel et l'obligation de veiller à la sécurité des données de santé.

299. Enfin, les mesures encadrant l'accès sélectif aux données de santé s'accompagnent de sanctions en cas de violation caractérisée. Ces sanctions sont devenues véritablement dissuasives avec l'entrée en vigueur du Règlement général relatif à la protection des données[825] : les amendes peuvent atteindre, en fonction du manquement constaté, entre 10 millions et 20 millions d'euros s'agissant des acteurs publics ou privés à but non lucratif.

Les acteurs concernés par l'accès sélectif aux données de santé sont donc étroitement sélectionnés et contrôlés depuis la création des premiers accès au SNIIRAM. Les traitements qu'ils envisagent de réaliser ne peuvent être mis en œuvre qu'à la condition qu'ils se conforment à l'ensemble des dispositions prévues par les droits européen et national. L'élargissement de l'accès sélectif depuis 2016 s'est aussi accompagné d'un durcissement des sanctions possibles en cas de mauvais comportement. Mais nous allons constater que c'est véritablement la

[821] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[822] Les finalités interdites sont traitées *infra* n° 496.

[823] Projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019.

[824] *Ibid.*

[825] Règlement 2016/679, *op. cit.*

procédure d'accès aux données de santé qui constitue l'épreuve principale que les demandeurs de l'accès sélectif doivent passer pour en devenir bénéficiaires.

CHAPITRE II
L'ACCÈS SÉLECTIF SOUMIS À UNE PROCÉDURE PROTECTRICE DE LA VIE PRIVÉE

300. Un mécanisme d'autorisation préalable pour accéder aux données de santé de l'Assurance maladie existait[826] déjà avant la création du SNIIRAM, dans un but de recherche respectueux de la vie privée des individus. Toutefois c'est avec la mise en ligne de toutes les données de soins de ville et de soins d'hospitalisation que le législateur s'est réellement investi dans la création d'une norme encadrant les modalités d'accès à ces données. Nous nous intéresserons à la nature des conditions imposées aux demandeurs d'accès avant la réforme mise en œuvre en 2016 (Section 1) puis nous analyserons l'assouplissement de ces conditions devenues, à certains égards, moins contraignantes avec la réforme du 26 janvier 2016[827] (Section 2).

SECTION 1 : LA NATURE CONTRAIGNANTE DE LA PROCÉDURE D'ACCÈS SÉLECTIF

301. Le dispositif d'accès sélectif aux données de santé s'est construit en plusieurs années. Le mécanisme qui a longtemps prévalu en droit français se décompose en deux catégories bien distinctes afin d'adapter les exigences de protection de la vie privée au type de traitement envisagé (§1). La spécificité de l'accès sélectif réside également dans les modalités de contrôle mises en œuvre afin de garantir la protection des données (§2).

Paragraphe 1 : La structure binaire de l'accès sélectif aux données de santé

302. Avant même la création du SNIIRAM, le traitement de données de santé était encadré. Dès la loi du 1er juillet 1994 créant le chapitre V bis dans la loi relative à l'informatique et aux libertés[828], les traitements de données de santé pouvaient être autorisés dans un seul objectif : la recherche dans le domaine de la santé. Dans ce cadre, toutes les demandes de traitement étaient systématiquement soumises à la même procédure. Tout d'abord, le comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé

[826] Loi n° 94-548 du 1 juillet 1994 *op. cit.*

[827] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[828] Loi n° 94-548 du 1 juillet 1994, *op. cit.*, qui a créé le chapitre V bis de la loi n° 78-17 du 6 janvier 1978, *op. cit.*

(CCTIRS[829]) était invité à rendre son avis. Cet avis devait impérativement être sollicité avant l'intervention de la CNIL. Ainsi, le CCTIRS avait un mois pour se prononcer, son silence équivalait à un avis favorable. Il revenait finalement à la CNIL d'autoriser ou d'interdire le traitement. Mais les dispositions légales ne s'arrêtaient pas à ce simple point de procédure : plusieurs articles de loi portaient surtout sur les droits des individus à l'égard de ces traitements et posaient les fondations qui sont toujours à la base de notre SNDS actuel. A titre d'exemple, les personnes devaient être informées de l'existence du traitement, de leur finalité, des personnes physiques ou morales éventuellement destinataires des données ainsi que de leurs droits d'accès et de rectification des données, d'opposition au traitement. L'aspect technique de la protection de la vie privée n'était pas en reste car si les données permettaient « *l'identification des personnes, elles* [devaient] *être codées avant leur transmission* » et le « *responsable de la recherche* [… veillait] *à la sécurité des informations et de leur traitement ainsi qu'au respect de la finalité de celui-ci* ». Même si des dérogations à cette pseudonymisation des données étaient possibles, le principe restait bien la protection des individus.

303. Puis, avec l'ambition de créer le SNIIRAM, concrétisée par la loi de financement de la sécurité sociale de 1998[830], la construction juridique de l'accès sélectif aux données de santé s'est fondée sur deux procédures, par moment complémentaires, d'abord prévues par les articles V bis[831] et V ter de la loi relative à l'informatique et aux libertés. Le chapitre V bis ayant déjà été présenté au point précédent, il convient d'aborder le chapitre V ter. Ce chapitre, créé par l'article 41 de la loi portant création de la couverture maladie universelle[832] a mis en place la possibilité de traiter les données personnelles de santé à des fins d'évaluation ou d'analyse des activités de soins et de prévention, complétant ainsi la « *panoplie* » des traitements possibles. Rappelons que l'arrêté du 22 avril 2002[833] y faisait directement référence[834]. La procédure créée par ce chapitre dispose que la CNIL étudie le dossier du demandeur en commençant par les

[829] Le CCTIRS a été initialement défini par l'article 40-2 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, puis par l'article 54 de cette même loi suite à l'entrée en vigueur de la loi n° 2004-801 du 6 août 2004, *op. cit.* Composé de « *personnes compétentes en matière de recherche dans le domaine de la santé, d'épidémiologie, de génétique et de biostatistique* », le CCTIRS avait pour mission de se prononcer sur « *la méthodologie de recherche au regard des dispositions de la* [loi relative à l'informatique et aux libertés], *la nécessité du recours à des données à caractère personnel et la pertinence de celles-ci par rapport à l'objectif de la recherche* ».

[830] Loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale pour 1999, *op. cit.*

[831] *Supra* n° 302.

[832] Loi n° 99-641 du 27 juillet 1999 *op. cit.*

[833] Arrêté du 11 avril 2002, *op. cit.*

[834] *Supra* n° 252 et 253.

garanties qu'il apporte et en vérifiant la conformité de sa demande à ses missions ou à son objet social. La Commission doit s'assurer que la demande d'accès sélectif aux données de santé à caractère personnel est bien nécessaire et pertinente. Elle doit aussi examiner le contenu des données personnelles dont le traitement est prévu afin de confirmer qu'elles ne comportent « *ni le nom, ni le prénom des personnes concernées, ni leur numéro d'inscription au Répertoire national d'identification des personnes physiques* ». Dans le cadre de cette procédure d'autorisation, la CNIL peut interdire la transmission de certaines données personnelles si elle estime que ces données ne sont pas nécessaires pour le traitement envisagé. C'est aussi la CNIL qui fixe la durée de conservation des données et donne son avis sur les mesures prises par le demandeur pour assurer leur sécurité. Enfin, le chapitre V ter donne à la Commission deux mois pour se prononcer, renouvelable une fois. Il est bien précisé, dans un souci de sécurité inhérent à la protection de la vie privée, que le silence de cette autorité vaut rejet de la demande d'accès sélectif.

304. Les chapitres V bis et V ter ont, par l'adoption de la loi du 6 août 2004 transposant la directive de 1995[835], été transférés et intégrés dans deux nouveaux chapitres de la loi relative à l'informatique et aux libertés[836] : le chapitre V bis est devenu le chapitre IX relatif aux traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé – notons la suppression de la mention « *données nominatives* »[837] – et le chapitre V ter est devenu le chapitre X relatif aux 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. Dans le même temps, la procédure de référence en cas de demande d'accès sélectif a été transférée du chapitre V ter au chapitre X par l'arrêté de 2005[838].

305. Le chapitre X n'a pas révolutionné le fonctionnement de l'accès sélectif aux données de santé du SNIIRAM : les dispositions sont, à quelques mots prêts, identiques à celles de l'ancien chapitre V ter créé en 1999[839]. Nous y retrouvons le principe de mise à disposition des données sous « *forme de statistiques agrégées ou de données par patient constituées de telle sorte que*

[835] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[836] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[837] V. plus haut notre analyse de l'impact des termes « données nominatives » *supra* n° 273.

[838] Arrêté du 20 juin 2005, *op. cit.*

[839] Loi n° 99-641 du 27 juillet 1999 *op. cit.*

les personnes concernées ne puissent être identifiées ». La CNIL demeure l'interlocuteur principal des demandeurs d'accès aux données de santé : elle est toujours chargée de vérifier la constitution des données personnelles transmises aux demandeurs et dispose bien de la faculté d'interdire la transmission de certaines données si le demandeur n'apporte pas *« d'éléments suffisants pour attester la nécessité de disposer de certaines informations parmi l'ensemble des données à caractère personnel dont le traitement est envisagé* ». Le même constat peut être dressé à l'égard du chapitre IX qui n'est que la nouvelle numérotation de l'ancien chapitre V bis.

En parcourant la loi, nous comprenons que toute la procédure d'accès sélectif aux données personnelles de santé est encadrée dans le but de protéger la vie privée des individus. Nous constatons surtout que l'ensemble de cette procédure repose sur les épaules de la CNIL qui prend, quasiment seule, la responsabilité d'autoriser les traitements. Ce rôle central pourrait d'ailleurs avoir eu des conséquences sur le nombre d'autorisations d'accès aux données personnelles de santé finalement accordées[840].

306. Conscient de cela, le pouvoir réglementaire a apporté un soutien à la CNIL en la personne de l'Institut des données de santé (IDS), groupement d'intérêt public créé en 2004[841]. L'arrêté relatif au SNIIRAM de 2005[842] précise ainsi que tout demande d'accès aux données de santé du SNIIRAM à des fins de traitement provenant de structures ne bénéficiant pas de l'accès permanent[843] doit être approuvée par le conseil d'administration de l'Institut des données de santé. Cet Institut avait pour mission principale de « *veiller à la qualité des systèmes d'information utilisés pour la gestion du risque maladie et de veiller à la mise à disposition* […] *des données issues des systèmes d'information de ses membres, dans des conditions garantissant l'anonymat* »[844]. Cependant, comme nous le verrons plus tard[845], cette étape préalable à l'examen des dossiers par la CNIL n'a pas été immédiatement mise en œuvre.

---

[840] *Infra* n° 385 à 390 et n° 398.

[841] Loi n° 2004-810 du 13 août 2004, *op. cit.*, art. 64.

[842] Arrêté du 20 juin 2005, *op. cit.*

[843] Pour l'analyse des bénéficiaires de l'accès sélectif, v. *supra* n° 251 à 260.

[844] Art. 161-36-5 du code de la sécurité sociale dans sa version issue de la loi n° 2004-810 du 13 août 2004, *op. cit.*

[845] *Infra* n° 326.

307. En revanche, un élément capital de procédure a été créé par un décret de 2005[846]. Il s'agit du décret qui organise le fonctionnement de la CNIL, notamment dans le cadre de l'examen des dossiers de demandes de traitement de données personnelles de santé prévues par les chapitre IX et X de la loi relative à l'informatique et aux libertés[847]. Ce décret donne ainsi une description précise du contenu attendu dans le dossier du demandeur d'accès[848]. Doivent notamment être donnés à la Commission l'identification du responsable de traitement avec ses coordonnées, ses missions, les personnes qui auront accès aux données, un descriptif de la finalité du traitement et de la population qu'il vise, la durée souhaitée de conservation des données, ou encore les dispositions prises pour assurer la sécurité du traitement. Le document donne toutes les clefs aux demandeurs pour transmettre à la Commission un dossier complet afin qu'il soit examiné dans les délais définis par la loi.

308. Avant d'aller plus loin dans notre réflexion, une question d'ordre théorique mérite d'être posée : pourquoi nous sommes-nous intéressés aux chapitres V bis et V ter, devenus IX et X, alors que l'accès sélectif aux données de santé prévu par l'arrêté de 2002[849], puis par les arrêtés publiés depuis 2005[850], renvoient spécifiquement à l'unique procédure prévue par le chapitre V ter devenu chapitre X ?

---

[846] Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[847] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[848] Aux termes de l'article 41 du décret n° 2005-1309 du 20 octobre 2005, *op. cit.*, voici les informations à faire figurer dans le dossier à transmettre à la CNIL :

« *1° L'identité et l'adresse du responsable du traitement et s'il n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de la Communauté européenne celles de son représentant en France ; les missions ou l'objet social de l'organisme dont il relève ; les catégories de personnes qui auront accès aux données ;*
2° Un descriptif de la finalité du traitement et de la population qu'il concerne ; la nature des données dont le traitement est envisagé et la justification du recours à celles-ci ; la durée souhaitée de leur conservation et leurs méthodes d'analyse ; l'identification des personnes, services ou organismes qui en sont détenteurs et qui sont susceptibles de les communiquer au demandeur si celui-ci est autorisé à mettre en œuvre le traitement ; le type de diffusion ou de publication des résultats du traitement envisagé, le cas échéant, par le demandeur ;
3° Les caractéristiques techniques du traitement ;
4° Les rapprochements ou interconnexions envisagés ou toute autre forme de mise en relation des informations ;
5° Les dispositions prises pour assurer la sécurité des traitements et des informations et la garantie des secrets protégés par la loi ;
6° Le cas échéant, la mention de toute transmission de données à caractère personnel vers un Etat n'appartenant pas à la Communauté européenne ;
7° Le cas échéant, la liste des traitements répondant aux caractéristiques prévues au deuxième alinéa de l'article 65 de la loi du 6 janvier 1978 susvisée ; le dossier précise, en ce cas, les catégories de données, les destinataires ou les catégories de destinataires. »

[849] Arrêté du 11 avril 2002, *op. cit.*

[850] Arrêté du 20 juin 2005, *op. cit.*

Tout simplement parce qu'un acteur peut demander à obtenir des données de santé à caractère personnel afin de les utiliser pour un traitement relevant de la finalité prévue par le chapitre IX[851]. Dans un tel cas de figure, le demandeur est d'abord soumis à la procédure prévue dans le cadre de l'accès sélectif, puis doit par la suite se plier à la procédure spécifique au type de traitement qu'il souhaite mettre en œuvre. Ainsi, en plus de l'examen préalable du dossier par l'Institut des données de santé (IDS), dont l'intervention a été introduite par l'arrêté de 2005[852], le CCTIRS[853] est aussi invité à rendre son avis sur la méthodologie de la recherche. Le déroulement de ce processus implique donc un délai supplémentaire car rappelons que le CCTIRS disposait d'un mois pour transmettre son avis.

309. De 2004, année de mise en conformité du droit français avec le droit européen, à 2016, année du vote de la loi de modernisation de notre système de santé[854] et du Règlement pour la protection des données[855], le chapitre X de la loi relative à l'informatique et aux libertés est resté l'unique point d'entrée de l'accès sélectif aux données de santé du SNIIRAM. Nous aborderons ultérieurement[856] les apports et perspectives des dispositions adoptées en 2016. Mais nous pouvons d'ores et déjà remarquer que le législateur français, contrairement à son retard de transposition manifeste du droit européen dans le courant des années 1990, a cette fois-ci pris les devants en proposant une refonte complète de l'accès sélectif aux données personnelles de santé alors même que le nouveau cadre européen n'était pas encore voté. Ces propos peuvent malgré tout être minorés car la réforme portée par la ministre M. TOURAINE, et plus particulièrement l'article 193 de la loi, est le fruit de plusieurs années d'études, rapports et réflexions portant directement sur l'amélioration de l'accès sélectif dans un cadre respectueux de la vie privée. Cependant, le Règlement européen entré en vigueur le 25 mai 2018[857] a eu un impact que les rédacteurs de la réforme du 26 janvier 2016[858] n'avaient pas entièrement prévu.

[851] Rappelons que le chapitre IX de la loi n° 78-17 du 6 janvier 1978, *op. cit*,. modifiée par la n° 2004-810 du 13 août 2004, *op. cit*.,vise les traitements « *ayant pour fin la recherche dans le domaine de la santé* ».

[852] S*upra* n° 306.

[853] *Supra* n° 302.

[854] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[855] Règlement 2016/679, *op. cit.*

[856] *Infra* n° 330 à 336.

[857] Règlement 2016/679, *op. cit.*

[858] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

310. A l'issue de cette présentation des modalités d'autorisation des traitements de données personnelles de santé à des fins de recherche, ou bien à des fins d'évaluation ou d'analyse, nous comprenons que l'accès sélectif aux données de santé était strictement encadré pour que toute demande soit inexorablement soumise à l'expertise de la CNIL. Ce double cadre contraignant avait pour objectif de couvrir l'ensemble des traitements potentiellement amenés à utiliser des données de santé à caractère personnel. Cependant, ce dispositif a fait preuve de certaines rigidités et dysfonctionnements qui ont conduit à sa remise en cause et à sa refonte par la réforme de l'article 193 de la loi du 26 janvier 2016[859] dont nous aborderons prochainement les effets[860]. Pour ne pas laisser les bénéficiaires de l'accès sélectif toute latitude pour ne pas respecter leurs engagements, la loi a également mis en place un système de contrôle, *a posteriori*, par la Commission.

Paragraphe 2 : Le contrôle renforcé de l'accès sélectif aux données de santé

311. Nous venons de l'étudier, la question sensible de l'accès aux données personnelles de santé s'est toujours accompagnée de mesures de contrôle préventif afin de garantir la sécurité des informations et le respect de la vie privée. A ce titre, la CNIL est investie, depuis la création de l'accès sélectif, de la mission de vérifier directement qu'aucune information nominative ou identifiante n'est présente parmi les données à traiter. Il est d'ailleurs possible que les créateurs de ce mécanisme d'autorisation préalable aient sous-estimé les conséquences de l'omniscience de la Commission et n'aient pas mesuré l'ampleur de la tâche[861] à accomplir. Ceci est d'autant plus flagrant qu'en complément de son rôle de gardien de l'accès sélectif, la CNIL se voit aussi attribuer le rôle de contrôleur des traitements de données mis en œuvre.

312. Il est évident que soumettre le bénéfice de l'accès sélectif à des prérequis n'a de sens réel que dans le cas où une autorité administrative est mandatée pour vérifier, le cas échéant, que les obligations sont bien respectées. Depuis l'entrée en vigueur de la loi relative à l'informatique et aux libertés[862], c'est à la CNIL qu'est revenue cette mission capitale : l'article 11 de la loi relative à l'informatique et aux libertés prévoyait ainsi, de 1978 à 2004, que la Commission

[859] *Ibid.*

[860] *Infra* n° 330 à 336.

[861] *Infra* n° 434.

[862] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

dirige des missions d'investigation et de contrôle à travers la délégation d'un magistrat et d'experts éventuels[863]. Au-delà de cette simple possibilité de mandatement d'une autorité judiciaire, aucune autre procédure de contrôle par des agents de la CNIL n'était présente dans la loi.

313. Cette faculté a été élargie et simplifiée en 2004 par la suppression du recours au magistrat : il a ainsi été permis à la Commission d'habiliter[864] directement ses membres ou ses agents pour procéder à des vérifications portant sur des traitements de données et pour obtenir copie de tous documents ou supports d'informations utiles[865]. Cette évolution a également donné lieu à la description des conditions dans lesquelles le contrôle par les membres ou agents de la CNIL pouvait s'effectuer[866] afin que toute structure ayant mis en œuvre un traitement de données personnelles de santé soit au fait des modalités de contrôle dont elle peut faire l'objet. A ce titre, le législateur a défini une plage horaire de 6 heures à 21 heures pendant laquelle le contrôle peut avoir lieu. La définition des lieux potentiels de contrôle a également été donnée afin que tout traitement puisse être vérifié, quel que soit l'endroit où il se situe. Les membres ou agents de la CNIL peuvent ainsi demander et obtenir tous les documents nécessaires à leur mission et en faire une copie, quelle que soit le support, accéder aux programmes informatiques et en demander une transcription des données directement utilisable. Face à de tels pouvoirs de contrôle, des précautions ont été prises afin de garantir que la Commission agisse conformément à la loi : ainsi le procureur de la République doit être informé préalablement à toute intervention. Il a aussi été prévu que si le responsable des lieux dans lesquels se situe le traitement de données ne donne pas son accord, dans ce cas, les intervenants doivent obtenir une ordonnance motivée du président du tribunal de grande instance compétent. En cas d'autorisation, ce dernier peut même décider de se rendre sur place au moment de l'intervention. Il dispose également du pouvoir d'arrêter, ou de suspendre, la visite à tout moment. Soulignons toutefois, que dès lors

[863] Article 11 de la loi n° 78-17 du 6 janvier 1978, *op. cit.* : « *La commission peut demander aux premiers présidents de cour d'appel ou aux présidents de tribunaux administratifs de déléguer un magistrat de leur ressort, éventuellement assisté d'experts, pour des missions d'investigation et de contrôle effectuées sous sa direction* ».

[864] Article 19, alinéa 5 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.* : « *Ceux des agents qui peuvent être appelés à participer à la mise en œuvre des missions de vérification mentionnées à l'article 44 doivent y être habilités par la commission ; cette habilitation ne dispense pas de l'application des dispositions définissant les procédures autorisant l'accès aux secrets protégés par la loi.* »

[865] Article 11, 2°, f) de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.* : « *Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou des agents de ses services, dans les conditions prévues à l'article 44, de procéder à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions* ».

[866] Article 44 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

que le président du tribunal de grande instance donne son aval à une intervention sur place, les personnes responsables du traitement de données contrôlé sont tenues de répondre de bonne foi à toutes les sollicitations dont elles pourraient être destinataires de la part des membres ou agents de la Commission : pour rappel, toute entrave à l'action des représentants de la CNIL dans l'exercice de leurs missions est passible de sanctions[867].

314. Les lois du 29 mars 2011[868] et du 18 mars 2014[869] ont apporté des évolutions supplémentaires à l'encadrement du contrôle des traitements de données par la CNIL. En premier lieu, en cas de refus du responsable des lieux dans lesquels se situe un traitement à contrôler, ce n'est plus le président du tribunal de grande instance mais le juge des libertés et de la détention qui autorise l'intervention. De plus, en cas d'urgence ou de risque avéré de destruction ou dissimulation de documents, le juge des libertés et de la détention peut autoriser une intervention sans que le responsable des lieux n'en soit préalablement informé. En second lieu, la possibilité de consultation de documents a été étendue à ce qui aurait été rendu accessible même par imprudence, négligence ou par le fait d'un tiers : cela permet donc au personnel de la CNIL de procéder, par tous moyens, à la récupération des informations qui leur sont utiles dans le cadre de leur mission.

315. Tous les agents de la Commission ne peuvent pas forcément être habilités à intervenir dans le cadre de tous les contrôles. A partir de 2005, un décret[870] est ainsi venu encadrer les modalités d'habilitation des agents, de contrôle sur place, d'audition sur convocation, et de recours à des experts. Ce décret, encore d'actualité car il fait l'objet de mises à jour régulières, pose plusieurs limites à l'habilitation des agents à effectuer des contrôles sur place. D'abord, seuls les agents de catégorie A ou assimilés peuvent être choisis, et ce, pour une durée de 5 ans renouvelable. Des limites claires sont fixées : aucun agent de la CNIL ne peut être habilité à faire « *une visite ou une vérification s'il a fait l'objet d'une condamnation à une peine correctionnelle ou criminelle inscrite au bulletin n° 2 du casier judiciaire* ». Dans le même temps, afin de prévenir tout conflit d'intérêt, un agent ne peut pas participer à une visite ou une vérification auprès d'un organisme s'il détient avec celui-ci « *un intérêt direct ou indirect, s'il y exerce des fonctions ou*

[867] *Supra* n° 288 à 295.

[868] Loi n° 2011-334 du 29 mars 2011 *relative au Défenseur des droits*, JORF, n° 0075, 30/03/2011.

[869] Loi n° 2014-344 du 17 mars 2014 *relative à la consommation*, JORF, n° 0065, 18/03/2014.

[870] Décret n° 2005-1309 du 20 octobre 2005, *op. cit*,

une activité professionnelle ou s'il y détient un mandat ». La participation de l'agent de la CNIL sera aussi interdite si, au cours des trois années précédant la visite ou la vérification, l'un des critères précédemment mentionnés est rencontré.

316. Outre la définition des conditions d'habilitation des agents de la CNIL, le décret[871] précise comment doit se dérouler la procédure de contrôle sur place. Ainsi, comme le prévoit la loi[872], aucun contrôle ne peut avoir lieu sans que le procureur de la République n'en soit informé au préalable au moins vingt-quatre heures avant la date de l'intervention. La Commission doit porter à la connaissance du procureur de la République la date, l'heure, le lieu et l'objet du contrôle. S'agissant du responsable des lieux dans lesquels la vérification se tient, il peut n'être prévenu du contrôle qu'au moment où celui-ci débute : la CNIL doit l'informer de l'objet des vérifications, ainsi que de l'identité et de la qualité des personnes qui effectuent la visite. Le responsable de traitement doit aussi avoir connaissance de ces informations : s'il n'est pas présent au moment du contrôle, la Commission a huit jours pour lui faire part de ces éléments. La procédure détaillée par le décret indique également que si la vérification a lieu à la demande d'une autorité d'un autre Etat membre de l'Union européenne exerçant des missions similaires à celles de la CNIL, cette dernière doit en informer le responsable du traitement et lui indiquer que toutes les informations récupérées peuvent être transmises à ladite autorité. Il est important de noter que les individus contrôlés, et pas uniquement le responsable des lieux ou le responsable de traitement, peuvent demander aux agents chargés par la CNIL de procéder à des vérifications sur place leur ordre de mission et leur habilitation.

317. Comme nous l'avons vu précédemment[873], le responsable des locaux peut refuser que la visite ait lieu. Il faut alors que le juge des libertés et de la détention du tribunal de grande instance statue dans un délai de quarante-huit heures : dans un tel cas, l'ordonnance rendue doit préciser l'adresse des lieux à visiter, le nom et la qualité du ou des agents habilités, les heures auxquelles la visite peut avoir lieu. Le responsable des locaux et le responsable de traitement ne sont pas totalement impuissants face à cette ordonnance : ils peuvent faire appel devant le premier président de la cour d'appel dans un délai de quinze jours à compter de la notification de l'ordonnance ; ils peuvent également se pourvoir en cassation.

---

[871] *Ibid.*

[872] *Supra* n° 313.

[873] *Supra* n° 314.

318. Tout contrôle sur place fait nécessairement l'objet d'un procès-verbal extrêmement détaillé comme nous allons le constater. Celui-ci doit nécessairement comporter une série d'informations telles que : la nature, le jour, l'heure et le lieu des vérifications ou contrôles effectués[874]. Ce procès-verbal n'est valide que s'il répond à tous les critères prévus et qu'il est signé, à la fois, par les personnes chargées du contrôle qui y ont procédé et par le responsable des lieux ou une personne désignée par celui-ci. Le procès-verbal est ensuite obligatoirement notifié au responsable des lieux ainsi qu'au responsable de traitement. Dans le cas où la visite n'aurait pas pu se dérouler, ou en cas d'absence du responsable des lieux, le procès-verbal doit indiquer, d'une part les raisons ayant empêché ou entravé la visite, d'autre part la mention de l'absence dudit responsable. Nous le comprenons, toute cette procédure est extrêmement précise et le moindre élément qui viendrait à manquer disqualifierait immanquablement le contrôle mis en œuvre par la CNIL.

319. Les modalités d'audition sur convocation et de recours à des experts sont aussi détaillées par le décret[875]. Toute personne convoquée pour être auditionnée par les personnes chargées du contrôle par la CNIL doit l'être au moins huit jours avant son audition et doit être informée de son droit à être assistée par un conseil de son choix. L'audition fait l'objet d'un procès-verbal dans les mêmes conditions que celles décrites au point précédent. Concernant le recours à des experts, ceux-ci sont désignés dans les mêmes conditions que les agents habilités par la CNIL[876]. Ces experts sont indemnisés et doivent remettre leur rapport au président de la Commission qui doit en transmettre une copie au responsable du traitement.

320. Enfin, des mesures très spécifiques sont prévues en cas de contrôle d'un traitement de données médicales individuelles mis en œuvre par un membre d'une profession de santé. Afin de ne pas violer le secret médical, seul un médecin peut demander la communication de telles données. Ce médecin est désigné par le préfet ou le directeur général de l'agence régionale de santé à la demande du président de la CNIL : il s'agit soit d'un médecin inspecteur du travail,

[874] La liste complète des informations devant figurer dans le procès-verbal de visite est la suivante : la nature, le jour, l'heure et le lieu des vérifications ou contrôles effectués, l'objet de la mission, les membres présents, les personnes rencontrées, les déclarations éventuelles des personnes rencontrées, les demandes formulées par les membres de la mission, les difficultés rencontrées, la liste exhaustive des pièces et documents copiés lors du contrôle. Retrouvez-la à l'article 64 du décret n° 2005-1309 du 20 octobre 2005, *op. cit*,

[875] Décret n° 2005-1309 du 20 octobre 2005, *op. cit*,

[876] *Supra* n° 315.

soit d'un médecin chargé de requérir la communication des données, doit d'un médecin inscrit sur une liste d'experts judiciaires. Ce médecin répond nécessairement aux mêmes exigences que les experts ordinaires.

321. Nous le comprenons, les acteurs qui bénéficient de l'accès sélectif pour effectuer leurs traitements de données de santé restent, en théorie, drastiquement contrôlés par les services de la CNIL. La procédure de contrôle *a posteriori* est très encadrée et a été adaptée, depuis sa création en 2005, aux évolutions législatives et réglementaires. Combiné à la procédure préalable d'autorisation d'accès sélectif, le système présente un caractère très dissuasif pour quiconque souhaite mettre en œuvre un traitement de données de santé issues du SNIIRAM : les textes laissent présager un parcours long et rigoureux qui ne peut souffrir d'aucun faux pas jusqu'à la fin du traitement envisagé. C'est probablement la complexité et, nous l'aborderons ultérieurement, certains dysfonctionnements constatés dans la pratique, qui ont conduit le législateur à chercher un autre compromis entre le contrôle inévitable de l'accès aux données de santé, à des fins de protection de la vie privée, et la simplification du dit accès sélectif, depuis la préparation du dossier jusqu'à la mise en œuvre du traitement.

SECTION 2 : L'ASSOUPLISSEMENT NÉCESSAIRE DE LA PROCÉDURE D'ACCÈS SÉLECTIF

322. La possibilité d'obtenir des données de santé provenant des bases de données administratives telles que le SNIIRAM ou le PMSI s'est construite progressivement. Au fil des réflexions au niveau national mais aussi européen, et plus largement au niveau mondial, c'est un système à deux entrées qui est devenu la référence en droit français. Cependant, le mécanisme mis en œuvre en France a rapidement montré des signes de faiblesse en raison de sa grande rigidité (§1). La réforme de l'accès aux données de santé de l'Assurance maladie engagée par la loi du 26 janvier 2016[877] permet alors l'harmonisation des mécanismes pour une nouvelle approche plus souple et praticable de l'accès sélectif (§2).

[877] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

Paragraphe 1 : La rigidité initiale de l'accès sélectif aux données de santé

323. Dès 2002[878] et la création officielle de la base de données SNIIRAM ainsi que de l'accès sélectif aux données qu'il contient, la procédure s'est découpée en deux parties qui n'étaient pas nécessairement exclusives l'une de l'autre, régies par le chapitre X de la loi relative à l'informatique et aux libertés[879] pour la première, et par le chapitre IX de la même loi pour la seconde. Comme nous l'avons étudié précédemment[880], tout acteur non bénéficiaire d'un accès permanent était obligé de passer par le dépôt d'une demande de traitement dans le cadre de l'ancien chapitre X de la loi relative à l'informatique et aux libertés[881]. Ce prédicat simple, prévu depuis l'arrêté relatif à la mise en œuvre du SNIIRAM de 2005[882], permettait, *a priori*, à tous les demandeurs d'un accès sélectif de savoir comment ils pourraient se voir autoriser un accès, et dans quels délais. Mais plusieurs obstacles se présentent sur ce cheminement.

324. Le premier obstacle est tout simplement juridique. Si les arrêtés successifs renvoient aux dispositions du seul chapitre X de la loi relative à l'informatique et aux libertés[883], les demandeurs d'un accès sélectif peuvent très bien être confrontés à une procédure supplémentaire si leur objectif est d'effectuer un traitement ayant pour fin la recherche dans le domaine de la santé. Cela signifie que, pensant passer par l'unique procédure du chapitre X, un demandeur souhaitant faire de la recherche en santé pouvait être à nouveau soumis à la procédure du chapitre IX. Le processus pouvait donc s'avérer particulièrement long : le chapitre X, qui expose la marche à suivre afin d'obtenir un accès sélectif, indique que la CNIL dispose de deux mois renouvelables une fois pour rendre sa décision. En cas de silence, celui-ci vaut rejet de la demande. En admettant que l'autorisation ait été obtenue après 4 mois d'attente, si le demandeur souhaitait faire de la recherche en santé, il devait ensuite être soumis à la procédure d'autorisation prévue par le chapitre IX. Nous l'avons étudiée[884], cette dernière

[878] Arrêté du 11 avril 2002, *op. cit.*

[879] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version antérieure à la loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[880] *Supra* n° 302 à 310.

[881] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version antérieure à la loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[882] L'arrêté du 20 juin 2005, *op. cit.* a mis à jour la référence à la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.* En effet, avant cela, la procédure à suivre n'était pas au chapitre X mais au chapitre V ter de la loi relative à l'informatique et aux libertés.

[883] *Ibid.*

[884] *Supra* n° 302 à 308.

implique le CCTIRS qui a un mois pour donner son avis sur le projet de recherche. La CNIL se prononce par la suite dans un délai de deux mois renouvelable une fois sur décision motivée de son président. De manière identique à ce qui est prévu dans le chapitre X, le silence de la CNIL vaut refus d'autorisation de traitement.

325. Ce premier point est important. En admettant que la CNIL renouvelle son délai de réflexion, un demandeur qui croit être soumis à un délai maximum de quatre mois pour être autorisé à traiter des données provenant du SNIIRAM peut rapidement être soumis à cinq mois supplémentaires (un mois pour le CCTIRS et quatre autres pour la CNIL) si son projet de traitement vise à faire de la recherche en santé. La possibilité de créer des méthodologies de référence homologuées par la CNIL afin de favoriser les traitements de données ne permettant pas une identification directe des personnes dans le cadre de la recherche en santé a bien été pensée[885], mais en près de douze ans, seulement trois méthodologies de référence ont, semble-t-il, été homologuées[886], dont deux bien tardivement en 2015 et 2016. De plus, si nous nous intéressons de plus près au contenu de ces méthodologies, nous nous rendons compte que chacune d'entre elles exclut spécifiquement de leur champ d'application les « *recherches nécessitant un appariement avec des données issues des bases médico-administratives* » voire même, pour la méthodologie MR-002[887] une référence directe à l'accès sélectif aux données de santé : « *sont exclus du champ d'application de la présente méthodologie* […] *les études épidémiologiques, les études médico-économiques et notamment celles relevant des dispositions du chapitre X de la loi Informatique et libertés* ». Nous pouvons évidemment saluer l'intention de simplifier les modalités d'autorisation de certains traitements de données personnelles de santé. Mais le fait que tout traitement de données issues du SNIIRAM en soit exclu, forçant le demandeur à se soumettre à un processus deux fois plus long que ce qui est annoncé par les arrêtés qui ne font qu'un simple renvoi au chapitre X de la loi relative à

[885] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version antérieure à la loi n° 2016-41 du 26 janvier 2016, *op. cit.*, art. 54.

[886] Nous pouvons citer la méthodologie pour les traitements de données personnelles opérés dans le cadre des recherches biomédicales **(**MR-001), homologuée le 5 janvier 2006 et modifiée le 21 juillet 2016. Ont aussi été homologuées la méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des études non interventionnelles de performances en matière de dispositifs médicaux de diagnostic in vitro (MR-002) le 16 juillet 2015, et la méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé ne nécessitant pas le recueil du consentement exprès ou écrit de la personne concernée (MR-003), le 21 juillet 2016.

[887] Délibération n° 2015-256 du 16 juillet 2015 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des études non interventionnelles de performances en matière de dispositifs médicaux de diagnostic in vitro (MR-002).

l'informatique et aux libertés[888], est une marque profonde de la rigidité et du manque de pédagogie dont pouvait faire preuve l'ancien accès sélectif aux données personnelles de santé. Nous pouvons également signaler que les délais d'autorisation de traitement découlant de la procédure prévue par les textes étaient bien supérieurs à ce que le demandeur pouvait être en droit d'attendre. Ce facteur lourd de conséquences sur l'effectivité de l'accès sélectif a notamment été soulevé avec force par P.-L. BRAS dans son rapport remis en 2013[889].

326. Le second obstacle est d'ordre pratique et concerne la mise en œuvre des dispositions légales et réglementaires relatives à l'accès sélectif. En effet, le mécanisme prévu par l'arrêté de 2005[890], mis à jour en conformité avec la loi de 2004[891], inclut dans le processus d'autorisation d'accès sélectif l'intervention d'un nouvel acteur : l'Institut des Données de Santé (IDS). Or, cela a déjà été évoqué dans la présente étude[892], si l'IDS a bien été créé en 2005, il n'a été mis en place que deux ans plus tard[893] ! Pendant toute cette période de flottement, aucun accès sélectif aux données personnelles de santé du SNIIRAM ne pouvait donc être déposé ni obtenu. Au-delà de ce détail important, rappelons que toute autorisation finale de traitement repose sur la CNIL, et éventuellement sur l'intervention du CCTIRS. Chacun de ces acteurs agit alors comme un rouage de l'accès sélectif. Si un seul de ces rouages se trouve grippé, rouillé ou totalement bloqué, l'intégralité du dispositif est affectée. Or, comme n'a pas manqué de le signaler P.-L. BRAS[894], « *l'augmentation du nombre des demandes* […] *est de nature à engorger les services de la CNIL et les services chargés de l'instruction.* […] *Ni le CCTIRS ni encore moins l'IDS ne disposent de moyens et de compétences suffisants pour faire face à ce défi* ». Nous pouvons en déduire que les mesures prises par les autorités françaises afin de fixer des délais *maxima* d'autorisation ou de refus d'un dossier n'ont pas été suffisamment suivies d'effet en pratique. Ceci est d'autant plus vrai qu'une fois l'autorisation obtenue, l'attente était loin d'être terminée car les données personnelles de santé devaient encore être transmises par la CNAMTS, gestionnaire du SNIIRAM.

---

[888] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version antérieure à la loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[889] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 40.

[890] Arrêté du 20 juin 2005, *op. cit.*

[891] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[892] *Supra* n° 165, 214 et 306.

[893] Arrêté du 30 avril 2007, *op. cit*.

[894] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 37.

327. Nous explorerons plus en détails les imperfections et dysfonctionnements de l'accès sélectif dans le prochain titre[895]. Le premier aperçu que nous venons de réaliser permet de se rendre compte de la rigidité d'un mécanisme qui repose sur des processus variés et des acteurs divers dont le bon fonctionnement dépend de l'allocation de moyens humains et techniques à chacun des intervenants. Les quelques mesures visant à simplifier les modalités d'autorisation de traitement auraient pu fonctionner mais elles excluaient précisément tout traitement qui utiliserait des données issues des bases de données médico-administratives dont fait partie le SNIIRAM.

328. Nous le savons, l'édifice de l'accès sélectif aux données personnelles de santé a, avant tout, été bâti sur les fondations de la protection de la vie privée des individus. Cependant, au regard des développements précédents, il est évident que la volonté de protéger le droit au respect de la vie privée a pris l'ascendant sur l'ensemble du dispositif, ayant pour conséquence de le rendre trop rigide vis-à-vis de la finalité pour laquelle il a été conçu. Ce constat a conduit plusieurs personnalités à s'engager en faveur d'une refonte de l'accès sélectif pour que celui-ci soit enfin utilisé dans le cadre de la mission en vue de laquelle il a été créé. C'est ainsi que D. SICARD et J. de KERVASDOUE publiaient une tribune[896] en 2013 prônant la révision de l'accès sélectif. Bien qu'affirmant que les accès autorisés au SNIIRAM étaient « *déjà nombreux, qu'ils soient permanents* […] *ou ponctuels* », ils reconnaissaient dans le même temps que « *les procédures* [restaient] *très longues et les services chargés de l'instruction des demandes nombreuses* [étaient] *trop diversifiés et surchargés* ». Cela dit, les deux auteurs ne manquaient pas de rappeler leur attachement au respect de la vie privée en détectant deux freins potentiels à l'ouverture des données de santé : la réidentification et le mésusage. Ce sont précisément ces deux risques qui ont pesé sur le fonctionnement de l'accès sélectif dès sa mise en œuvre. Cet exemple de réflexion qui a accompagné la préparation de la réforme du 26 janvier 2016[897] est emblématique des enjeux à prendre en compte et de la difficulté à trouver un équilibre entre le partage de la connaissance pour le bien commun et la protection de la vie

[895] *Infra* n° 357 à 392.

[896] De KERVASDOUE J. et SICARD D., « Plus grave que le débat sur la pilule, l'affaire des données de santé publique », *Le Monde*, 15 janvier 2013, in DEBOST C., « Publication du rapport sur la gouvernance et l'utilisation des données de santé, la promesse d'un entrebâillement de l'Open data dans le secteur de la santé ? », *RDS*, janvier 2014, n° 57, p. 947 à 949.

[897] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

privée. Le nouveau cadre juridique français est encore dans ses premiers mois de mise en œuvre mais force est de constater que son objectif affiché, tant dans les textes que dans la pratique, est la proposition d'un accès sélectif plus simple, plus rapide et plus souple que dans sa version précédente.

Paragraphe 2 : La nouvelle approche simplifiée de l'accès sélectif

329. La loi du 26 janvier 2016[898] a donné lieu à une large réécriture des dispositions légales et réglementaires destinées à encadrer l'accès aux données de santé à caractère personnel contenues notamment dans les bases de données hospitalières et de l'assurance maladie. L'accès sélectif aux données de santé a fait l'objet d'une importante unification du dispositif sans délaisser la nécessaire protection de la vie privée (A). Cependant, la volonté de simplification du législateur a dû faire face à l'entrée en vigueur du Règlement européen relatif à la protection des données[899], à peine plus de deux ans après la réforme française (B).

A) L'esprit unificateur de la réforme du 26 janvier 2016

330. L'article 193 de la loi relative à la modernisation de notre système de santé[900] a été envisagé, dès la présentation du projet de loi[901], dans une optique d'assouplissement et de simplification de l'accès sélectif aux données de santé. Son premier apport réside dans la création du système national des données de santé (SNDS) qui regroupe en son sein les données du SNIIRAM, du PMSI, et de l'INSERM concernant les causes médicales de décès[902]. A terme, le SNDS contiendra également les données « *médico-sociales* » relatives aux maisons départementales des personnes handicapées, ainsi qu'un échantillon représentatif des données de remboursement par bénéficiaire transmis par les organismes de complémentaire santé[903] :

---

[898] *Ibid.*

[899] Règlement 2016/679, *op. cit.*

[900] *Ibid.*

[901] ROMANENS J.-L., « Projet de loi relative à la santé : chronique d'une vie annoncée », *RDS*, 2015, n° 64, p. 201-212.

[902] DEVILLIER N., « Les dispositions de la loi de modernisation de notre système de santé relatives aux données de santé », *Journal International de Bioéthique*, 2017/3, vol. 28, p. 57-61.

[903] Le projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019 prévoit également l'ajout de nouvelles données dans le SNDS : « *Les données destinées aux professionnels et organismes de santé recueillies à l'occasion des activités mentionnées au I de l'article L. 1111-8 du* [code de la santé publique] *donnant lieu à la prise en charge des frais de santé en matière de maladie ou de maternité mentionnée à l'article L. 160-1 du code de la sécurité sociale et à la prise en charge des prestations mentionnées à l'article L. 431-1 du même code en matière d'accidents du travail et de*

cependant, les travaux visant à la constitution, au rassemblement et à l'intégration de ces données dans le SNDS ne seront pas terminés avant le courant de l'année 2019[904]. La constitution de cette base unique destinée à centraliser toutes les données de santé clarifie immédiatement le paysage des bases de données potentiellement accessibles. Avec ce changement de taille, tout demandeur potentiel sait que les données auxquelles il peut accéder sont contenues dans le SNDS et non dans une obscure base de données à l'acronyme imprononçable pour le profane. Ce rassemblement des données dans une seule base a toutefois un revers : en cas de faille dans la protection du système, un nombre très important d'informations pourrait être mis en danger, ce que nous ne manquerons pas d'analyser dans un chapitre ultérieur[905].

331. Le second apport directement visible de la réforme est la suppression du chapitre X de la loi relative à l'informatique et aux libertés[906] qui fixait la procédure à suivre en cas de demande d'accès sélectif. Le législateur a souhaité mettre fin à l'aspect binaire de l'autorisation de traitement en supprimant la dichotomie qui existait jusqu'alors. Tout le mécanisme est venu reposer sur le chapitre IX de ladite loi[907], dont les articles figurent aujourd'hui à la sous-section 2 de la section 3 du chapitre III de son Titre 2 depuis l'ordonnance du 12 décembre 2018[908], qui vise uniformément toutes les demandes d'autorisation de traitement de données personnelles dans le cadre d'une recherche, d'une étude ou d'une évaluation dans le domaine de la santé : le traitement des données personnelles de santé entre donc directement dans le champ d'application de ce texte. Le nouvel article L. 1461-3 du code de la santé publique dispose ainsi que les « *accès aux données à caractère personnel du système national des données de santé ne peut être autorisé que pour permettre des traitements* […] *à des fins de recherche, d'étude ou d'évaluation contribuant à une finalité mentionnée au III de l'article L. 1461-1 et répondant à un motif d'intérêt public* ». Nous l'avons étudié dans la première partie, l'autre cas

maladies professionnelles » et les « *données à caractère personnel des enquêtes dans le domaine de la santé, lorsque ces données sont appariées avec* [les autres données contenues dans le SNDS] ».

[904] GIRARD M., cheffe de la mission accès aux données de santé à la DREES, a annoncé le calendrier de complétion du SNDS à l'occasion du colloque « Santé et protection des données », *Cycle Conseil d'Etat en droit social*, 01/12/2017.

[905] *Infra* n° 436 à 440.

[906] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[907] *Ibid.*

[908] Ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

d'autorisation d'accès aux données du SNDS concerne l'accès permanent[909] nécessaire à l'accomplissement des missions de service public. Le chapitre IX est donc devenu la porte d'entrée unique de l'accès sélectif aux données personnelles de santé et le processus d'autorisation préalable qu'il décrit est une fois de plus assoupli[910] par rapport au précédent.

332. Si nous pouvons considérer sans crainte que ce nouveau mécanisme est simplificateur, il ne faut pas non plus omettre de préciser que des éléments de complexité demeurent. L'accès sélectif reste soumis à un examen préalable dont l'objectif est de permettre de faire coexister, *in fine*, les ambitions du responsable de traitement avec la vie privée des individus. Cette complexité est inhérente au sujet de la protection de la donnée personnelle de santé mais nous pouvons souligner que le législateur a travaillé à transformer l'accès sélectif pour que, d'une route sinueuse parsemée d'embûches parfois imprévisibles, il devienne, ne serait-ce que dans les textes, un chemin rectiligne agrémenté de quelques points de contrôle connus et anticipables.

333. Avec le nouvel accès sélectif aux données de santé, un acteur unique, l'Institut national des données de santé (INDS) est créé[911] en lieu et place de l'ancien IDS, sert de secrétariat[912] au dépôt des demandes. Ainsi, la mission de l'INDS est de guider les demandeurs dans la constitution de leur dossier, de veiller à ce qu'aucune pièce ne manque, et de ne laisser passer à l'étape suivante que les dossiers complets. L'objectif est d'effectuer un premier filtre sur l'ensemble des demandes afin que le prochain acteur ne soit pas amené à travailler sur des dossiers incomplets ou mal construits.

Les dossiers déposés et validés par l'INDS sont ensuite examinés par le Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (CEREES)[913] qui

---

[909] V. Partie I.

[910] PECHILLON E., « L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ? », *L'information psychiatrique*, 8/2015, volume 91, p. 645-649**.**

[911] L'INDS a été créé par l'article L. 1462-1 du code de la santé publique et mis en place par l'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 », JORF n° 0096 du 23/04/2017. Signalons que le projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019 prévoit la transformation de l'INDS en un nouveau GIP appelé « *Plateforme des données de santé* ».

[912] Article 54, alinéa 8 de la loi n° 78-17 du 6 janvier 1978, *op. cit.* : « *Les dossiers présentés dans le cadre du présent chapitre* […] *sont déposés auprès d'un secrétariat unique, qui assure leur orientation vers les instances compétentes* ».

[913] La composition et le fonctionnement du CEREES ont été détaillés dans le décret n° 2016-1872 du 26 décembre 2016 modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier

remplace l'ancien CCTIRS. Ce Comité est chargé de rendre un avis sur la méthodologie du traitement de données envisagé, sur la *« nécessité du recours à des données à caractère personnel, sur la pertinence de celles-ci par rapport à la finalité du traitement et, s'il y a lieu, sur la qualité scientifique du projet »*[914]. Tout comme le CCTIRS avant lui, le CEREES ne dispose que d'un mois pour se prononcer et son silence vaut avis favorable. De façon ponctuelle, l'avis complémentaire de l'INDS peut être requis au sujet du caractère d'intérêt public de l'étude envisagée[915]. Il est saisi soit par la CNIL, soit par le ministre chargé de la santé. L'INDS peut même s'auto-saisir au plus tard une semaine après l'avis du CEREES uniquement lorsque le traitement envisagé n'implique pas la personne humaine. Si l'INDS est amené à rendre son avis, il dispose d'un délai d'un mois pour se prononcer et le demandeur de l'accès sélectif est informé à la fois de la saisine et du contenu de l'avis[916].

334. Un autre acteur peut être amené à rendre son avis. Il s'agit du comité de protection des personnes[917] (CPP) qui intervient dans la procédure d'autorisation lorsque les données obtenues *via* l'accès sélectif sont destinées à être appariées[918] avec des données impliquant la recherche sur la personne humaine[919]. Dans un tel cas de figure, le dossier n'est pas déposé auprès de l'INDS, il est transmis directement à un CPP qui dispose, en principe, de 45 jours pour rendre son avis[920]. Son silence vaut rejet de la demande de traitement. En revanche, tout dossier qui reçoit un avis peut ensuite passer à l'étape suivante. Soulignons le fait que, même dans ce cadre,

1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* n° 0301 du 28/12/2016 ; ainsi que dans l'arrêté du 5 mai 2017 portant nomination au Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé, *JORF* n° 0110 du 11 mai 2017.

914 Article 54, alinéa 6 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2016-41 du 26 janvier 2016, *op. cit*.

915 Article 54, alinéa 7, *ibid.*, modifiée par la loi n° 2016-41 du 26 janvier 2016, *op. cit*.

916 Pour le détail de la procédure de saisine et de décision de l'INDS à propos du caractère d'intérêt public que présente une recherche, une étude ou une évaluation justifiant une demande d'autorisation de traitement de données en application du chapitre IX de la loi relative à l'information et aux libertés modifiée par modifiée par la loi n° 2016-41 du 26 janvier 2016, *op. cit.*, v. décret n° 2016-1872 du 26 décembre 2016, *op. cit*.

917 L'intervention des comités de protection des personnes est prévue depuis la loi n° 2012-300 du 5 mars 2012 *relative aux recherches impliquant la personne humaine*, JORF n° 0056 du 06/03/2012, dite loi Jardé.

918 Apparier : mettre ensemble des choses qui vont par paires. Apparier des données signifie que deux types de données sont reliées entre elles pour être traitées ensemble.

919 Article 54, alinéa 3 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2016-41 du 26 janvier 2016, *op. cit*.

920 Art. R. 1123-23 du code de la santé publique.

l'INDS peut être amené à se prononcer, dans les conditions évoquées précédemment[921], sur le caractère d'intérêt public de l'étude envisagée.

335. Au premier abord, cette partie du nouveau mécanisme d'accès sélectif ne semble pas grandement différente du précédent. L'IDS devient l'INDS, le CEREES remplace le CCTIRS et dispose même d'un délai identique pour rendre son avis, un CPP n'intervient dans des cas spécifiques. Pourtant, plusieurs nouveautés, qui pourraient être qualifiées d'améliorations, sont présentes. L'INDS a, par exemple, un rôle différent de celui qu'avait son prédécesseur : il sert de porte d'entrée à l'accès sélectif et n'a plus à systématiquement approuver, comme c'était le cas auparavant pour l'IDS[922], les dossiers. L'INDS est véritablement chargé de s'assurer que tout soit mis en œuvre pour que les dossiers soient complets, lisibles, afin de faciliter et fluidifier leur étude par les autres acteurs. Tout l'intérêt de la nouvelle mouture de l'accès sélectif est finalement de permettre à la pratique d'être aussi efficace que la théorie prévue par les textes.

336. Intéressons-nous à nouveau à la procédure d'autorisation pour étudier sa dernière étape. Une fois examinés par le CEREES ou par un CPP et, le cas échéant, par l'INDS, les dossiers de demande d'accès sélectif sont transmis à la CNIL pour autorisation finale, ou refus. Un élément est de nature à nous surprendre immédiatement : la CNIL n'a pas, d'après la loi de modernisation de notre système de santé[923], de délai imposé pour rendre son avis. Cela est d'autant plus étonnant que l'ancien dispositif prévu au chapitre X désormais abrogé de la loi relative à l'informatique et aux libertés[924] prévoyait un délai de deux mois renouvelable une fois[925]. D'après le texte de la réforme du 26 janvier 2016[926], la Commission est libre de rendre l'autorisation d'accès sélectif aux données de santé dans le délai qui lui conviendra : mais, nous nous en doutons, l'objectif du législateur et de la Commission n'est pas de transformer l'absence de délai maximum imposé en attente interminable pour le demandeur. D'ailleurs, en prévision de l'entrée en vigueur du Règlement européen relatif à la protection des données[927] au 25 mai 2016, le législateur a proposé d'ajouter, à l'article 54 de la loi relative à l'informatique

[921] *Supra* n° 333.

[922] *Supra* n° 306.

[923] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[924] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[925] *Supra* n° 324.

[926] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[927] Règlement 2016/679, *op. cit.*

et aux libertés[928], la précision selon laquelle la CNIL doit se prononcer dans un délai de deux mois sur la demande d'accès sélectif, renouvelable une fois. La réintroduction de ce délai de deux mois renouvelable a bel et bien été confirmée avec l'adoption finale de la loi du 20 juin 2018 relative à la protection des données personnelles[929] mais aussi par l'ordonnance du 12 décembre 2018[930] qui a déplacé l'ancien article 54 vers le nouvel article 66.

L'intérêt de l'avis rendu par chacun des acteurs intervenus jusqu'alors est de faciliter et fluidifier le travail des membres de la CNIL. Dans le nouveau système, cette dernière n'est supposée recevoir que des dossiers complets, dont les principaux enjeux ont déjà été étudiés et mis en exergue par le CEREES, un CPP, et l'INDS s'il a été saisi. Cette ambition semblerait sur le point d'être atteinte si nous nous reposons sur les premiers retours officiels[931]. Pendant les trois premiers mois d'activité du nouveau mécanisme d'accès aux données du SNDS, entre l'ouverture de l'accès sélectif (le 28 août 2017) en vue de la première séance du CEREES (le 21 septembre 2017) et la fin du mois de novembre 2017, cent-vingt demandes avaient été déposées parmi lesquelles quarante dossiers portaient exclusivement sur des données du SNDS. Le CEREES avait émis un avis favorable à propos de trois dossiers sur cinq en moyenne et les premières autorisations de la CNIL concernant les dossiers déposés avant la mi-septembre avaient été délivrées avant la fin du mois de novembre. Il se serait donc écoulé deux mois et demi entre le dépôt d'un dossier et la décision finale d'autorisation ou de refus d'accéder aux données de santé. Nous sommes, pour le moment, bien loin des délais extensibles qui pouvaient auparavant être imposés aux demandeurs[932]. Le système devra toutefois faire ses preuves dans la durée ainsi que face au nombre de dossiers à traiter qui évoluera probablement *crescendo*.

[928] Art. 54 V de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version issue du projet de loi n° 490 relatif à la protection des données personnelles déposé le 13 décembre 2017.

[929] Loi n° 2018-493 du 20 juin 2018, *op. cit*.

[930] Ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[931] GIRARD M., cheffe de la mission accès aux données de santé à la DREES, a présenté le compte-rendu des premiers mois de mise en œuvre du nouvel accès sélectif aux données du SNDS à l'occasion du colloque « Santé et protection des données », *Cycle Conseil d'Etat en droit social*, 01/12/2017.

[932] *Infra* n° 379 à 390.

B) La simplification de la réforme altérée par l'adaptation au droit européen

337. Après le vote de la réforme du 26 janvier 2016[933], il n'aura fallu attendre que trois petits mois pour que des dispositions supplémentaires viennent affecter les acteurs souhaitant traiter des données de santé à caractère personnel. Bien que ces nouvelles mesures ne viennent pas du droit national mais du droit européen[934], nous pouvons souligner que tous les demandeurs de données de santé à caractère personnel qui pensaient avoir enfin un socle stable et concret issu de la loi française pouvaient craindre une nouvelle période d'instabilité législative et réglementaire. Alors que le Règlement européen[935] entré en vigueur le 25 mai 2018, soit deux ans après avoir été voté, laissant en théorie le temps au législateur et aux acteurs de s'adapter, certains impacts notables sur le nouvel accès aux données de santé sont à signaler.

338. Le premier impact a lieu sur la nature du droit applicable. En effet, le nouveau système d'autorisation préalable nécessaire à l'accès aux données de santé contenues dans le SNDS trouve sa source dans le titre VI du livre IV du code de la santé publique intitulé « *Titre VI : Mise à disposition des données de santé* » et dans les mesures modifiées de la loi relative à l'informatique et aux libertés[936]. L'ensemble est complété par les décrets d'application nécessaires. Le mécanisme d'accès aux données de santé à caractère personnel repose donc sur ce cadre unique, très strict et encadré, qui peut être qualifié de « *droit dur* ». Cette théorie qu'il devrait suffire d'appliquer de façon automatique pour pouvoir obtenir une autorisation d'accès de la part de la CNIL a été complétée par un droit beaucoup plus souple émanant du Règlement européen[937]. Effectivement, ledit Règlement « *donne toute leur importance aux instruments de droit souple, qui sont de source, de nature et de forme très variables* »[938]. Ainsi, le demandeur de données de santé provenant du SNDS doit être vigilant à la fois s'agissant du respect des dispositions propres à la procédure d'accès définies par la loi française mais aussi concernant l'application des nouvelles mesures prévues par le droit européen.

[933] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[934] Règlement 2016/679, *op. cit.*

[935] *Ibid.*

[936] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[937] Règlement 2016/679, *op. cit.*

[938] FAUVARQUE-COSSON B., « Protection des données personnelles », *D.*, 2018, p. 1033.

339. L'émergence d'un « *droit souple* » n'est pas nécessairement incompatible avec le « *droit dur* » qui encadre initialement l'accès aux données de santé. En effet, il aurait même pour intérêt principal de simplifier la mise en œuvre du « *droit dur* » d'après I. FALQUE PIERROTIN[939], présidente de la CNIL de septembre 2011 à février 2019. Toutefois, les outils développés dans ce cadre semblent être de plus en plus variés et nombreux, ce qui est susceptible de perdre les demandeurs d'accès aux données de santé dans le maquis juridique comme le souligne B. FAUVARQUE-COSSON qui estime que « *il est de plus en plus difficile de se repérer dans le labyrinthe des instruments de droit souple* »[940]. L'auteure ajoute que le DPO, *data protection officer* ou délégué à la protection des données[941], aura justement pour mission de connaître toutes les subtilités issues du droit souple. Ce « *droit souple* » apporté par le Règlement européen, malgré un objectif de simplification de mise en œuvre du « *droit dur* », comporte des inconvénients dès lors qu'il donne lieu à la création de dispositifs nombreux et variés. Ce qui est plus difficile pour tous ceux qui traitent des données à caractère personnel, qu'elles concernent la santé ou non, c'est que le texte européen « *introduit un véritable changement de paradigme en ce qu'il repose avant tout sur une logique de conformité dont les acteurs sont responsables alors que la loi informatique et libertés repose en grande partie sur une logique de formalités préalables* »[942]. Les acteurs qui souhaitent accéder aux données de santé rendues accessibles par la réforme du 26 janvier 2016 doivent nécessairement investir une nouvelle fois dans les compétences et les connaissances suffisantes afin de maîtriser au mieux les nouveaux aspects juridiques en provenance du droit européen.

340. Le second impact est localisé dans la loi relative à l'informatique et aux libertés[943] dont le chapitre IX a entièrement été réécrit successivement par la réforme du 20 juin 2018[944] et par l'ordonnance du 12 décembre 2018[945]. Tous les acteurs souhaitant bénéficier d'un accès aux SNDS sont, de fait, concernés par cette modification substantielle. Rappelons que la finalité

---

939 FALQUE PIERROTIN I., « Le droit souple vu de la CNIL : un droit relais nécessaire à la crédibilité de la régulation des données personnelles », *in* « Le droit souple », *Conseil d'Etat*, Etude annuelle 2013, p. 239 à 245, *in* FAUVARQUE-COSSON B., « Protection des données personnelles », *op. cit*.

940 FAUVARQUE-COSSON B., « Protection des données personnelles », *D.*, 2018, p. 1033.

941 V. notre analyse de la fonction de DPO *supra* n° 263 à 267.

942 EL BOUJEMAOUI W., MAZARS M.-F., « Maîtriser le socle du droit de la protection des données pour aborder l'application du Règlement européen (RGPD) », *Revue droit du travail*, 2018, p. 298.

943 Loi n° 78-17 du 6 janvier 1978, *op. cit.*

944 Loi n° 2018-493 du 20 juin 2018, *op. cit*.

945 Ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

première de cette loi est d'adapter le droit national au Règlement général relatif à la protection des données[946] (qui est pourtant, par sa nature, d'application directe). Dès la présentation des premiers travaux sur le projet de loi[947], des questions ont été posées sur l'opportunité de changer, une fois de plus, les mesures relatives aux données de santé au risque de revenir sur le fonctionnement du nouveau système. Les objectifs annoncés et attendus dans le cadre de cette nouvelle loi sont à la fois de développer l'utilisation des données de santé, grâce à une simplification des modalités d'autorisation de traitement, mais aussi de faciliter l'accès aux données de santé[948]. Cependant, une telle réforme, sur un système qui vient d'être réorganisé à peine deux ans auparavant n'est pas anodine : si les mesures ajoutées dans le code de la santé publique[949] par la loi de modernisation de notre système de santé[950] ne sont pas modifiées, tout le chapitre IX de la loi relative à l'informatique et aux libertés[951] est déplacé et remodelé. Les dispositions sont aujourd'hui trouvées à la sous-section 2 de la section 3 du chapitre III du Titre 2 de ladite loi. Or, la procédure spécifique d'examen des demandes d'accès aux données de santé relève spécifiquement de ce chapitre IX initial. Toute imprécision présente dans l'écriture de la loi est nécessairement de nature à compliquer la compréhension de la procédure d'accès au SNDS par les bénéficiaires.

341. La lecture de l'avis de la CNIL sur les modifications apportées par le projet de loi est sans équivoque. Dans sa délibération du 30 novembre 2017[952], la Commission « *s'interroge très fortement sur la rédaction* [du chapitre IX de la loi relative à l'informatique et aux libertés[953]] *qui opère une confusion entre les règles applicables, d'une part, aux traitements à des fins de recherche, d'étude et d'évaluation et, d'autre part, celles – nécessairement plus générales – applicables aux traitements comportant des données de santé. Il en résulte une réelle incertitude juridique, notamment sur les outils de simplification développés précédemment par*

[946] Règlement 2016/679, *op. cit.*

[947] Le projet de loi relatif à la protection des données personnelles a été présenté par la ministre de la justice le 13 décembre 2017.

[948] Projet de loi relatif à la protection des données personnelles, *Etude d'impact*, 12/12/2017, p. 122.

[949] Code de la santé publique, Première partie, Livre IV, Titre VI, Art. L. 1460-1 à L. 1462-1.

[950] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[951] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[952] Commission nationale de l'informatique et des libertés, « Délibération n° 201-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 », *op. cit*., p. 24.

[953] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

la Commission en la matière ». La Commission exprime ainsi de sérieux doutes concernant l'intelligibilité de la loi, ce qui peut nuire à l'effectivité de l'accès au SNDS. Par ces propos, la CNIL, rejointe par le Conseil d'Etat[954], met en garde le législateur à propos du contenu du projet de loi qui pourrait être de nature à mettre un frein au bon développement du nouveau mécanisme d'accès aux données de santé issu de la loi du 26 janvier 2016. Dans le même temps, la Commission soulève la non-conformité au droit européen des modalités d'information des personnes dont les données de santé sont recueillies et utilisées dans un traitement automatisé ayant pour finalité la recherche dans le domaine de la santé. Elle affirme dans son avis que la « *modalité d'information individuelle atténuée des personnes* […] *n'est pas conforme aux exigences posées par les articles 13 et 14 du Règlement* [général relatif à la protection des données] »[955]. Les députés et sénateurs ont pris en considération ce rappel de la CNIL en proposant une version adaptée du texte final qui se contente de renvoyer « *aux dispositions du règlement (UE) 2016/679* ».

342. Il ressort de la réécriture du chapitre IX de la loi relative à l'informatique et aux libertés[956] que les dispositions réglementaires d'application qui en découlent doivent également être révisées. Le décret n° 2016-1872 du 26 décembre 2016[957] doit ainsi être entièrement remanié pour répondre à la réforme portée par le projet de loi. Ce décret est hautement important pour pouvoir accéder aux données de santé du SNDS et mettre en œuvre un traitement de données de santé à caractère personnel dans le cadre de la recherche en santé car il décrit précisément la procédure de dépôt des dossiers auprès de l'INDS. Chaque candidat à l'accès et au traitement de données de santé y retrouve notamment la liste des informations à fournir, le déroulé de la procédure impliquant le CEREES, ainsi que la description de la composition et du fonctionnement de ce dernier. La réécriture de ce décret peut être à la fois attendue (son contenu pourrait faciliter l'accès aux données) et redoutée (son contenu pourrait demander une nouvelle adaptation coûteuse pour les demandeurs d'accès) par les acteurs qui accèdent au SNDS et dont l'activité est portée sur la recherche en santé.

---

[954] Conseil d'Etat, « Avis sur un 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 », *op. cit.*, p. 9.

[955] Commission nationale de l'informatique et des libertés, « Délibération n° 201-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 », *op. cit.*, p. 25.

[956] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[957] Décret °2016-1872 du 26 décembre 2016 *modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, JORF n° 0301, 28/12/2016.

343. Nous le comprenons, le texte de la loi du 20 juin 2018[958], repris et déplacé par l'ordonnance du 12 décembre 2018[959], bien qu'il ne modifie aucune des mesures du code de la santé publique relatives à l'accès aux données de santé du SNDS et issues de la réforme du 26 janvier 2016[960], apporte des modifications substantielles au chapitre IX de la loi relative à l'informatique et aux libertés. Ces changements font naître des subtilités supplémentaires et des interrogations propres aux traitements ayant pour finalité la recherche dans le domaine de la santé. Sans défaire le mécanisme mis en place pour créer le SNDS, ces derniers apports européen et national ont amené une dose complémentaire de normes à assimiler que les bénéficiaires de l'accès sélectif auraient, sans doute, été heureux, d'éviter.

[958] Loi n° 2018-493 du 20 juin 2018, *op. cit*.

[959] Ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit*.

[960] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

CONCLUSION DU CHAPITRE II

344. Accéder aux données de santé à caractère personnel impose aux demandeurs de se soumettre à une procédure contraignante. Son objectif est simple : s'assurer du respect de l'ensemble des dispositions légales et réglementaires afin de préserver le droit au respect de la vie privée des individus. La préparation du dossier de demande d'accès sélectif en vue de son examen par les autorités compétentes est donc une étape clef pour tous les demandeurs.

345. Les références légales de l'accès sélectif aux données de santé ont beaucoup évolué avec le temps. Le mécanisme a longtemps reposé sur une structure binaire, c'est-à-dire sur deux chapitres de la loi relative à l'informatique et aux libertés[961]. Le premier, créé en 1994[962], était dédié aux traitements de données personnelles à finalité de recherche en santé. Le second, créé en 1999[963], concernait les traitements de données personnelles à finalité d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention. Malgré la proximité apparente de ces deux chapitres, c'est le second qui fait référence dans les arrêtés successivement parus jusqu'à la réforme de 2016[964]. C'est cette dernière qui a regroupé les dispositions légales dans le même chapitre IX de la loi relative à l'informatique et aux libertés[965]. Puis, en 2018, une ordonnance[966] prise dans le cadre de la loi adaptant le droit français au droit européen[967] issu du RGPD[968] a, une fois de plus, modifié les repères légaux de l'accès sélectif. C'est désormais à la sous-section 2 de la section 3 du chapitre III du Titre 2 de la loi relative à l'informatique et aux libertés[969] que la procédure d'accès sélectif est définie.

346. Le contenu même de la procédure d'accès a également fait l'objet de plusieurs modifications au fil des années. Bien que le principe du contrôle de conformité soit resté le même, sa mise en œuvre s'est tardivement adaptée aux besoins exprimés par les acteurs

[961] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[962] Loi n° 94-548 du 1 juillet 1994 *op. cit.*

[963] Loi n° 99-641 du 27 juillet 1999 *op. cit.*

[964] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[965] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[966] Ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[967] Loi n° 2018-493 du 20 juin 2018, *op. cit*.

[968] Règlement 2016/679, *op. cit.*

[969] Loi n° 78-17 du 6 janvier 1978, *op. cit.* modifiée par l'ordonnance n° 2018-493 du 20 juin 2018, *op. cit*.

bénéficiaires. En effet, la CNIL est au cœur du mécanisme d'autorisation depuis sa création. D'abord chargée, seule, d'autoriser les accès sélectifs aux données de santé, c'est l'arrêté SNIIRAM de 2005[970] qui a fait intervenir pour la première fois l'IDS comme antichambre de l'autorisation par la CNIL. La loi du 13 août 2004[971] a aussi posé les bases de l'intervention du CCTIRS qui est chargé de donner son avis sur la méthodologie du traitement envisagé par le demandeur d'accès sélectif. L'examen des demandes d'accès en trois temps (IDS – CCTIRS – CNIL) est un pilier de l'accès sélectif qui continue aujourd'hui de faire référence bien que les intervenants ne soient plus les mêmes. En effet, le CCTIRS a été remplacé par le CEREES en 2016, puis par le comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES) avec le projet de loi relatif à l'organisation et à la transformation du système de santé[972]. L'IDS a, pour sa part, été remplacé par l'INDS en 2016, transformé en plateforme des données de santé (PDS). L'encadrement de l'accès sélectif aux données de santé a fait naître des lourdeurs procédurales, notamment dans les délais de traitement des demandes, à l'origine d'une insuffisante utilisation des opportunités offertes par les données contenues dans les bases médico-administratives. Le manque de moyens et de personnels formés, comme le signale P.-L. BRAS dans son rapport[973] a longtemps pénalisé les bénéficiaires potentiels de l'accès sélectif. Ce manque de moyens a, d'ailleurs, également affecté la CNIL dans sa capacité de contrôle des traitements autorisés au titre de l'accès sélectif.

347. La réforme du 26 janvier 2016[974] propose de rendre véritablement opérationnel l'accès sélectif aux données de santé sans sacrifier la protection du droit au respect de la vie privée. Chaque intervenant dispose de sa mission et semble, pour l'instant, avoir les moyens de s'en acquitter. Ainsi, les délais donnés pour rendre les avis, ou les décisions sont généralement respectés. La CNIL bénéficie donc maintenant du travail précieux de la PDS et du CESREES pour rendre ses décisions.

[970] Arrêté du 20 juin 2005, *op. cit.*

[971] Loi n° 2004-810 du 13 août 2004, *op. cit.*

[972] Projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019.

[973] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.*

[974] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

CONCLUSION DU TITRE I

348. La construction de l'accès sélectif a été difficile et s'est faite par tâtonnements successifs du législateur et du pouvoir réglementaire. Débutée au début des années 2000 avec les premiers pas du SNIIRAM, le mécanisme n'a, semble-t-il, jamais su trouver sa véritable voie avant la réforme opérée par la loi de modernisation de notre système de santé[975]. Les mesures prises pour encadrer l'accès aux données de santé des bases médico-administratives ont été pensées pour assurer au maximum la sécurité desdites données mais ont été modifiées à de multiples reprises, empêchant à la fois la stabilisation du dispositif et son appropriation par ses éventuels bénéficiaires. L'ensemble du dispositif permet, certes, un contrôle strict du bénéficiaire de l'accès sélectif qui souhaite obtenir et traiter des données de santé, mais la rigidité des contrôles effectués et le manque de fluidité des procédures ont lui ont ôté une partie de son efficacité.

349. Aujourd'hui, avec l'application de la réforme du 26 janvier 2016[976], l'accès sélectif aux données de santé à caractère personnel n'a jamais été aussi ouvert. Alors que le mécanisme a spécifiquement exclu certaines catégories d'acteurs dès sa création, le développement des mesures de précautions et de contrôle mises en œuvre dans un cadre strict, influencé par le droit européen, ont permis de proposer une plus grande transparence dans le nouveau SNDS. Les demandeurs sont appelés à être coopératifs dans leur démarche afin de permettre de faire la lumière sur l'ambition des traitements qu'ils envisagent mais aussi sur la sécurité qu'ils proposent pour assurer la protection des données. Cela s'accompagne nécessairement de pouvoirs de contrôle et de sanction au profit des autorités administratives qui peuvent agir aussi bien à l'encontre des responsables de traitements que de leurs employeurs.

350. Il est difficile de ne pas remarquer une certaine analogie de raisonnement avec l'accès permanent aux données de santé. En effet, l'accès sélectif, tout comme l'accès permanent, ont pour objectif de permettre à un maximum de données de santé à caractère personnel d'être étudiées sans risquer de porter atteinte au droit au respect de la vie privée. Ceci passe par la création d'une norme destinée à maîtriser le parcours et l'usage des données une fois qu'elles ont été confiées au bénéficiaire de l'accès.

---

975 *Ibid.*

976 *Ibid.*

351. Cependant, l'objet du présent titre était de présenter la structure et l'évolution juridique de l'accès sélectif. Son application soulève, depuis sa création, de nombreuses interrogations quant à son effectivité, notamment en raison du contenu et de la durée de la procédure. La réforme du 26 janvier 2016 est justement intervenue pour poser une nouvelle norme. Mais l'entrée en vigueur du Règlement européen du 27 avril 2016 et sa traduction dans le droit national avec la loi du 20 juin 2018, à laquelle a succédé l'ordonnance du 12 décembre 2018, ont apporté de sérieuses modifications qui ont impacté l'ensemble du mécanisme nouvellement créé. Le fonctionnement de l'accès sélectif aux données de santé du SNDS ne semble pas pour autant avoir été perturbé par ces changements. L'enjeu du prochain titre sera d'identifier les critiques portées à l'encontre de l'accès sélectif depuis sa création et de décrypter l'impact, positif ou négatif, des dernières réformes.

TITRE II

L'ACCÈS SÉLECTIF AUX DONNÉES DE SANTÉ EFFECTIF SOUS CONDITIONS

352. La base de données de santé à caractère personnel de l'assurance maladie, dite SNIIRAM[977], a été pensée, dès sa création, afin d'être accessible dans le cadre d'une procédure d'autorisation préalable venant s'adjoindre à la procédure d'accès permanent réservée à une liste spécifique de bénéficiaires[978]. Cette procédure permet initialement aux acteurs publics ne bénéficiant pas d'un accès permanent ainsi qu'aux acteurs privés à but non lucratif d'accéder, à travers un processus strictement encadré, à des données de santé stockées dans les bases de données médico-administratives. Dénommée « *accès sélectif* » à travers la présente étude, la procédure a connu de nombreux bouleversements au fil des années, qu'il s'agisse des principes qui la régissent, des garanties à apporter afin d'assurer la protection de la vie privée, des autorités impliquées dans la vérification desdites garanties, ou encore des modalités de contrôle et de sanction *a posteriori*.

Nous l'avons abordé dans le précédent titre[979], le fonctionnement de cet accès sélectif s'est avant tout bâti sur des fondations protectrices de la vie privée des individus qui sont à l'origine des données stockées dans les bases de données de l'Assurance maladie. C'est un sentiment de sévérité qui ressort de la procédure mise en œuvre dès la parution des premiers arrêtés[980], et surtout de la loi du 6 août 2004[981] transposant la directive européenne du 24 octobre 1995[982]. Fort justifiée, la protection renforcée des données de santé à caractère personnel est nécessaire en raison des risques existants dès lors qu'un traitement automatisé est réalisé. Ces risques sont

[977] Le SNIIRAM, ou Système National d'Information Inter-Régimes de l'Assurance Maladie, a été créé par la loi n° 98-1194 du 23 décembre 1998 *de financement de la sécurité sociale pour 1999, op. cit.*

[978] Retrouvez notre analyse de l'accès permanent au SNIIRAM dans la Partie I de la présente étude.

[979] V. Partie II, Titre I.

[980] Le premier arrêté relatif au SNIIRAM est l'arrêté du 11 avril 2002, *op. cit*., puis l'arrêté qui adapte, durablement, l'accès aux données de santé est celui du 20 juin 2005, *op. cit*.

[981] 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.*

[982] Directive 95/46/CE 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.

peu nombreux mais sont hautement critiques : se trouve d'une part le risque de ré-identification[983], d'autre part le risque de mésusage[984].

353. A propos du risque de ré-identification, le facteur de risque repose principalement sur le contenu de la donnée et la capacité de l'acteur qui traite la donnée à la recouper avec d'autres. Comme le rappellent H. TANGHE et P.-O. GIBERT[985], une donnée non nominative qui ne comporte ni le nom, ni le prénom de l'individu, est potentiellement ré-identifiante et présente un risque pour la vie privée : ainsi, dès l'année 2000, la chercheuse américaine L. SWEENEY a démontré que 87% de la population de son pays pouvait être identifiée à l'aide du croisement du code postal, de la date de naissance et du sexe[986]. Aujourd'hui, la démocratisation et l'évolution des nouvelles technologies favorise la production de données potentiellement ré-identifiantes si un traitement spécifique leur est appliqué. Mais cela ouvre un autre débat[987] que nous poursuivrons dans le cadre du prochain titre[988].

354. S'agissant du risque de mésusage des données de santé, l'appréciation du « *danger* » qui menace est bien plus subtile et dépend de chacun des cas envisagés. P.-L. BRAS décrit parfaitement la signification de ce risque dans son rapport remis en 2013[989] : les données de santé de l'assurance maladie n'ont de sens que lorsqu'elles sont traitées de manière adéquate et mises en perspective avec le contexte dans lequel elles s'inscrivent. Pour appuyer cette explication, nous pouvons citer l'un des exemples donnés dans ledit rapport qui souligne qu'une

---

983 Sur le risque de réidentification, v. *supra* n° 58 et BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 26, p. 49, p. 55 ; De KERVASDOUE J. et SICARD D., « Plus grave que le débat sur la pilule, l'affaire des données de santé publique », *op. cit.* ; TANGHE H., GIBERT P.-O., « L'enjeu de l'anonymisation à l'heure du Big Data », *Revue française des affaires sociales*, 2017/4, p. 79-93.

984 V. BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 45-46 ; BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé*, 9 juillet 2014, p. 43, p. 54 ; DEBOST C., « Publication du rapport sur la gouvernance et l'utilisation des données de santé, la promesse d'un entrebâillement de l'Open data dans le secteur de la santé ? », *RDS*, janvier 2014, n° 57, p. 947 à 949 ; DESMARAIS P, « Open data santé, un rapport décevant pour un retard de transposition certain ? », *JCP A*, 08/09/2014, n° 36, 716 ; GORCE G. et PILLET F., Rapport d'information au Sénat, *La protection des données personnelles dans l'open data : une exigence et une opportunité*, 16 avril 2014, p. 60.

985 TANGHE H., GIBERT P.-O., « L'enjeu de l'anonymisation à l'heure du Big Data », *op. cit.*

986 SWEENEY L., « Uniqueness of simple Demographic in the U.S. population », *Carnegie Mellon University, Pittsburgh*, 2000, *in* TANGHE H., GIBERT P.-O., « L'enjeu de l'anonymisation à l'heure du Big Data », *op. cit.*

987 Dans leur article, *ibid.*, les auteurs TANGHE H. et GIBERT P.-O. soulignent, à la page 4 du document, l'opposition intrinsèque qui existe entre la protection de la vie privée par l'anonymisation des données, et la démocratisation des traitements de données à grande échelle, ou big data : « *la recherche de l'anonymisation paraît alors contradictoire avec l'essence même du big data* ».

988 *Infra* n° 528 à 533.

989 BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 45-46.

« *différence entre deux zones géographiques en matière de densité médicale doit, au moins, être pondérée par le niveau d'activité des praticiens pour apprécier le niveau de service de soins dont bénéficient les résidents de la zone* ». En 2014, les auteurs P. BURNEL et F. VON LENNEP ont, pour leur part, proposé leur solution pour limiter les risques de mésusage qui vise à « *inciter les utilisateurs à rendre compte des méthodes utilisées pour traiter les données* »[990].

355. Nous serions tentés de penser que l'architecture de l'accès sélectif a été basée autour de ces problématiques identifiées et analysées par différents groupes de travail. Pourtant, chronologiquement, le système d'accès sélectif s'est développé une dizaine d'années[991] avant que des réflexions poussées soient menées en France sur le thème d'une meilleure accessibilité des bases de données en santé qui soit compatible avec les impératifs de protection de la vie privée. Cependant, la logique aurait voulu que l'inverse se produise, avec des avis et rapports remis avant le lancement de l'accès sélectif. Ce simple constat de l'inversement chronologique entre la mise en pratique et la réflexion théorique est intéressant : une telle situation est de nature à favoriser la naissance de dysfonctionnements à plusieurs niveaux, tant du fait de la structure même de l'accès sélectif tel qu'il a été conçu, que dans sa mise en œuvre par les différents acteurs impliqués. En effet, comment le législateur et le pouvoir réglementaire auraient-ils pu bâtir une procédure d'accès sélectif correspondant aux capacités des autorités sollicitées et aux attentes des demandeurs potentiels alors que les réflexions préalables nécessaires n'avaient pas été conduites ? Cette interrogation n'amène pas nécessairement de réponse tant celle-ci peut sembler évidente. L'objet du présent chapitre est d'exposer les points de tension de l'accès sélectif tel qu'il a été initialement pensé pour détailler les solutions successives qui ont été apportées jusqu'à la réforme du 26 janvier 2016[992].

356. Deux développements sont envisageables. Le premier consistera à analyser les différents dysfonctionnements dont a pu pâtir l'accès sélectif (Chapitre 1), le second nous conduira à

---

[990] BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé*, *op. cit.*, p. 43.

[991] Le premier arrêté officialisant la possibilité d'accéder, sur autorisation préalable, aux données du SNIIRAM date du 11 avril 2002, *op. cit.*, tandis que les avis et rapports remis dans le cadre des réflexions autour d'une plus grande souplesse dans l'accès sélectif datent du début des années 2010 avec notamment l'avis de la Conférence Nationale de Santé, *Avis sur les données de santé informatisées*, 19 octobre 2010, 11 p. ; ainsi que le rapport GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *Pour une meilleure utilisation des bases de données administratives et médico-administratives nationales pour la santé publique et la recherche*, 2012, 56 p.

[992] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

détailler et comprendre les adaptations demandées puis opérées par la réforme du 26 janvier 2016[993] (Chapitre 2).

[993] *Ibid.*

CHAPITRE I
L'ACCÈS SÉLECTIF ENTRAVÉ PAR SES DYSFONCTIONNEMENTS

357. L'accès sélectif a, dès sa conception, été bâti autour de critères destinés à protéger la vie privée par la création de multiples contrôles, *a priori* et *a posteriori*, que nous avons présentés dans le titre précédent[994]. Ces impératifs, s'ils ont permis, et permettent encore aujourd'hui, la sécurité de l'accès sélectif, ont également conduit à décourager les potentiels demandeurs d'accès en raison des difficultés qui pouvaient être rencontrées. L'étude de ce qui pourrait être qualifié de freins à l'accès sélectif se décompose donc en deux étapes essentielles : l'examen des éléments signalant un affaiblissement de l'accès sélectif dans un premier temps (Section 1), puis dans un second temps, l'analyse concrète des blocages émaillant l'accès sélectif, une fois autorisé (Section 2).

SECTION 1 : L'ACCÈS SÉLECTIF AFFAIBLI PAR SA STRUCTURE

358. L'accès sélectif aux données de santé est entièrement encadré par une série de textes[995] qui ont évolué et ont été mis à jour avec le temps. Ces textes définissent les données accessibles, les acteurs impliqués, et surtout une procédure stricte, comprenant de nombreuses subtilités. Mais il existe un écart important entre la théorie et la pratique : il est donc nécessaire de dresser le bilan objectif des signes avant-coureurs de l'inadaptation de la procédure (§1), puis il convient de mettre en relation ces signes avec la confusion qui a pu être provoquée par la multiplicité des acteurs intervenant lors de la procédure (§2).

Paragraphe 1 : Le constat de l'inadaptation de l'accès sélectif

359. L'objectif du traitement des données de santé à caractère personnel est, avant tout, l'intérêt général et notamment la santé publique comme le soulignait G. BRAIBANT dans son rapport remis en 1998[996]. Il y indiquait que « *les progrès des technologies de l'information permettent*

[994] V. Partie II, Titre I.

[995] Nous pouvons notamment citer, de manière non exhaustive, les lois n° 98-1194 du 23 décembre 1998, *op. cit.*, n° 2004-801 du 6 août 2004, *op. cit.*, les arrêtés du 11 avril 2002, *op. cit.*, du 20 juin 2005, *op. cit.*, mais aussi du 19 juillet 2013, *op. cit.*

[996] BRAIBANT G., *Données personnelles et société de l'information : transposition en droit français de la directive n° 95-46 / rapport au Premier Ministre*, la Documentation française, 1998, p. 5.

de franchir de véritables sauts qualitatifs, aussi bien dans la garantie des droits individuels à la santé que dans une démarche globale de santé publique ». Ainsi, bien avant la parution du premier arrêté relatif à la mise en œuvre du SNIIRAM[997], créant le premier accès sélectif, l'auteur avait déjà isolé et identifié l'intérêt de pouvoir accéder à des données préalablement codées pour permettre « *de garantir simultanément la fiabilité des échantillons et leur anonymat* » dans le cadre de la recherche scientifique. C'est dans cette optique d'utilisation des données de santé que l'accès sélectif a été créé avec l'installation, en 2005[998], d'un mécanisme qui a perduré jusqu'à la réforme de 2016[999].

360. Etant donné la sensibilité des données contenues dans la base SNIIRAM et les risques[1000] qui pèsent sur la protection de la vie privée dans le cadre de leur traitement automatisé, le législateur a mis en place une procédure contraignante[1001] permettant de contrôler les demandes d'accès. Cette procédure était supposée permettre aux acteurs ne disposant pas d'un accès permanent[1002] de déposer une demande d'accès à des données spécifiques : si l'on prend en considération la stricte rédaction des textes, ce mécanisme aurait dû mener à une diffusion de données de santé issues du SNIIRAM de manière fluide mais contrôlée et respectueuse de la vie privée des individus. Or, la pratique a montré que si la protection de la vie privée a bien été au cœur de toutes les préoccupations, la diffusion des données de santé s'est trouvée freinée par une procédure grippée de l'intérieur.

361. L'élément principal permettant de se rendre compte de l'inadaptation de la procédure d'accès sélectif à l'usage qui lui est réservé, notamment l'évaluation et l'analyse des activités de soins et de prévention, est son faible taux de recours. A titre d'exemple, en 2010, soit un peu plus de 7 ans après la création de l'accès sélectif, l'Institut des données de santé[1003] ne recensait qu'un peu moins de 20 demandes d'accès au SNIIRAM provenant d'organismes publics et privés divers d'après le rapport de M. GOLDBERG[1004]. Si l'on se base précisément sur le

[997] Arrêté du 11 avril 2002, *op. cit*.

[998] Arrêté du 20 juin 2005, *op. cit.*

[999] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1000] *Supra* n° 53 à 62, 353 et 354.

[1001] *Supra* n° 301 à 322.

[1002] Pour l'analyse de l'accès permanent, v. Partie I.

[1003] A partir de l'arrêté du 20 juin 2005, *op. cit.*, l'Institut des données de santé est devenu la porte d'entrée à l'accès sélectif. V. *supra* n° n° 301 à 322.

[1004] GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *Pour une meilleure utilisation*

rapport remis par l'Institut des données de santé au Parlement en 2010[1005], les informations sont plus impressionnantes : seulement 3 demandes d'accès sélectif ont été reçues en 2008, 9 demandes en 2009, et 13 demandes entre les mois de janvier et août 2010. Le rapport de l'Institut des données de santé daté de 2015[1006] donne, lui, le détail des demandes approuvées (contrairement à celui de 2010 qui ne donnait que le nombre de demandes reçues) : 7 en 2009, 11 en 2010, dix-huit en 2011, 17 en 2012, 25 en 2013, puis 49 en 2014 et 34 à la fin du mois de septembre 2015. Entre les premières réunions de travail de l'Institut des données de santé en 2008[1007] et celles de 2015 (jusqu'au mois de septembre de cette année-là), seulement 161 autorisations d'accès sélectif ont donc été délivrées, ce qui est relativement faible compte tenu du délai de 7 ans et de l'utilité reconnue et même vantée que représentent les données contenues dans le SNIIRAM.

La tendance s'est inversée dans les années qui ont suivi. La consultation du document de travail de l'Institut des données de santé regroupant les demandes d'accès sélectif déposées jusqu'en 2017[1008] révèle qu'en 9 ans d'activité (soit de 2008 à 2017), 255 demandes ont été approuvées par le groupement d'intérêt public (sur un total de 321 dossiers déposés) : c'est alors plus d'un tiers (36,8% exactement) des autorisations d'accès sélectif qui ont été délivrées sur les deux dernières années d'existence de l'Institut des données de santé. Nous pouvons saluer la montée en charge très nette qui a été opérée pendant les années 2016 et 2017. Cela semble être le signe d'une meilleure maîtrise de la procédure et de son bon fonctionnement. Cependant, deux remarques peuvent être formulées à l'égard de ce constat.

362. La première remarque a trait au délai qui a été nécessaire pour que les acteurs concernés par le droit de demander un accès sélectif aux données du SNIIRAM soient au fait de la possibilité qui leur était offerte. Le faible taux de demande d'accès sélectif n'est pas nécessairement lié à l'efficacité ou l'inefficacité de la procédure bien que, nous y reviendrons

des bases de données administratives et médico-administratives nationales pour la santé publique et la recherche, 2012, p. 13.

[1005] Institut des données de santé, « Enjeux et étapes », *Rapport au Parlement*, 2010, p. 43.

[1006] Institut des données de santé, « Ouverture, qualité, partage : des avancées », *Rapport au Parlement*, 2015, p. 26.

[1007] Rappelons que, bien que créé par l'arrêté du 20 juin 2005, *op. cit.*, l'Institut des données de santé n'a été installé que par l'arrêté du 30 avril 2007 *portant approbation du groupement d'intérêt public « Institut des données de santé »*, JORF n° 109 du 11/05/2017.

[1008] Institut des données de santé, « Workflow sur les demandes d'utilisation des données du SNIIRAM », 03/05/2017.

ultérieurement[1009], il s'agisse d'un facteur important. Ce manque d'attractivité de l'accès sélectif pendant ses premières années d'existence est également probablement dû à une absence de réelle volonté de communiquer sur les possibilités offertes par le mécanisme. Nous le constatons aujourd'hui avec la mise en œuvre du nouveau SNDS[1010], les autorités responsables de ce nouveau système sont très actives en termes de communication, de mise en ligne de guides d'utilisation, et de pédagogie à destination des utilisateurs potentiels[1011]. Or, pour la mise en œuvre de l'accès sélectif nécessitant un avis préalable de l'Institut des données de santé, aucune campagne de cette ampleur n'avait été réalisée. Si le site du groupement d'intérêt public[1012] propose bien des documents à consulter pour comprendre le fonctionnement de l'accès sélectif, sa structure peu intuitive et l'absence d'un guide clair destiné à aiguiller le demandeur potentiel dans sa démarche sont de nature à décourager l'utilisateur et à conférer à l'accès sélectif un usage confidentiel. Signalons toutefois l'existence d'un « *Mode d'emploi pour l'utilisation des données du SNIIRAM* », mis en ligne tardivement en septembre 2012, qui récapitule en trois pages succinctes les grandes étapes de l'accès sélectif. Un sentiment de contradiction émane de cette situation : la possibilité d'avoir un accès, sur autorisation préalable, aux données du SNIIRAM a été créée pour que lesdites données soient utilisées à des fins d'intérêt général, or pour que cet objectif d'œuvrer en faveur de l'intérêt général soit atteint, il faut que ce mécanisme fasse l'objet d'une communication suffisante pour être utilisé par le maximum de bénéficiaires visés par les textes. Dans la pratique, il semble que les opportunités offertes par l'accès sélectif, tel qu'il existait avant la réforme, ont été insuffisamment diffusées pour être portées à la connaissance de tous les demandeurs potentiels. Ce manque de promotion du dispositif n'a pu que nuire à son essor et participe de son affaiblissement.

363. La seconde remarque vise le rapport qui peut être fait entre la proportion du nombre de demandes reçues par l'Institut des données de santé et le nombre potentiel de demandeurs. Nous nous rendons rapidement compte que le système d'accès sélectif, tel qu'il existait avant la réforme n'a pas atteint son objectif de servir l'intérêt général. En effet, comme nous l'avons

[1009] *Infra* n° 365 à 371.

[1010] Le Système national des données de santé (SNDS) a été créé par la loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1011] Le site du SNDS peut être visité à l'adresse suivante : www.snds.gouv.fr

[1012] Le site était consultable à l'adresse www.institut-des-donnees-de-sante.fr mais il a été délaissé au profit du nouveau site www.indsante.fr.

exposé dans le précédent titre[1013], à partir de l'arrêté de 2005[1014], tous les organismes de recherches, universités, écoles ou autres structures d'enseignement liés à la recherche que ceux disposant de l'accès permanent ont automatiquement été concernés par le bénéfice de l'accès sélectif, à l'exception des organismes qui poursuivent un but lucratif. Cette définition des bénéficiaires potentiels de l'accès sélectif aux données du SNIIRAM est alors extrêmement large lorsque nous avons à l'esprit qu'il existe en France plus de soixante universités[1015], si nous ajoutons à cela toutes les autres écoles, structures d'enseignement et de recherche[1016], il apparaît clairement que l'utilisation « normale » de l'accès sélectif par ses bénéficiaires désignés aurait dû conduire au dépôt d'un nombre bien plus élevé de demandes que les trois-cent-vingt-et-unes comptabilisées en neuf ans par l'Institut des données de santé.

364. Ces éléments objectifs appuient l'idée selon laquelle l'accès sélectif n'a pas eu les moyens de démontrer son plein potentiel. Mais un autre facteur non moins important nous amène à penser que le fonctionnement de l'accès sélectif ne pouvait pas être optimal : c'est celui de la confusion entrainée par la multiplicité des acteurs intervenant au cours de la procédure.

Paragraphe 2 : La dispersion des compétences nuisible à l'accès sélectif

365. Pour tenter d'expliquer pourquoi les demandes d'accès aux données de santé furent déposées en si petite quantité dans le cadre de l'accès sélectif[1017], nous devons avant tout nous mettre à la place d'un demandeur qui découvre la procédure. Cela a été indiqué précédemment[1018], la démarche de communication, d'explication et de présentation de la marche à suivre pour obtenir des données de santé provenant du SNIIRAM n'était pas le point fort du système. Dès lors, il n'est pas difficile d'imaginer la réaction que pouvait avoir un bénéficiaire, profane concernant l'accès sélectif, en découvrant les acronymes des acteurs impliqués et les rôles qui leurs étaient attribués : CNIL, CCTIRS (Comité consultatif sur le

[1013] *Supra* n° 302 à 310.

[1014] Arrêté du 20 juin 2005, *op. cit.*

[1015] Au 1er janvier 2018, il existait 67 universités et 1 institut national polytechnique.

[1016] Nous pouvons, à titre d'exemples non exhaustifs, indiquer que le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation compte au moins 36 établissements publics de recherche, 137 établissements publics à caractère scientifique, culturel et professionnel (dont les 67 universités et l'institut national polytechnique), 96 établissements publics à caractère administratif, 11 groupements d'intérêts publics, auxquels nous pouvons ajouter les 32 Centres Hospitaliers Universitaires de France.

[1017] *Supra* n° 359 à 364.

[1018] *Ibid.*

traitement de l'information en matière de recherche dans le domaine de la santé), IDS (Institut des données de santé), sachant qu'un acteur supplémentaire, le groupement d'intérêt public (GIP) « études en santé publique » a bien failli s'ajouter à cette liste. Mais, fort heureusement pour le demandeur d'accès probablement déjà perdu dans la variété des normes applicables, il n'en fut rien. Le GIP aurait dû être constitué par l'Etat, la HAS, l'ANSM, l'InVS et la CNAMTS, aux termes de la loi du 29 décembre 2011[1019], afin d'autoriser les accès aux données de santé à des fins d'études en santé publique de vigilance et d'épidémiologie. Mais le décret censé entériner la création de ce nouvel acteur n'a jamais été publié[1020].

366. L'existence de plusieurs points d'entrée pour demander un accès sélectif constitue le premier facteur déterminant dans le manque de clarté du dispositif. Comme l'indique P.-L. BRAS dans son rapport, « *les voies par lesquelles la demande est instruite sont multiples et imbriquées de sorte qu'il n'est pas facile de savoir où s'adresser* »[1021]. Si c'est bien la CNIL qui a toujours la responsabilité de décider d'autoriser, ou de refuser, une demande d'accès sélectif aux données du SNIIRAM, l'interlocuteur initial n'est, à aucun moment, clairement défini. Avant la création de l'Institut des données de santé[1022], c'est directement à la CNIL que les demandeurs devaient s'adresser d'après l'arrêté de 2002[1023]. Puis avec la transposition de la directive européenne de 1995[1024] et la parution de l'arrêté de 2005[1025], la nouvelle version des textes a mis en avant le CCTIRS et l'IDS. Le demandeur devait alors fournir un effort conséquent pour se plonger dans les textes législatifs et réglementaires. Il devait d'abord s'appuyer sur le texte de l'arrêté pour savoir que c'est auprès de l'IDS qu'il devait faire sa demande d'accès sélectif. Mais, dans le cas où son projet de recherche en santé impliquait aussi la personne humaine, son interlocuteur changeait et devenait prioritairement le CCTIRS avant

[1019] Loi n° 2011-2012 du 29 décembre 2011 *op. cit.*

[1020] *Supra* n° 110.

[1021] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 36.

[1022] L'Institut des données de santé a été créé par l'arrêté du 20 juin 2005, *op. cit.*, puis installé par arrêté du 30 avril 2007, *op. cit.*

[1023] Arrêté du 11 avril 2002, *op. cit.* : « *Toute autre demande d'accès à des données individuelles relatives aux bénéficiaires devra faire l'objet d'une demande d'autorisation auprès de la CNIL dans les conditions prévues aux articles 40-11 à 40-15 de la loi du 6 janvier 1978 susvisée* ».

[1024] Directive 95/46/CE du 24 octobre 1995, *op. cit.*,transposée en droit français par la loi n° 2004-801 du 6 août 2004, *op. cit*.

[1025] Arrêté du 20 juin 2005, *op. cit*.

que le dossier ne soit réexaminé par l'IDS. Or, pour connaître cette subtilité, ce n'est plus l'arrêté qu'il fallait lire, mais la loi relative à l'informatique et aux libertés[1026].

Bien que la présence de deux ou trois portes d'entrée différentes à l'accès sélectif soit critiquable c'est avant tout la méthode utilisée par le législateur pour les présenter qui est discutable. En effet, le manque de pédagogie à l'attention des utilisateurs potentiels, ajouté au fait que les procédures puissent s'imbriquer sans davantage d'explications concrètes et l'empilement successif des normes juridiques ont participé à complexifier le mécanisme et, semble-t-il, à en faire un repoussoir plutôt qu'une opportunité à saisir. L'objet de cette réflexion n'est pas de dénoncer la complexité du système car cette complexité est inhérente au caractère sensible des données convoitées. Ceci étant signalé, les évolutions de l'accès sélectif auraient pu, à défaut de devoir s'accompagner d'un travail effectué en amont sur son application en situation réelle pour atteindre l'objectif d'intérêt public annoncé. Un simple document officiel récapitulant les chemins à emprunter en tant que demandeur d'accès aux données de santé du SNIIRAM, en fonction des finalités envisagées, aurait probablement suffi à aiguiller les acteurs profanes désirant bénéficier de l'accès sélectif.

367. Pour illustrer le fait que les demandeurs sont, d'une certaine manière, livrés à eux-mêmes dans leur démarche et dépendent de la moindre subtilité, nous pouvons étudier le chevauchement des examens dont relève la demande d'accès sélectif qui concerne la recherche en santé impliquant la personne humaine associée, en guise de complément, à l'extraction de données de santé à caractère personnel issues du SNIIRAM. En effet, nous l'avons évoqué précédemment[1027], il est possible de déposer une demande d'accès sélectif dans le cadre d'un traitement ayant pour fin la recherche dans le domaine de la santé. Deux procédures se chevauchent donc, celle qui est liée à la recherche dans le domaine de la santé, qui implique que le CCTIRS rende son avis sur le dossier, puis celle qui est liée à l'accès sélectif, qui implique que l'IDS rende également son avis sur le dossier. Enfin, la CNIL prend la décision finale. Or, cela n'est précisé à aucun endroit dans les textes législatifs et réglementaires, dès lors qu'un dossier obtient un avis favorable de la part du CCTIRS, l'IDS donne apparemment un avis systématiquement positif et la CNIL autorise sans sourciller la demande d'accès au SNIIRAM.

[1026] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1027] *Supra* n° 302 à 308.

Cet état de fait, dévoilé par M. GOLDBERG dans son rapport remis en 2010[1028], est, en soi, une bonne nouvelle pour le demandeur qui n'a pas à redouter un avis négatif de l'IDS dès lors que le CCTIRS s'est prononcé en faveur du projet. Cependant, cette subtilité qui relève d'un accord entre les trois « *gardiens* » des données de santé n'est pas officiellement édictée. De plus, si un premier avis favorable entraîne l'autorisation systématique de l'accès sélectif demandé puis du traitement envisagé, nous pouvons déduire qu'un avis défavorable lors de l'examen par le CCTIRS a un effet négatif sur l'entièreté de la procédure ultérieure. Cela reste une supposition mais le raisonnement paraît fondé considérant les révélations faites par M. GOLDBERG. Ces règles du jeu officieuses, qui restent inconnues des principales personnes concernées que sont les bénéficiaires de l'accès sélectif, sont caractéristiques du fonctionnement de l'accès sélectif avant la réforme du 26 janvier 2016[1029]. Elles ajoutent une dose supplémentaire d'incertitude qui impacte l'intégralité du dispositif, ce qui nuit à son attractivité.

368. Après avoir témoigné des difficultés que la multiplicité d'intervenants que sont l'IDS, le CCTIRS et la CNIL, peut engendrer chez les bénéficiaires de l'accès sélectif, il est important d'aborder le sujet lorsque nous nous plaçons du côté desdits intervenants. La Cour des comptes s'est essayée à l'exercice dans son rapport daté de mars 2016[1030]. Mais, nous pouvons le regretter, les rédacteurs du document n'analysent pas les risques et difficultés pouvant être engendrées dans le cadre de l'accès sélectif et traitent la problématique du nombre élevé d'acteurs uniquement par le prisme de la gouvernance du SNIIRAM. Bien que le sujet de la gouvernance soit bien plus étendu que celui de l'accès sélectif, les enseignements exposés par les magistrats de la Cour des comptes apportent un éclairage nouveau à notre analyse.

Ainsi, le rapport indique clairement que les « *nombreux acteurs* [sont] *mal coordonnés* »[1031] en citant notamment l'IDS et la CNIL. Il indique que si le comité d'orientation et de pilotage de l'information interrégimes (COPIIR) était, depuis 2001, seul habilité à assurer le pilotage

[1028] GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *op. cit.*

[1029] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1030] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *Communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale*, 03/2016, 176 p.

[1031] *Ibid.* p. 8.

stratégique du SNIIRAM, un nouvel intervenant, l'IDS, est venu lui disputer sa suprématie, puis la CNAMTS elle-même a progressivement repris le flambeau de la gouvernance à partir de 2010[1032]. Un parallèle peut être fait entre la dispersion des acteurs et des compétences dans le cadre de la gouvernance du SNIIRAM d'une part, et les multiples portes d'entrée de l'accès sélectif qui impliquent potentiellement, au gré de l'évolution du mécanisme, trois entités différentes[1033], d'autre part. Nous retrouvons dans les deux cas plusieurs éléments similaires : la coexistence d'acteurs divers et la définition de missions qui peuvent parfois se rejoindre et se confondre, le tout pouvant faire émerger une certaine confusion aussi bien entre les intervenants eux-mêmes que chez les tiers qui pourraient les solliciter. En somme, un tel imbroglio qui entremêle sans distinction les aspects théoriques et les aspects pratiques ne peut être dénoué et simplifié que par une réforme en profondeur de l'accès sélectif, et, plus largement, de la gouvernance des données de santé dans son ensemble. C'est notamment l'un des objectifs de la réforme du 26 janvier 2016[1034] dont les apports seront étudiés dans le prochain chapitre[1035] de cette partie.

369. Nous constatons donc que les compétences inhérentes à l'accès sélectif sont dispersées entre plusieurs acteurs, faisant ainsi écho aux modalités de gouvernance du SNIIRAM. Cette atomisation n'est pas un problème en soi : tout dépend de la façon dont cela est expliqué aux usagers du système qui doivent être en mesure d'appréhender concrètement la procédure à suivre. Or, nous venons de le détailler, la pédagogie n'était pas le point fort de l'accès sélectif avec le chevauchement des procédures, ou encore la création (parfois ratée[1036]) de nouveaux acteurs.

[1032] *Ibid.* p. 21.

[1033] L'Institut des données de santé (IDS) dans le cadre d'évaluations ou d'analyses des pratiques ou des activités de soins et de prévention, le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé (CCTIRS) dans le cadre de la recherche dans le domaine de la santé, et la Commission nationale informatique et libertés (CNIL) qui, dans les deux cas, doit délivrer l'autorisation finale d'accès et de traitement. Rappelons qu'avant la création de l'IDS par la loi 2004-810 du 13 août 2004, *op. cit.*, puis par l'arrêté du 20 juin 2005, *op.cit.*, aboutissant à son installation par l'arrêté du 30 avril 2007, *op.cit.*, la CNIL était l'unique interlocuteur dans le cadre de l'accès sélectif aux données de santé n'ayant pas pour objet la recherche dans le domaine de la santé.

[1034] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1035] *Infra* n° 393 à 442.

[1036] Nous faisons ici référence au GIP composé de l'Etat, de la HAS, de l'ANSM, de l'InVS et de la CNAMTS, *supra* n° 365.

370. L'accès sélectif ne semble pas avoir été optimisé pour une utilisation facile et régulière au profit de ses éventuels bénéficiaires. Le faible nombre de demandes déposé[1037] et la confusion provoquée par la multiplicité des acteurs jouent un rôle capital dans le manque de recours au dispositif. Cependant, il ne faut pas omettre d'analyser les difficultés apparaissant lorsque les bénéficiaires se lançaient dans le dépôt et l'obtention d'une demande d'accès sélectif. Les obstacles à une démocratisation de l'utilisation de cet accès sont, alors, encore plus flagrants, c'est tout l'objet du paragraphe suivant.

SECTION 2 : L'ACCÈS SÉLECTIF DÉCRÉDIBILISÉ PAR SES BLOCAGES INTERNES

371. Les signes extérieurs des dysfonctionnements de l'accès sélectif[1038] ne sont pas de nature à expliquer, seuls, l'échec relatif de ce mécanisme. Des éléments bien plus concrets méritent d'être étudiés afin de comprendre les raisons qui ont poussé le pouvoir législatif et réglementaire à proposer une réforme globale. Deux problèmes sont discernables : celui de la complexité des données contenues dans les bases accessibles via l'accès sélectif (§1), et celui de l'incapacité des intervenants à faire aboutir la procédure dans les temps impartis (§2).

Paragraphe 1 : La complexité des données issues de l'accès sélectif

372. L'objectif annoncé de l'accès sélectif aux données du SNIIRAM est de permettre à ses bénéficiaires d'avoir un moyen d'obtenir des données dans le cadre de l'évaluation ou de l'analyse des pratiques ou des activités de soins et de prévention[1039]. La démocratisation de ce mécanisme et son utilisation, poussée au maximum de son potentiel, ne peut être réalisée qu'à des conditions particulières. S'il faut avant tout que les chemins d'accès soient limpides afin de favoriser l'accroissement du nombre de dépôts de demandes[1040], il paraît aussi très utile que les données proposées soient utilisables rapidement et compréhensibles par les destinataires finaux. Pourtant, cette logique ne semble pas aller de soi et la complexité des données fait partie des grands obstacles au développement de l'accès sélectif.

[1037] *Supra* n° 359 à 364.

[1038] Tels que le faible taux de recours, ou l'absence de communication claire sur les processus clefs.

[1039] Il s'agit de l'intitulé du chapitre X de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifié par la loi n° 2004-801 du 6 août 2004, *op. cit.*, dont la procédure était la référence en matière d'accès sélectif entre l'arrêté du 20 juin 2005, *op. cit.*, et la loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1040] *Supra* n° 361.

373. Nous le savons[1041], la base de données SNIIRAM contient des milliards de données. La volumétrie a son importance : elle induit une architecture nécessairement détaillée permettant de « *classer* » toutes les données au bon endroit. Si nous nous permettions de faire une analogie, nous pourrions parler de « *bibliothèque d'Alexandrie* » numérique de l'Assurance maladie[1042]. Et cette expression serait probablement un euphémisme tant la quantité de données est grande. Dans son rapport[1043], pour expliquer à quel point la base de données SNIIRAM est compliquée à appréhender, P.-L. BRAS dévoile quelques nombres évocateurs. La base contenait ainsi près de 20 milliards de lignes de prestation en 2013, ces données étaient dispersées en 7 dictionnaires et 785 000 objets (l'auteur donne l'exemple de tables, d'index, de synonymes…). De son côté, la Caisse nationale d'Assurance maladie indiquait[1044] en 2011 que le SNIIRAM répartissait ses données dans trois bases ayant chacune une volumétrie supérieure à 18 TéraOctets[1045] ce qui est considérable pour cette époque. Le volume de données contenu dans le SNIIRAM passé reste moindre par rapport à ce que contient le SNDS[1046] aujourd'hui, ce qui nous laisse penser que des solutions existent nécessairement pour faciliter l'utilisation de cette masse d'informations numérisées.

374. Dans le cadre de l'accès sélectif, avant d'arriver dans les mains du demandeur initial, les données doivent être identifiées, récupérées et regroupées par les gestionnaires des bases de données. Cette étape est importante à souligner car son étude permet de comprendre ce que la masses d'informations quantitatives vue au point précédent[1047] provoque comme véritable impact sur la pratique. En effet, la complexité de la base SNIIRAM a des effets directs sur les gestionnaires chargés de procéder au traitement de la demande d'accès sélectif, or, comme l'indique le rapport BRAS : « *une part de cette complexité est irréductible, un prix à payer pour la richesse de la base qui ne se laisse pas connaître sans efforts et justifie que les utilisateurs s'organisent autour de pôles de compétence comme ont commencé à le faire les*

[1041] *Supra* n° 22, 93, 238.

[1042] Cette expression n'est, sauf erreur de l'auteur de ces lignes, pas une citation provenant d'un ouvrage tiers.

[1043] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 41.

[1044] POLTON D., RICORDEAU P., « Le SNIIRAM et les bases de données de l'Assurance Maladie en 2011 », *CNAM*, 30/03/2011.

[1045] Un TéraOctet représente 1 000 GigaOctets. 18 TéraOctets représentent donc 18 000 GigaOctets.

[1046] *Supra* n° 330.

[1047] *Supra* n° 373.

épidémiologistes, avec le soutien financier de la CNAMTS »[1048]. Un autre auteur, M. GOLDBERG, évoque les moyens colossaux qui doivent être en œuvre pour assurer l'extraction de données demandées notamment dans le cadre de l'accès sélectif : cela implique « *des moyens humains, et une organisation rigoureuse : formulation des requêtes en fonction des besoins des utilisateurs, tests, production, vérifications, transferts sécurisés…* »[1049]. Nous le comprenons en lisant le contenu des rapports produits sur le sujet, le facteur humain est central dans la réussite de l'accès sélectif.

375. Au-delà de la taille de la base qui crée, dès l'origine, une barrière à surmonter, c'est aussi la composition brute des données qui rend leur exploitation directe difficile : des problématiques insoupçonnées entrent en jeu et compliquent davantage les manipulations envisagées. Pour illustrer cet état de fait, le rapport annuel relatif au SNIIRAM pour 2011 détaille les principales questions qu'un gestionnaire doit se poser avant même de construire une requête informatique. Le cas mis en exergue[1050] est celui où le demandeur souhaite connaître les effectifs des personnes ayant bénéficié d'une Assistance Médicale à la Procréation (AMP) et d'une Fécondation *In Vitro* (FIV). Huit questions[1051] sont posées, chacune exigeant un degré d'expertise accru pour y répondre convenablement. Dans le même temps, M. GOLDBERG indique[1052] qu'une « *connaissance suffisante des bases de données par nature très complexes, de leur structure, des données enregistrées, des nomenclatures utilisées, et des évolutions constantes est indispensable pour les utiliser correctement* ». Il ajoute que cela « *implique un investissement intellectuel important, le plus souvent sans commune mesure avec les ressources des équipes potentiellement concernées, particulièrement quand il s'agit d'une étude ponctuelle de durée limitée* ». Autrement dit, les demandes d'accès sélectif aux données de santé, qui rentrent dans la catégorie des études ponctuelles de durée limitée, demandent un investissement humain bien trop important en comparaison avec le résultat final de la requête réalisée. C'est

[1048] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.*, p. 42.

[1049] GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *op. cit.*, p. 34.

[1050] POLTON D., RICORDEAU P., « Le SNIIRAM et les bases de données de l'Assurance Maladie en 2011 », *op. cit.*, p. 49.

[1051] Parmi ces questions, nous pouvons citer les suivantes : « *Quels sont les traitements médicamenteux aujourd'hui utilisés et les examens biologiques spécifiques ?* », « *Comment les inducteurs de l'ovulation sont-ils facturés par les hôpitaux (inclus dans les séjours, facturés en sus des forfaits, rétrocédés) ?* », « *Quels sont les délais de transmission de ces informations (actes techniques, médicaments) par les établissements et les professionnels et ces délais de transmission sont-ils homogènes sur l'ensemble du territoire ?* ».

[1052] GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *op. cit.*, p. 35.

un signal fort envoyé par l'auteur du rapport en faveur de la refonte des modalités d'accès aux données, notamment de l'accès sélectif.

376. Consciente des difficultés inhérentes aux données et à leur architecture, la CNAM a procédé par étapes pour aider les équipes dont la mission est de recevoir les demandes d'accès sélectif autorisées afin de les traiter. La première étape menée a consisté dans la conduite d'enquêtes de terrain auprès des utilisateurs. Ces enquêtes ont notamment été diligentées en 2010 et 2012[1053] (soit au moins 2 années après la mise en œuvre de l'accès sélectif) pour recueillir les revendications des personnes dont la mission quotidienne est de réaliser les requêtes dans la base SNIIRAM. Quatre enseignements principaux ont été notés par la CNAM : « *manque de documentation, délai de formation, simplification de certaines bases, information régulière* »[1054]. Si ces 4 éléments sont vraiment succincts et sujets à interprétation, il est probable que les utilisateurs aient émis les demandes suivantes : ils souhaitent avoir plus de documentation sur les bases de données afin de favoriser leur maîtrise du SNIIRAM ; ils souhaitent que le délai de formation soit écourté dans le but d'accroître le volume de personnel compétent ; ils souhaitent que certaines bases soient simplifiées, notamment au niveau de leur architecture, pour faciliter le travail de requêtage[1055] ; enfin, ils souhaitent être destinataires d'une information régulière sur des sujets tels que le contenu des bases, les évolutions techniques envisagées ou en cours.

La seconde étape s'est traduite par la mise en œuvre d'actions spécifiques visant à épauler les personnes habiliter à formuler les requêtes et effectuer les extractions. Ces réponses de la CNAM aux revendications recueillies sur le terrain sont le développement de neuf modules de formation (sans que le détail de ces modules ne soit explicité) ; la mise à disposition d'un « *dictionnaire de concepts* » ainsi que d'un « *dictionnaire de données* » (faisant office de documentation) ; la création de « *forums, de clubs utilisateurs, de supports d'information (lettre trimestrielle, amphi d'information, présentations aux chercheurs)* » (en guise d'information

[1053] POLTON D., « Le SNIIRAM et les bases de données de l'assurance maladie : fonctionnement, potentiel et limites », *CNAM*, 15/07/2013, p. 68.

[1054] *Ibid.*

[1055] Terme technique utilisé en informatique pour signifier le fait de lancer une requête dans une base de données.

régulière) ; et enfin la mise en œuvre de « *bases, notamment EGB*[1056] *simplifié*[1057] » (en retour de la demande de simplification des bases de données).

En revanche, la CNAM concède que des limites pratiques existent quant aux solutions qui peuvent être apportées aux différentes réclamations formulées par les utilisateurs du SNIIRAM. S'agissant de la demande de raccourcissement des délais entre les formations, le nombre de places disponibles est trop faible pour qu'une solution soit trouvée : un problème d'engorgement est clairement détecté et semble incompressible.

377. Nous le comprenons, les facteurs humain et technique se rejoignent lorsque l'on parle de la complexité des données de santé disponibles dans le cadre de l'accès sélectif. Si les personnes chargées de gérer les bases sont, de leur propre aveu, dépassées par la complexité des données disponibles, imaginons ce qu'il en est des bénéficiaires de l'accès sélectif qui n'ont pas accès à la documentation et aux formations délivrées par la CNAM, et qui souhaitent formuler une demande. Le degré de technicité est tel que nous comprenons finalement que les demandes d'accès déposées entre 2007 (année d'installation de l'IDS) et la réforme de 2016[1058], aient été aussi peu nombreuses[1059]. En effet, il est évident que la complexité inhérente aux données brutes extraites ne disparaît pas, ou du moins pas complètement, après le travail de synthèse réalisé par les équipes chargées de traiter les demandes d'accès sélectif. Les bénéficiaires de l'accès sélectif sont finalement tenus d'avoir, en leur sein, un spécialiste de la manipulation des données pour être apte à analyser les fichiers obtenus et les exploiter dans le cadre prévu par leur étude autorisée par la CNIL.

378. Il est primordial de garder à l'esprit que les données disponibles dans le cadre de l'accès sélectif possèdent une part incompressible de complexité. Ceci étant connu, il est intéressant de faire un point sur l'impact des difficultés rencontrées par les gestionnaires sur la fluidité de la procédure et les délais d'aboutissement des demandes déposées. Nous pouvons redouter des

[1056] Sur la définition de l'EGB, v. *supra* n° 148.

[1057] L'EGB simplifié a été mis en œuvre à partir de 2013 par la CNAM et consiste dans la réorganisation des données pour qu'elles soient plus facilement compréhensibles, v. BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit*., p. 70.

[1058] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1059] *Supra* n° 361.

effets négatifs, principalement sur les délais de traitement des demandes qui vont bien au-delà des limites imposées par les dispositions en vigueur.

Paragraphe 2 : Les délais de traitement aléatoires de l'accès sélectif

379. La possibilité d'accéder à des données de santé stockées dans les bases élargies du SNIIRAM est attrayante à partir du moment où les informations demandées et obtenues s'inscrivent dans un projet de recherche, d'étude ou d'analyse[1060]. Ces projets sont réfléchis et financés en amont, planifiés et répondent, bien souvent à des impératifs temporels irréductibles. En effet, un projet de recherche doit aboutir à la production de résultats quelle que soit leur nature, dans un instant donné. Les délais de réalisation de ces travaux, bien que parfois étendus sur plusieurs années, peuvent difficilement souffrir de reports trop nombreux et doivent présenter une prévisibilité fiable tout au long de leur accomplissement.

380. Un projet de recherche qui inclurait, dans son raisonnement, l'accès sélectif à des données issues du SNIIRAM devrait donc proposer un calendrier d'obtention de ces données et de réalisation des traitements. Cette nécessité s'impose, que ces données soient une partie centrale du projet ou de simples éléments parmi d'autres. Nous l'avons étudié dans le titre précédent[1061], le cheminement permettant d'obtenir l'autorisation d'accéder à des données de santé de l'Assurance maladie, en vue de leur traitement, avant la réforme de 2016[1062], est soumis à plusieurs étapes. Chaque étape induit un temps nécessaire d'examen du dossier par l'acteur compétent d'après les textes législatifs et réglementaires. Or, ces délais d'examens sont imprévisibles et instables pour permettre à la recherche de bénéficier sereinement et largement de l'accès sélectif.

381. Commençons par la porte d'entrée de l'accès sélectif prévue dès l'arrêté de 2005[1063] : l'Institut des données de santé (IDS). Nous ne reviendrons pas sur le retard pris dans la mise en

[1060] Si nous distinguons les projets de recherche, d'étude ou d'analyse, c'est simplement parce que la section 2 du chapitre IX de la loi relative à l'informatique et aux libertés du 6 janvier 1978 devenue sous-section 2 de la section 3 du chapitre III du Titre 2 avec l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*, opère cette distinction dans son intitulé : « *Dispositions particulières relatives aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé* ». La différence qui pourrait exister entre les trois termes n'étant pas précisée par le législateur, nous retiendrons le terme générique de recherche dans la présente étude.

[1061] V. Partie II, Titre I.

[1062] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1063] Arrêté du 20 juin 2005, *op. cit.*

place de ce groupement d'intérêt public[1064], qui a véritablement impacté l'effectivité de l'accès sélectif les premières années, pour nous consacrer uniquement au délai d'examen des dossiers. Etant donné que ledit arrêté mentionne clairement que le conseil d'administration de l'IDS doit donner son approbation à tout traitement demandé dans le cadre de l'accès sélectif, le bénéficiaire potentiel de la mesure est en droit de s'attendre à ce qu'un délai de délivrance de la décision soit prévu par les textes. Il est pourtant intrigant de constater que ni le chapitre X de la loi relative à l'informatique et aux libertés[1065], ni les décrets ou arrêtés successifs[1066], n'ont pris soin de déterminer le délai maximum donné à l'IDS pour approuver ou non une demande d'accès sélectif. L'effet « repoussoir » que cette absence d'information produit à l'égard des chercheurs qui pensaient pouvoir inclure des données provenant du SNIIRAM dans leur projet, est immédiat. En effet, comment espérer prédire un calendrier d'étude quand, dès la première étape de l'accès sélectif, une telle inconnue de temps s'immisce dans la procédure ? Nous comprenons, une fois de plus, qu'il s'agit probablement de l'une des raisons pour lesquelles le nombre de demandes d'accès déposées a été si faible entre 2007 et 2016[1067].

382. Cependant, dans la pratique, il semblerait que l'IDS ait eu une politique interne auto-contraignante, c'est-à-dire que le groupement d'intérêt public se serait imposé à lui-même une obligation de rendre sa décision d'approbation ou de désapprobation dans une limite de temps donnée. Examinons ce qu'il en est vraiment. Ainsi, dans un document[1068] qui semble avoir été diffusé par l'IDS au démarrage de son activité, entre 2007 et 2008, nous retrouvons l'information selon laquelle deux types d'examens sont envisagés.

Le premier est un examen par l'IDS dans le cadre d'une demande dite « *offre standard* » qui ne requiert qu'un accès à des données de tableaux de bord, des entrepôts de données agrégées, ou bien à l'EGB. Dans ce cas « *l'IDS émet son avis dans un délai minimum de 2 à 3 mois à réception du dossier complet et correctement rempli ; ce délai est susceptible de varier à l'issue de la première année d'exercice* ».

[1064] *Supra* n° 326.

[1065] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, dans sa version modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1066] Nous pouvons par exemple citer le décret n° 2005-1309 du 20 octobre 2005, *op. cit.*, ou l'arrêté du 19 juillet 2013, *op. cit.*

[1067] *Supra* n° 361.

[1068] Institut des données de santé, « Accès aux données du SNIIRAM : mode d'emploi ».

Le second est un examen par l'IDS dans le cadre d'une demande dite « *offre non-standard* » qui nécessite la création d'un échantillon ad-hoc à partir des données du SNIIRAM. Il est alors indiqué que « *l'IDS émet son avis dans un délai minimum de 6 mois à réception d'un dossier complet et correctement rempli ; ce délai est susceptible de varier à l'issue de la première année d'exercice* ».

383. Deux éléments majeurs retiennent notre attention. D'abord, nous remarquons que l'IDS prend bien soin de ne pas se fixer de délai maximum d'examen. Bien au contraire, le groupement d'intérêt public prévient l'utilisateur de la durée minimum prévue ! Bien que cela donne un premier indice au demandeur concernant la durée d'obtention des données, nous ne pouvons que déplorer ce caractère aléatoire : la seule chose dont le bénéficiaire soit certain, c'est que la première étape de sa demande ne pourra pas aboutir avant des délais minima. Cela signifie surtout que les chances sont grandes pour que lesdits délais d'examen par l'IDS soient supérieurs aux minima mentionnés dans le document.

Ensuite, nous comprenons que la décision de l'IDS, préalable à tout examen par la CNIL, ne pourra pas être délivrée dans un délai inférieur à « *2 à 3 mois* » dans le meilleur des cas pour des fichiers de données déjà constitués, et ce délai ne saurait être moins long que « *6 mois* » dans la configuration idéale s'agissant d'une demande impliquant la création d'un nouveau fichier spécifique de données.

Nous pourrions penser que ces délais plutôt extensibles, étant donné qu'aucune limite maximale de temps n'est donnée, démontrent un certain pessimisme des équipes de l'IDS. Pourtant, P.-L. BRAS donne une explication concrète à cela : le groupement d'intérêt public ne dispose pas « *de moyens et de compétences suffisants pour faire face à ce défi* »[1069].

384. L'examen du dossier par l'IDS est prévu dans le cadre de la procédure d'accès sélectif que nous pourrions qualifier de « classique », c'est-à-dire ne relevant que du chapitre X de la loi relative à l'informatique et aux libertés[1070]. Nous le savons, lorsque le demandeur souhaite accéder à des données du SNIIRAM dans le cadre d'un projet de recherche en santé, il doit dans

[1069] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 37.

[1070] Loi n° 78-17 du 6 janvier 1978, *op. cit*, dans sa version modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

un premier temps soumettre un dossier au CCTIRS[1071]. Le délai alors donné à ce comité spécifique est d'un mois d'après le chapitre IX de la loi relative à l'informatique et aux libertés[1072]. Le point fort intéressant des dispositions relatives au CCTIRS concerne l'effet de son silence : il est prévu que si aucun avis n'est rendu par le comité dans ce délai d'un mois, son avis est réputé favorable. Ce détail est positif pour les acteurs qui déposent une demande de traitement de données dans le cadre du chapitre IX : le silence du comité ne les pénalise pas pour la suite de l'examen de leur dossier par la CNIL.

Une subtilité, déjà évoquée à travers notre étude[1073], n'est pas précisée par les textes. Il s'agit de l'accord qui existait entre le CCTIRS, l'IDS et la CNIL afin que tout avis positif rendu (l'avis non rendu et réputé favorable serait alors exclu de cet accord) par le comité aboutisse nécessairement à une autorisation d'accès aux données de santé du SNIIRAM.

385. Une fois l'examen préalable effectué par l'IDS ou par le CCTIRS, le dossier de demande d'accès sélectif doit être vérifié par la CNIL. Dans les deux cas, la Commission est tenue de rendre sa décision dans un délai de 2 mois renouvelable. Cependant, bien que l'objectif soit le même, les fondements légaux sont différents selon la procédure. En cas d'examen préalable par le CCTIRS, c'est l'article 25 de la loi relative à l'informatique et libertés[1074] qui sert de fondement. Tandis que dans le cadre du chapitre X de la loi relative à l'informatique et aux libertés[1075], ce sont les articles 64 à 66 qui font référence. Malgré cette divergence, le délai d'examen alloué à la CNIL est le même : 2 mois renouvelables une fois. A défaut de décision, c'est un rejet qui est prononcé. La Commission a donc au maximum 2 mois, voire 4 si elle l'estime nécessaire, pour rendre sa décision.

386. Si nous récapitulons les délais les plus courts dans lesquels les demandeurs sont supposés obtenir une réponse, d'après les textes, voici ce qui devrait être précisé : dans le cadre d'un accès sélectif passant par l'IDS, le demandeur doit s'attendre à recevoir le retour de la CNIL après 4 mois dans le meilleur des cas (2 mois requis pour l'avis de l'IDS et 2 mois pour l'examen

[1071] *Supra* n° 302 à 309.

[1072] Loi n° 78-17 du 6 janvier 1978, *op. cit*, dans sa version modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1073] *Supra* n° 367.

[1074] Loi n° 78-17 du 6 janvier 1978, *op. cit*, dans sa version modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1075] *Ibid.*

par la CNIL), et après 10 mois dans le cas le moins favorable *a minima* (6 mois requis pour l'avis de l'IDS et 2 mois renouvelés une fois pour l'examen par la CNIL). Dans le cadre d'un accès sélectif passant par le CCTIRS, le demandeur doit obtenir une réponse de la CNIL après 3 mois dans le cas le plus optimiste (1 mois pour l'avis du CCTIRS et 2 mois laissés à la CNIL), et après 5 mois dans le cas le plus pessimiste (1 mois pour l'avis du CCTIRS et 2 mois d'examen renouvelés une fois par la CNIL). L'amplitude possible, qui demeure une hypothèse basée sur des délais d'examens théoriques, reste très large et impose aux demandeurs d'accès sélectif un aléa qu'il est très difficile de gérer dans la pratique. En réalité cet aléa est bien plus important.

387. D'après le rapport de P.-L. BRAS[1076], les délais imposés aux bénéficiaires de l'accès sélectif aux données de santé sont beaucoup plus étendus que ce qui est prévu par les textes et entravent directement les possibilités de recherches censées être offertes par le mécanisme. En effet, quand certains articles relatifs à la durée d'autorisation d'accès se contentent d'évoquer, de façon trop vague des procédures qui « *restent très longues* »[1077], le rapport remis en septembre 2013 donne une estimation concrète : « *les demandes ponctuelles d'extraction d'un échantillon demandent en moyenne, selon l'IDS, un délai de 17 mois* »[1078]. Sachant que ce délai inclut le temps d'extraction du fichier par la CNAMTS qui serait d'environ 6 mois, cela induit que, dans la pratique, une demande d'accès sélectif n'était autorisée qu'à l'issue d'un délai total de 11 mois, au lieu des 4 mois théoriquement prévus pour un examen ordinaire sans reconduction des délais par l'IDS ou la CNIL.

388. Nous remarquons d'emblée l'écart important entre les délais de traitement des demandes d'accès sélectifs annoncés par les textes, dont le caractère aléatoire a été souligné, et le temps véritablement nécessaire à l'aboutissement de la procédure d'avis par l'IDS ou le CCTIRS et d'examen par la CNIL. Cela indique directement que le processus n'est pas du tout maîtrisé par les différents protagonistes, ce qui est parfaitement reconnu par les principaux intéressés dont « *les services chargés de l'instruction des demandes nombreuses sont trop diversifiés et surchargés* »[1079].

[1076] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.*

[1077] DEBOST C., « Publication du rapport sur la gouvernance et l'utilisation des données de santé, la promesse d'un entrebâillement de l'Open data dans le secteur de la santé ? », *op. cit.*

[1078] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.*, p. 40.

[1079] DEBOST C., « Publication du rapport sur la gouvernance et l'utilisation des données de santé, la promesse d'un entrebâillement de l'Open data dans le secteur de la santé ? », *op. cit.*

389. Nous pouvons également nous intéresser au délai d'extraction finalement autorisée des données par la CNAMTS qui est, en moyenne, de 6 mois. Cela représente une attente supplémentaire pour le bénéficiaire de l'accès sélectif qui pensait probablement être satisfait rapidement de sa demande à l'issue de la procédure d'autorisation par la CNIL. Ce détail supplémentaire montre qu'un travail devait aussi être réalisé sur la réduction du temps nécessaire à la création et à la livraison des fichiers de données, dont l'extraction est autorisée dans le cadre de l'accès sélectif.

390. L'ensemble du dispositif de l'accès sélectif semblait inadapté à une application pratique réelle dès sa conception. Nous l'avons détaillé dans la présente section, le très faible nombre de bénéficiaires à avoir osé déposer une demande d'accès témoigne des maux qui ont affaibli le dispositif pendant ses années d'existence. Sa structure complexe, la difficulté des acteurs gestionnaires des accès à maîtriser les bases de données et le caractère flou et aléatoire des délais de traitement ont eu raison de ce système qui, en dix années, n'est pas parvenu à se développer convenablement. Cet échec est regrettable dans la mesure où l'esprit de l'accès sélectif est parfaitement louable car il implique le développement de recherches et d'études utilisant des données provenant de l'une des plus grandes bases de données de santé au monde. Cependant, les autorités n'ont pas souhaité conférer à ce système les moyens de ses ambitions. La réforme du 26 janvier 2016 s'est donc présentée comme une refonte de l'accès sélectif repensé sous de nouvelles perspectives.

CONCLUSION DU CHAPITRE I

391. Les demandeurs passant par la procédure d'accès sélectif ont, jusqu'à la réforme du 26 janvier 2016[1080], eu beaucoup de difficultés à accéder aux données de santé souhaitées. Pour s'en rendre compte, un simple regard sur le nombre de demandes déposées entre 2007 (année d'entrée en fonction de l'IDS) et 2015 suffit. Au total, seules 161 autorisations d'accès sélectif ont été délivrées ce qui est bien faible lorsque l'on sait que bon nombre d'acteurs publics (non bénéficiaires de l'accès sélectif) ou privés à but non lucratif peuvent avoir un projet de recherche en santé présentant un intérêt public certain. Bien qu'entre 2016 et 2017, avant la mise en place du nouveau système issu de la loi de modernisation de notre système de santé[1081], le nombre de dossiers autorisés ait augmenté, cette montée en charge est trop tardive pour effacer les dysfonctionnements constatés. En effet, la structure même de l'accès sélectif, composée de multiples intervenants aux acronymes peu engageants, associée au manque de pédagogie à l'intention des bénéficiaires potentiels ont impacté négativement la portée du dispositif.

392. Les dysfonctionnements internes de l'accès sélectif sont aussi à l'origine de son développement insuffisant jusqu'à la réforme de 2016. Plusieurs facteurs déterminants entrent en jeu avec, en premier lieu, la complexité des données de santé contenues dans les bases médico-administratives. Cette complexité demande à chaque gestionnaire de données intervenant dans la procédure de maîtriser correctement son sujet. Or, l'expérience montre que le personnel est rarement suffisamment nombreux, formé, ni même organisé pour rendre fluide l'accès aux données. Il en résulte des retards dans les délais de traitements des demandes d'accès sélectif ce qui est de nature à décourager les bénéficiaires potentiels. Ainsi, certaines demandes d'accès sélectif ont pu mettre jusqu'à 17 mois avant que le bénéficiaire n'obtienne véritablement l'accès aux données de santé souhaitées. Cela représente un inconfort indéniable avec lequel étaient contraints de composer les demandeurs. Le respect des délais d'examen des dossiers est donc un élément primordial du nouveau mécanisme d'accès sélectif aux données contenues dans le SNDS.

[1080] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1081] *Ibid*.

CHAPITRE II
L'ACCÈS SÉLECTIF RÉFORME SOUS DE NOUVELLES CONDITIONS

393. Le fonctionnement de l'accès sélectif aux données de santé de l'assurance maladie, qui pourrait être qualifié de chaotique tant pour ses usagers que pour ses administrateurs, ne pouvait rester en l'état. Les rapports et études commandés par les gouvernements successifs ont fait émerger des dysfonctionnements majeurs[1082] auxquels des solutions devaient être proposées. Ainsi, l'accès sélectif a fait l'objet d'un travail important pour trouver un nouveau paradigme (Section 1) et mettre en œuvre un nouveau dispositif devant faire la preuve de son efficience (Section 2).

SECTION 1 : LE NÉCESSAIRE CHANGEMENT DE PARADIGME DE L'ACCÈS SÉLECTIF

394. Le fait de diagnostiquer les errements de l'accès sélectif n'est que la première étape de la réforme de cet accès. Pour aller plus loin, il est nécessaire de proposer des solutions aux diverses problématiques identifiées. C'est pourquoi nous aborderons dans un premier temps les pistes d'évolution envisagées (§1) avant de nous intéresser dans un second temps aux complexités inhérentes au processus qui peuvent difficilement être supprimées (§2).

Paragraphe 1 : Les solutions de simplification de l'accès sélectif

395. Nombreuses sont les recommandations et pistes données pour améliorer l'accès sélectif aux données de santé de l'assurance maladie. Si nous reprenons les différents blocages identifiés dans la précédente section, nous pouvons tenter de dresser leur liste. Ainsi, se retrouvent la complexité des données, le dépassement systématique des délais de traitement des demandes d'accès, la diversification des acteurs, la répartition imprécise des missions entre ces acteurs : c'est, en somme, l'inadaptation du processus à un usage ordinaire et concret qui est caractérisée et unanimement reconnue.

[1082] *Supra* n° 357 à 392.

396. Commençons par les solutions proposées à la complexité des données. Le reproche que nous pouvons retenir à l'encontre de l'accès sélectif, tel qu'il existait avant la réforme[1083] concerne l'inadaptation des données de santé à leur réutilisation. Nous l'avons déjà mis en exergue[1084], la manipulation des données pour répondre aux demandes des bénéficiaires de l'accès sélectif nécessite des compétences précises qui requièrent des formations spécifiques afin d'obtenir suffisamment de personnels qualifiés pour s'y retrouver dans la masse de données disponibles. Pour alléger la tâche des manipulateurs de données et pour fluidifier leur mise à disposition, il a été plusieurs fois préconisé de procéder au traitement, en amont, des données.

La proposition phare que nous retrouvons dès 2013 consiste dans la réalisation d'un travail sur les données pour distinguer les données indirectement anonymes des lots de données véritablement nominatives[1085]. Cette solution permettrait de créer des lots de données ne permettant aucune réidentification, ou « *rend*[a]*nt ce risque très improbable* »[1086]. A l'inverse, les jeux de données présentant un risque avéré de réidentification resteraient soumis à une protection accrue pour les réserver à des traitements préalablement autorisés par les autorités compétentes. Ce raisonnement est également celui qui a été adopté par la Commission open data en santé dans son rapport de 2014[1087] dans lequel elle préconise l'ouverture des données anonymes « *relatives à la santé et au système de santé français* […] *sans préjuger de l'utilisation qui sera faite de ces données* »[1088] en privilégiant la mise en libre accès de « *données granulaires* ». Cependant, la lecture du rapport nous indique que ce projet d'ouverture n'était envisagé par la Commission que pour des bases identifiées, dont celles gérées par l'ATIH (gestionnaire du PMSI qui est intégré dans le SNIIRAM élargi), à l'exclusion du SNIIRAM. En effet, s'agissant du SNIIRAM élargi, la première solution envisagée est de favoriser la production de « *tableaux statistiques répondant par des données agrégées aux questions que se posent les différentes catégories d'utilisateurs* »[1089] en créant des outils spécifiques visant à rendre plus facile la production desdits tableaux. La seconde est la production de jeux de données anonymes. Dans les deux cas, la difficulté réside dans

[1083] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1084] *Supra* n° 372 à 378.

[1085] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 56.

[1086] *Ibid.*

[1087] BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé*, 9 juillet 2014, 122 p.

[1088] *Ibid.*, p. 44.

[1089] *Ibid.*, p. 51.

l'anticipation des demandes et requiert finalement une certaine efficacité dans la création des tableaux, comme des jeux de données.

397. Le remède à la complexité des données comporte donc trois volets qu'il est important de bien distinguer. En premier lieu, il est question de la mise à disposition du public de toutes les données anonymes qui ne présentent aucun risque de réidentification. Ce travail a été lancé par la CNAMTS[1090]par l'intermédiaire de son site AMELI et répond aussi à un impératif porté par les auteurs du rapport relatif aux données ouvertes en santé[1091]. Les auteurs du rapport d'information au Sénat sur les données ouvertes indiquent eux aussi que la création d'une base de données publique, centralisée, ouverte et facile d'utilisation, constitue une opportunité à saisir[1092]. Ils opposent toutefois une limite qui est de nature à freiner cet élan en matière de donnée de santé : ils estiment que le coût trop élevé d'anonymisation et de mise en ligne, ou que le moindre risque de réidentification, pourra justifier l'opposition à une mise à disposition des données de santé en données ouvertes. En deuxième lieu, il est question de la mise à disposition du public des données initialement identifiantes, qui ne devraient donc pas être rendues disponibles, traitées de manière à être proposées sous forme agrégée. Cette agrégation de données doit faire perdre aux données leur caractère réidentifiant. Cette priorité fait aussi partie des attentes de la commission relative à l'*open data* en santé[1093]. En troisième lieu, l'opportunité de fournir des données et des tableaux de bord sur demande est partagée par les auteurs des rapports précités[1094]. Cependant, les modalités de mise en œuvre de cette dernière étape varient d'un projet à l'autre. Dans son rapport, P.-L. BRAS estime ainsi que la fourniture des données sur demande doit demeurer payante car elle découle d'un travail spécifique réalisé exclusivement au profit du demandeur. *A contrario,* P. BURNEL et F. VON LENNEP pensent qu'il est suffisant de proposer des tableaux de bord généralistes qui répondraient à des demandes globales correspondant aux attentes de catégories d'acteurs prédéfinies.

398. Concernant la solution au dépassement des délais d'examen des demandes d'accès, le levier qui semble être privilégié est celui de la mise à disposition d'un maximum de données

[1090] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.,* p. 59.

[1091] BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé, op. cit.,* p. 44.

[1092] GORCE G. et PILLET F., Rapport d'information au Sénat, *op. cit.*, p. 57.

[1093] BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé, op. cit.,* p. 44.

[1094] *Ibid.* p. 51 et BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.,* p. 59.

anonymisées. Effectivement, l'avantage espéré d'un traitement en amont des données de santé pour les publier et les rendre disponibles, dans le respect de la vie privée, est la réduction du nombre de demandes déposées dans le cadre de l'accès sélectif. L'apport de cette mesure serait aussi d'améliorer l'architecture des bases de données en santé afin de les rendre plus aisément compréhensibles par les personnes travaillant au traitement des demandes. L'impact indirect de cette solution serait également le désengorgement des services chargés de traiter les demandes d'accès. Il est vrai que tant du côté du CCTIRS que de celui de la CNIL, les agents n'ont pas eu les capacités de faire face à un nombre de demandes en inflation. C'est ce que notait le rapport de P.-L. BRAS en estimant à 15 le nombre d'experts formés et disponibles alors que le volume de dossiers à traiter n'a cessé d'augmenter entre 2007 et 2012[1095] pour passer de 482 à près de 1 000. S'agissant de la CNIL, seulement 25 postes supplémentaires ont été créés entre 2011 et 2014, les équipes étant passées de 160 agents à 185[1096]. Traiter les données en amont permettrait potentiellement de diminuer le nombre de demandes d'accès déposées : cela aurait pour effet de permettre aux agents de traiter les demandes d'accès sélectif restantes dans des délais qui correspondent aux attentes des demandeurs, *a minima* dans le respect des délais prévus par les textes.

Nous aurions alors une sorte de cercle vertueux enclenché par la réorganisation des données de santé qui, grâce à leur manipulation rendue plus simple, permettrait de les traiter plus aisément, de publier toutes celles qui pourraient l'être sans risquer de compromettre le respect de la vie privée, de faciliter la mission des agents des autorités responsables de leur mise à disposition, et par extension de rendre l'accès sélectif pleinement opérationnel et efficace.

399. Au-delà de la meilleure organisation des données de santé, c'est l'organisation des acteurs qui participent au fonctionnement de l'accès sélectif qui est prônée par les différents auteurs : leur bonne identification et la répartition limpide des compétences entre eux est primordiale. La question de la gouvernance de l'accès sélectif est centrale en ce qu'elle détermine le degré de simplicité de la procédure. Pour cela, deux solutions sont proposées par M. GOLDBERG[1097] : la première est de laisser toute leur autonomie aux organismes gestionnaires de leur propre base de données ; la seconde est de créer un guichet unique destiné à recueillir

[1095] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit,* p. 38.

[1096] Commission nationale de l'informatique et des libertés, *Rapport d'activité 2014*, la Documentation française, 2015, p. 82.

[1097] GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *op. cit.*, p. 40-41.

les demandes d'accès sélectif. La première option est tentante car elle fait reposer sur chacun des acteurs disposant de données de santé la responsabilité de les rendre accessibles : or cela implique que chacun d'eux se dote d'un guichet, d'une équipe qualifiée pour traiter les demandes d'accès et manipuler les données. Cela n'a rien de vraiment simple pour les demandeurs d'accès sélectif qui verraient se multiplier les guichets potentiels auxquels s'adresser pour obtenir des informations. En revanche la seconde option rendrait beaucoup plus simple l'accès des demandeurs aux données de santé mais cela nécessite un travail de réorganisation de la part de l'Etat afin de définir des règles d'accès homogènes. De son côté, P.-L. BRAS approuve la simplification du chemin d'accès sélectif en définissant « *une seule voie d'accès pour en finir avec la complexité et la perplexité qu'entraine aujourd'hui l'existence de plusieurs circuits d'autorisation* »[1098].

400. Cette nouvelle gouvernance de l'accès sélectif aurait plusieurs effets directs. D'abord, les compétences seraient définies et réparties clairement entre les gestionnaires des bases de données faisant l'objet de l'accès sélectif : leur travail respectif s'en trouverait facilité et son efficacité en serait renforcée. Ensuite, la création d'un guichet unique, connu de tous les bénéficiaires de l'accès sélectif, mettrait fin aux incertitudes découlant de l'ancien système. Outre ces pistes qui restent à concrétiser, signalons qu'une solution propre à l'accès ouvert aux données anonymes, dont pourront faire partie les données de santé qui auront été entièrement anonymisées au préalable, a d'ores-et-déjà été mise en place avec la création d'un portail dédié. Il s'agit du site internet gouvernemental *data.gouv.fr* qui est l'illustration même du principe de guichet unique.

401. Les pistes de simplification n'ont donc pas manqué pour procéder à la réforme de l'accès sélectif aux données de santé. Leur faisabilité reste toutefois à confirmer car un écart important peut exister entre les annonces, les propositions formulées en théorie et leur mise en œuvre pratique[1099].

[1098] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit,* p. 63.

[1099] *Infra* n° 410 à 427.

Paragraphe 2 : Les complexités incompressibles de l'accès sélectif

402. L'objectif de la réforme mise en œuvre par la loi de modernisation de notre système de santé[1100] consistait avant tout à démystifier l'accès sélectif en lui retirant son caractère complexe qu'il avait alors, pour lui conférer une portée plus commune et apaisée. Plusieurs leviers étaient disponibles comme nous l'avons étudié précédemment[1101]. Mais tous ne pouvaient être actionnés avec la même intensité étant donné la sensibilité des données traitées et les nécessaires mesures de protection et de sécurité que cela implique[1102]. Le législateur a donc dû s'inspirer des travaux menés par les différents rapporteurs pour débattre et tenter de trouver un système qui accorde plus de place à l'accès aux données de santé, tout en continuant à garantir la protection de la vie privée des individus. Le maintien d'un niveau minimum élevé de protection est bien la clé de la réforme : cela emporte irrémédiablement des concessions en matière de simplification de la procédure d'accès sélectif.

403. La première concession prend forme dans la multiplication des acteurs intervenant au cours de la procédure. Nous aurions pu croire que la dualité entre le CCTIRS et l'IDS dans l'ancien système[1103] serait abandonnée pour ne laisser qu'un seul acteur, tel que l'IDS, pour se charger de l'examen de chaque demande. Un tel raisonnement aurait été bienvenu dans une logique de simplification pratique car souvenons-nous que les demandeurs de l'accès sélectif étaient parfois désorientés[1104] face au manque de clarté du dispositif. Pourtant, cela ne semble pas être la piste recherchée par le législateur. Il ressort de la réforme que le CCTIRS tout comme l'IDS disparaissent pour laisser leur place respective au CEREES[1105] et à l'INDS[1106]. Deux nouveaux acteurs voient donc le jour pour, semble-t-il, marquer le renouveau de l'accès sélectif, c'est ce que constatait en 2016 le président du CCTIRS, J.-L. SERRE[1107]. En sus, le texte de loi fait désormais référence au Comité de protection des personnes (CPP) qui est chargé de donner

[1100] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1101] *Supra* n° 395 à 401.

[1102] *Supra* n° 53 à 62.

[1103] Le CCTIRS était chargé d'examiner les demandes déposées dans le cadre de traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé (ce type de demande pouvait contenir une demande d'accès sélectif aux données du SNIIRAM) ; tandis que l'IDS était la porte d'entrée de l'accès sélectif au SNIIRAM.

[1104] *Supra* n° 365 à 370.

[1105] Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé.

[1106] Institut national des données de santé.

[1107] SERRE J.-L., « Le CCTIRS : passé et présent. L'INDS & le CEREES : futur », ADELF, 09/09/2016.

son avis, préalablement à l'examen du dossier par la CNIL, concernant les recherches impliquant la personne humaine. Bien que l'intervention d'un tel comité soit prévue par l'article L. 1123-6 du code de la santé publique depuis l'ordonnance du 15 juin 2000 relative au code de la santé publique[1108], il n'était jusqu'alors pas mentionné par la loi relative à l'informatique et aux libertés[1109] : il y figure désormais à l'article 76.

404. En guise de simplification, c'est donc une situation d'apparence presque plus complexe qui est proposée par la réforme. Mais nous pouvons adoucir ce constat pour les raisons suivantes : en premier lieu, le rôle de chacun des acteurs est beaucoup mieux défini. Ainsi, l'INDS devient le guichet unique de réception des demandes d'accès aux données du SNDS. Le CEREES, qui remplace le CCTIRS n'intervient plus que dans un cadre spécifique, bien défini par la loi, il en va de même pour le CPP. La CNIL conserve son rôle de décideur final concernant l'autorisation, ou non, de bénéficier de l'accès sélectif. Remarquons toutefois que l'intervention de l'INDS en tant que porte d'entrée de l'accès sélectif n'est pas indiquée lisiblement dans la loi relative à l'informatique et aux libertés[1110]. Cette référence se retrouve dans le code de la santé publique, aux articles L. 1462-1[1111] et L. 1461-3[1112] du même code. Les références juridiques à l'accès aux données de santé sont alors dispersées entre plusieurs sources. Il est regrettable que le législateur n'ait pas pris soin de rappeler dès 2016, même brièvement, le rôle de l'INDS par un rappel au sein de la loi relative à l'informatique et aux libertés. Cette répartition des informations à travers différents textes de loi, si elle est justifiable et parfois nécessaire juridiquement, est de nature à imposer au demandeur d'accès de devenir spécialiste de l'accès sélectif avant même de penser au contenu de sa demande.

[1108] Ordonnance n° 2000-548 du 15 juin 2000 relative à la partie Législative du code de la santé publique, JORF n° 143, 22 juin 2000.

[1109] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[1110] *Ibid.* dans sa version modifiée par la loi n°2016-41 du 26 janvier 2016, *op. cit.*, l'alinéa 8 de l'article 54 ne fait référence qu'au dépôt des dossiers auprès d'un « *secrétariat unique* » sans nommer directement l'INDS. La loi n° 2018-493 du 20 juin 2018, *op. cit.*, puis l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*, ont toutes deux inscrit la mention de l'INDS dans la loi relative à l'informatique et aux libertés comme étant le secrétariat unique de l'accès sélectif aux données de santé des bases médico-administratives.

[1111] Le point 2 de l'article L. 1462-1 du code de la santé publique, dans sa version antérieure à l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*, précise que l'INDS a pour rôle d'assurer « *le secrétariat unique mentionné à l'article 54* [de la loi relative à l'informatique et aux libertés] ».

[1112] Le point II, 2°, a) de l'article L. 1461-3 du code de la santé publique précise que l'accès aux données est subordonné « *Avant le début de la recherche, à la communication, par le demandeur, au groupement d'intérêt public mentionné à l'article L. 1462-1 de l'étude ou de l'évaluation de l'autorisation de la Commission nationale de l'informatique et des libertés, d'une déclaration des intérêts du demandeur en rapport avec l'objet du traitement et du protocole d'analyse, précisant notamment les moyens d'en évaluer la validité et les résultats* ».

405. Eu égard à la diversité des finalités et des modalités de traitement des données de santé qui peuvent exister, il est tout à fait compréhensible que le législateur ait souhaité conserver une multiplicité d'acteurs. Un certain degré de complexité est donc nécessairement rencontré, bien que des mesures aient été prises pour alléger cette impression de procédure pesante et contraignante. A titre d'exemple, un schéma simple de l'accès sélectif est proposé directement sur le site du SNDS. Il permet en quelques instants, à tout un chacun, de prendre connaissance du déroulement de la procédure et de savoir que c'est nécessairement par l'INDS, devenu PDS avec le projet de loi relatif à l'organisation et à la transformation du système de santé que la demande d'accès devra transiter. La pédagogie joue un rôle très important dans le fonctionnement du nouvel accès sélectif : la schématisation des différents types de procédures, mise en ligne et accessible sur le site du SNDS ressemble à ce que l'IDS avait l'habitude de proposer sur son site internet lorsqu'il était en charge de recueillir les demandes d'accès sélectif, pourtant un élément majeur distingue ces deux initiatives. C'est l'élément pédagogique qui améliore grandement la compréhension du système : grâce à une navigation que nous pouvons qualifier de simple et instinctive sur le site du SNDS, la complexité liée à la profusion d'acteurs est atténuée, sans pour autant disparaître. L'existence de plusieurs intervenants dans le cadre de l'accès sélectif est bien un élément de complexité qui semble naturellement attaché au processus : chaque acteur dispose de sa propre mission et l'ensemble est interconnecté par les textes de lois. Nous pouvons toutefois penser que la rédaction des textes issus de la réforme aurait pu être légèrement plus harmonisée en inscrivant toute la procédure de l'accès sélectif soit dans la loi relative à l'informatique et aux libertés[1113], soit dans le code de la santé publique.

406. Hormis les difficultés d'appréhension de l'accès sélectif qui peuvent être induites par l'intervention de plusieurs acteurs distincts, nous pouvons signaler une autre complexité qui, dans le cadre de la réforme, n'a pas pu être supprimée. Il s'agit de la structure des données de santé contenues dans les bases. En effet, nous avons constaté dans le chapitre précédent[1114] que les données traitées et potentiellement accessibles sont naturellement compliquées à comprendre pour plusieurs raisons qui tendent d'abord à la variété des informations qu'elles peuvent contenir, au grand nombre de critères différents grâce auxquels elles peuvent être triées, à la profondeur temporelle des données, mais aussi à la multiplicité des bases dont les données

[1113] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[1114] *Supra* n° 372 à 378.

proviennent. Pour pouvoir traiter de telles données par milliards[1115], l'architecture informatique de la ou des bases utilisées ne peut malheureusement pas être simple. Chaque acteur amené à travailler sur le SNDS dans le cadre de l'accès sélectif devra donc développer une expertise interne. Il est vrai que si le SNDS doit rassembler toutes les données de santé potentiellement accessibles dans le cadre de l'accès sélectif, il ne faut pas oublier que ces données proviennent de plusieurs bases de données différentes qui ont chacune leur référentiel et leur fonctionnement[1116]. Le personnel de la CNAMTS, qui est chargée de la gestion du SNDS, doit donc être en formation continue sur la maîtrise des technologies utilisées afin de répondre dans les meilleurs délais aux demandes formulées dans le cadre de l'accès sélectif.

407. Pour mettre fin à cette complexité des données, l'idée de proposer un traitement unifié sur toutes les données de santé pour les rendre entièrement anonymes pour les intégrer dans un système d'accès libre ne pouvait être la solution. Il a été démontré que, compte tenu de l'état de l'art actuel, l'anonymisation des données ne peut pas être fiable à cent pour cent à moins d'appauvrir les données et d'en réduire l'intérêt d'utilisation ou de réutilisation[1117]. Une base de données de santé entièrement anonymisées serait donc soit une base comportant un trop grand risque de réidentification pour être laissée en accès libre ; soit une base de données tellement altérées que leur traitement ne produirait que peu de résultats. Le choix a donc été fait de maintenir l'accès sélectif, dans sa configuration principale, au cœur d'une mécanique d'accès sur demande au SNDS, celui-ci contenant des données de santé complexes provenant de plusieurs bases et devant faire l'objet d'un retraitement pour être utilisables par le demandeur.

[1115] Reprécisons que le SNIIRAM traitait déjà 1,2 milliard de feuilles de soins, 500 millions d'actes médicaux, 11 millions de séjours hospitaliers au moment où le rapport BRAS était publié en 2013. BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit*.

[1116] Le SNDS contient les données des bases de données relatives aux soins de ville contenues dans le SNIIRAM, les données relatives aux activités des établissements de soins contenues dans l'ATIH, des données concernant les causes de décès stockées dans le CépiDc, et devrait à terme, en 2019, contenir les données sur les maisons départementales de personnes handicapées issues de la Caisse nationale de solidarité pour l'autonomie (CNSA) ainsi que les données relatives à l'activité des complémentaires santé provenant de l'échantillon représentatif des données de remboursement par bénéficiaires transmis directement par les organismes de complémentaire santé. Le projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019 prévoit également l'ajout de nouvelles données dans le SNDS : « *Les données destinées aux professionnels et organismes de santé recueillies à l'occasion des activités mentionnées au I de l'article L. 1111-8 du* [code de la santé publique] *donnant lieu à la prise en charge des frais de santé en matière de maladie ou de maternité mentionnée à l'article L. 160-1 du code de la sécurité sociale et à la prise en charge des prestations mentionnées à l'article L. 431-1 du même code en matière d'accidents du travail et de maladies professionnelles* » et les « *données à caractère personnel des enquêtes dans le domaine de la santé, lorsque ces données sont appariées avec* [les autres données contenues dans le SNDS] ».

[1117] TANGHE H., GIBERT P.-O., « L'enjeu de l'anonymisation à l'heure du Big Data », *Revue française des affaires sociales*, 2017/4, p. 11.

408. En conclusion, le mécanisme de l'accès sélectif n'est pas encore à la portée de n'importe quel individu. Malgré la volonté des autorités de réformer le système pour le simplifier et enlever le maximum de strates superflues, certains éléments semblent encore aujourd'hui nécessaires à son existence. C'est le cas de la multiplicité des intervenants et du caractère complexe des données disponibles. Cela implique, pour les demandeurs, comme pour les intervenants eux-mêmes, d'avoir des équipes spécialisées dans ce domaine particulier. Pourtant, ces particularités n'ont pas été des obstacles à la réforme issue de la loi du 26 janvier 2016[1118]. Adoptant une nouvelle philosophie de l'accès sélectif, cette réforme a été présentée comme une opportunité de démocratiser l'utilisation des données de santé pour en faire un outil citoyen de gouvernance et de surveillance du système de santé[1119]. Ce nouveau concept recèle néanmoins des imprécisions et des imperfections qui doivent être soulevées et décryptées.

SECTION 2 : LA MISE À L'ÉPREUVE CONSTRUCTIVE DE L'ACCÈS SÉLECTIF

409. La mise en œuvre officielle de l'accès sélectif a été retardée de quelques mois pour des raisons opérationnelles. Initialement prévue pour le 1er avril 2017[1120], celle-ci a en fait été repoussée au 28 août 2017[1121]. Depuis lors, le système peut être examiné dans son fonctionnement, ce qui fait naître certaines interrogations légitimes. Premièrement, c'est la question des lacunes encore palpables de l'accès sélectif (§1) qui se pose avec en point de mire l'absence de certaines caractéristiques pourtant essentielles du dispositif. Ensuite, nous nous

[1118] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1119] Intervention de Marisol TOURAINE, alors ministre de la santé, lors des débats à l'Assemblée nationale en première lecture du 10 avril 2015, relatifs à l'article 47 (devenu article 193 dans la version finale du texte) de la loi de modernisation de notre système de santé, *ibid.* : « *Cet article est maintenant bien identifié comme l'« article open data », qui nous fera entrer parmi les pays les plus volontaristes en matière d'ouverture des données de santé. La France est aussi l'un des pays – sinon le pays – qui possèdent les bases de données de santé les plus importantes, en raison de notre système de sécurité sociale. Sur ce sujet, certains ne voient que les risques liés à l'ouverture des données pour la vie privée. Pour notre part, nous voulons trouver un équilibre en indiquant que les données qui sont entièrement anonymes, c'est-à-dire qui ne font peser aucun risque sur la vie privée des personnes, doivent être ouvertes au public gratuitement et sans restrictions quant à leur réutilisation, tandis que celles qui présentent un risque de ré-identification doivent être mises à disposition de certaines personnes, associations, entreprises ou journalistes, mais dans un cadre garantissant la protection de la vie privée* ».

[1120] Décret n° 2016-1871 du 26 décembre 2016 *relatif au traitement de données à caractère personnel dénommé « système national des données de santé »*, JORF n° 0301 du 28/12/2016.

[1121] Comme indiqué sur le site du SNDS, le service de dépôt des demandes d'accès sélectif auprès de l'INDS n'a été ouvert qu'à partir du 28 août 2017.

intéresserons aux multiples inconnues qui demeurent déterminantes pour le bon fonctionnement de l'accès sélectif dans la durée (§2).

Paragraphe 1 : Les lacunes du nouvel l'accès sélectif

410. La proposition d'un nouveau fonctionnement de l'accès sélectif aux données de santé dans la loi du 26 janvier 2016[1122] était pleine de promesse pour tous les demandeurs potentiels. Certains commentateurs craignaient[1123] même que les pistes détectées par le rapport BRAS[1124] ne viennent occulter la problématique de la protection de la vie privée dans le cadre de l'accès sélectif aux données de santé et ne causent une trop grande influence sur le projet de loi réformant le dispositif. Pourtant, bien que la réforme du système soit notamment caractérisée par la création de certains acteurs et la suppression de quelques autres[1125], ainsi que par la redéfinition d'un processus d'accès assoupli[1126], nous pouvons mettre en lumière certaines lacunes qui pourraient aussi être qualifiées d'occasions manquées par les partisans d'une plus grande simplification de l'accès sélectif. Ainsi nous allons tenter de comprendre pourquoi la réforme de l'accès sélectif laisse un sentiment d'inachevé (A), couplé à une incertitude non levée concernant son coût éventuel (B). Puis nous évoquerons l'importance des accès simplifiés dont la mise en place reste lente (C).

A) Le sentiment d'inachevé du nouvel accès sélectif

411. Le premier reproche qui pourrait être fait au nouvel accès sélectif concerne le sentiment d'inachevé que peut faire transparaître la réforme. En effet, nous venons de l'indiquer, l'objectif était d'assouplir la procédure et de proposer un cadre juridique simplifié. Or, comme nos précédentes réflexions l'ont souligné, l'une des parts incompressibles de l'accès sélectif aux données de santé a trait à la complexité du processus[1127] qui, par la nécessité d'assurer un contrôle adéquat sur les données, tout en étant le plus rapide possible, impose l'intervention de

[1122] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1123] DEBOST C., « Publication du rapport sur la gouvernance et l'utilisation des données de santé, la promesse d'un entrebâillement de l'Open data dans le secteur de la santé ? », *op. cit*.

[1124] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.*

[1125] *Supra* n° 403.

[1126] *Supra* n° 330 à 336.

[1127] *Supra* n° 402 à 408.

plusieurs acteurs et le passage de plusieurs étapes. C'est ce que regrette la Cour des comptes dans son rapport de mars 2016[1128] : bien qu'elle souligne l'opportunité saisie par l'article 193 qui fusionne le chapitre X de la loi relative à l'informatique et aux libertés[1129] avec le chapitre IX, et qui crée un guiche unique destiné à recueillir toutes les demandes d'accès sélectif, elle déplore le fait que l'allègement de la procédure ne soit qu'une apparence.

En pratique, « *le circuit d'instruction des demandes reste* […] *d'une réelle complexité compte tenu de la pluralité des instances et de leurs compétences respectives* »[1130]. C'est bien cette complexité de l'accès sélectif, dommageable au développement de son utilisation, que la réforme n'a pas su supprimer entièrement. La Cour des comptes indique que les frontières entre le domaine de compétence des différentes instances restent ténues. Mais une autre problématique, plus profonde, est soulevée par le rapport : c'est celle de la cohérence du dispositif qui dépend grandement de la bonne collaboration entre les équipes de chaque intervenant. En d'autres termes, il pourrait suffire d'un grain de sable dans les rouages du nouvel accès sélectif pour que des « *conflits de légitimité* » naissent et fassent « *perdre en cohérence et en fluidité des procédures que la loi de modernisation de notre système de santé entendait simplifier et alléger* »[1131]. Ce premier élément est donc moins une lacune qu'un risque identifié que la loi réformant l'accès sélectif aurait omis de prendre en compte.

Nous pouvons ajouter que la cohérence du système d'accès sélectif a encore été bouleversée par la réécriture du chapitre IX de la loi relative à l'informatique et aux libertés[1132] dans le cadre du projet de loi relatif à la protection des données personnelles enregistré le 13 décembre 2017 à la Présidence de l'Assemblée nationale. Ce projet de loi adopté le 20 juin 2018[1133] adapte le droit français pour le rendre cohérent avec le Règlement général pour la protection des données[1134] qui est entré en vigueur le 25 mai 2018. Il a servi de base à la réécriture totale de la

[1128] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 101.

[1129] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi 2016-41 du 26 janvier 2016, *op. cit.*

[1130] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 102.

[1131] *Ibid.*

[1132] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[1133] Loi n° 2018-493 du 20 juin 2018, *op. cit.*

[1134] Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

loi relative à l'informatique et aux libertés par l'ordonnance du 12 décembre 2018[1135]. Ces deux textes adoptés en 6 mois apportent une nouvelle touche à l'accès sélectif aux données de santé : pour que le nouveau système monte en puissance et fasse ses preuves, il sera nécessaire de lui donner quelques années de répit, sans modification majeure comme c'est encore le cas avec ce projet de loi.

412. La seconde remarque que nous pouvons formuler à l'égard du nouvel accès sélectif concerne son incomplétude partielle. Ce caractère incomplet relève de deux critères différents : d'une part, il concerne la variété de procédures possibles, d'autre part, il vise les données de santé rendues disponibles dans le cadre de l'accès sélectif au SNDS.

413. Le premier critère concerne le développement de procédures d'accès annexes. C'est l'un des éléments clefs du mécanisme qui est supposé désengorger les services chargés de traiter les dossiers aussi bien du côté de la CNIL que de la CNAM. Il s'agit de la mise en place de procédures d'accès simplifiés, prévues par l'article 54 de la loi relative à l'informatique et aux libertés modifiée par la réforme du 26 janvier 2016[1136]. Les points IV, V et VI de l'article 54 prévoyaient respectivement la création, par la CNIL, de méthodologies de références[1137] dédiées aux « *catégories les plus usuelles de traitements automatisés de données de santé* » ; la mise à disposition de jeux de données agrégées ou d'échantillons de données « *pour des finalités et dans des conditions reconnues conformes à la* [loi relative à l'informatique et aux libertés] » par la CNIL ; et la délivrance par la CNIL d'une décision unique autorisant « *des traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques* ». Dans la nouvelle loi modifiée par ordonnance[1138], ces accès simplifiés sont prévus aux points II et IV de l'article 66 ainsi qu'à l'article 73. Les premières mises à jour des accès simplifiés sont intervenues entre avril et juin 2018 avec la publication des normes de mise à disposition de l'EGB[1139] et de 5 méthodologies

[1135] Ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[1136] Loi n° 78-17 du 6 janvier 1978, *op. cit*, art. 54, modifiée par la loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1137] V. *supra* n° 325 la liste des trois méthodologies de références publiées par la CNIL entre 2006 et 2016.

[1138] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[1139] Délibération n° 2018-134 du 12 avril 2018 *portant homologation de conditions de mise à disposition de l'échantillon généraliste des bénéficiaires (EGB) et des bases de données thématiques appelées « datamarts » du Système National d'Information Inter Régimes de l'Assurance Maladie (SNIIRAM).*

de référence[1140]. Ce délai s'explique par le fait que le chapitre IX de la loi relative à l'informatique et aux libertés[1141] qui incluait les mesures spécifiques aux procédures d'accès simplifiées a fait l'objet, à partir du mois de décembre 2017, d'une réécriture par la relative à la protection des données personnelles[1142] dédié à l'adaptation du droit français au Règlement général pour la protection des données[1143]. La nouvelle rédaction du chapitre IX de la loi relative à l'informatique et aux libertés préservait la notion de référentiels types proposés par la CNIL et crée même celle de « *règlements types* ». L'existence des décisions uniques était également préservée. En revanche, la mise à disposition de jeux de données agrégées ou d'échantillons disparaissait pour revenir entièrement au SNDS dont la gestion est confiée à la CNAMTS[1144]. Cette rédaction demeure aujourd'hui dans la loi relative à l'informatique et aux libertés issue de l'ordonnance du 12 décembre 2018[1145] : son article 66 mentionne au paragraphe II la possibilité pour la CNIL de créer des référentiels et règlements types complétés par des méthodologies de référence prévues par l'article 73, puis le paragraphe IV de l'article 66 porte sur la faculté accordée à la CNIL de prendre des décisions uniques. Signalons que si la CNIL n'a plus la faculté de mettre à disposition des jeux de données agrégées, les référentiels qu'elle rédige peuvent porter sur « *la description et les garanties de procédure permettant la mise à disposition en vue de leur traitement de jeux de données de santé présentant un faible risque d'impact sur la vie privée* ». L'instabilité des dispositions légales relatives aux accès simplifiés permet de comprendre pourquoi cette face alternative de l'accès sélectif n'a obtenu ses premières mises à jour qu'au milieu de l'année 2018.

[1140] Il s'agit de l'adoption par la CNIL des méthodologies de référence MR-001 par la délibération n° 2018-153, MR-003 par la délibération n° 2018-154, MR-004 par la délibération n° 2018-155, toutes trois datées du 3 mai 2018 ; et des méthodologies de référence MR-005 par la délibération n° 2018-256 et MR-007 par la délibération n° 2018-257, datées du 7 juin 2018.

[1141] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1142] Loi n° 2018-493 du 20 juin 2018, *op. cit*.

[1143] Règlement 2016/679, *op. cit.*

[1144] L'article R. 1461-5 du code de la santé publique créé par le décret n° 2016-1871, *op. cit.*, dispose que « *sont constitués à partir du système national des données de santé :*
1° Des jeux de données anonymes mis à disposition du public dans les conditions prévues au premier alinéa de l'article L. 1461-2 ;
2° Des jeux de données agrégées et semi-agrégées adaptés à différents types de recherches, d'études ou d'évaluation. Les données semi-agrégées sont individualisées pour les professionnels ou les établissements de santé et agrégées pour les bénéficiaires des soins ;
3° Des échantillons généralistes représentatifs de l'ensemble des bénéficiaires de l'assurance maladie, comprenant tout ou partie des données relatives aux personnes les constituant. »

[1145] Loi n° 78-17 du 6 janvier 1978, *op. cit*., modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

414. La deuxième justification de l'aspect incomplet de l'accès sélectif concerne l'étendue des données disponibles dans le cadre du SNDS. En effet, l'article 193 de la loi de modernisation de notre système de santé[1146] a notamment créé l'article L. 1461-1 du code de la santé publique. Cet article dresse la liste des données qui constituent le SNDS : nous y retrouvons les données du SNIIRAM (données de soins de ville), celles du PMSI (données de soins hospitaliers), celles de la base de causes médicales de décès (BCMD), mais aussi les données sur les maisons départementales des personnes handicapées provenant de la CNSA, ainsi que des données de remboursement par bénéficiaire transmises par les organismes de complémentaire santé. Pourtant, lors du lancement du SNDS avec l'ouverture de l'accès sélectif à la fin du mois d'août 2017, la réalité était toute autre : seules les données issues des bases SNIIRAM et PMSI étaient disponibles dans la pratique. Ce n'est que dix mois plus tard, en juin 2018, que les données relatives aux causes médicales de décès issues de la BCMD gérée par le CépiDC de l'Inserm ont été intégrées, de façon effective, dans le SNDS. C'est par une simple publication de la DREES sur le site internet du SNDS[1147] que cette mise en ligne de nouvelles données a été annoncée. Cependant, cette première mise à disposition des causes médicales de décès est limitée et ne permet pas aux bénéficiaires de l'accès sélectif de demander à obtenir des données historiquement très profondes. Seules les données relatives aux années 2013, 2014 et 2015 sont proposées à l'heure actuelle. Le communiqué de la DREES ajoute malgré tout que « *les bases seront progressivement enrichies des données de décès* »[1148]. Il est évident que l'attractivité de l'accès sélectif grandira au fur-et-à-mesure que le SNDS s'enrichira de nouvelles données.

415. Outre les causes médicales de décès qui n'ont été intégrées qu'à la moitié de l'année 2018, il est important de souligner que les deux dernières catégories de données de santé ne sont pas encore intégrées dans le SNDS. Sur ce point, les demandeurs de données de santé ne sont pas tout à fait surpris car le site internet du SNDS l'annonce clairement depuis sa mise en ligne : il y est précisé que « *les données* « médico-sociales » *des maisons départementales des personnes handicapées* » et « *un échantillon représentatif des données de remboursement par bénéficiaires transmis par les mutuelles* » ne seront intégrés que lorsque les trois premières

[1146] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1147] C'est par une simple communication sur le site internet du SNDS que la DREES (direction de la recherche, des études, de l'évaluation et des statistiques) a annoncé, le 3 septembre 2018 que les causes médicales de décès des années 2013, 2014 et 2015 étaient disponibles dans le SNDS depuis le mois de juin 2018. DREES, « Intégration des causes de décès dans le SNDS », *site internet du SNDS*, https://www.snds.gouv.fr/SNDS/Actualites/Actu-12, 03/09/2018.

[1148] *Ibid.*

bases « *seront constituées* »[1149]. Notons que certaines données des maisons départementales des personnes handicapées sont d'ores et déjà disponibles en libre accès mais il s'agit de données qui n'ont aucun caractère médical[1150]. Ce sont donc deux ensembles importants de données qui restent à intégrer au SNDS. En complément, le récent projet de loi relatif à l'organisation et à la transformation du système de santé[1151] prévoit l'ajout supplémentaires de données dans le SNDS : cette base devrait donc encore grandir très rapidement. Nous pouvons parfaitement comprendre que le système issu de la réforme du 26 janvier 2016[1152] ait été mis en place avec les données disponibles dans l'optique de l'enrichir avec de nouvelles informations. Le contraire aurait d'ailleurs été relativement frustrant pour tous les acteurs : nous n'aurions pas imaginé devoir attendre plusieurs années que toutes les données censées être proposées dans le SNDS y soient définitivement et correctement implémentées pour que celui-ci soit ouvert.

Sur le point particulier des données disponibles, l'élément qui renforce le sentiment d'inachevé est l'absence de calendrier précis. En effet, ni le site du SNDS, ni celui de l'INDS, ni même celui de la DREES ne proposent de date aux acteurs qui attendent potentiellement la mise en ligne des données de santé manquantes. Ce manque de visibilité témoigne de l'incertitude dans laquelle les responsables du SNDS sont eux-mêmes plongés. L'un des seuls indices a été donné lors du colloque tenu au Conseil d'Etat le 1er décembre 2017[1153]. M. GIRARD, alors cheffe de la mission accès aux données de santé à la DREES, y affirmait que les données médico-sociales provenant des maisons départementales des personnes handicapées et celles provenant des organismes de complémentaire santé ne feraient pas l'objet d'une intégration avant le courant

[1149] Voir la page « *Composantes du SNDS* » à l'adresse https://www.snds.gouv.fr/SNDS/Composantes-du-SNDS.

[1150] Le jeu de données « *Maisons départementales de personnes handicapées (MDPH)* » disponible sur la plateforme de données ouvertes de l'Etat propose de retrouver les informations suivantes : nom ; adresse postale ; code postal ; commune ; département ; région ; coordonnées géographiques pour la géolocalisation (longitude et latitude). Retrouvez-le à l'adresse https://www.data.gouv.fr/fr/datasets/maisons-departementales-de-personnes-handicapees-mdph-1/.

[1151] Le projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019 prévoit également l'ajout de nouvelles données dans le SNDS : « *Les données destinées aux professionnels et organismes de santé recueillies à l'occasion des activités mentionnées au I de l'article L. 1111-8 du* [code de la santé publique] *donnant lieu à la prise en charge des frais de santé en matière de maladie ou de maternité mentionnée à l'article L. 160-1 du code de la sécurité sociale et à la prise en charge des prestations mentionnées à l'article L. 431-1 du même code en matière d'accidents du travail et de maladies professionnelles* » et les « *données à caractère personnel des enquêtes dans le domaine de la santé, lorsque ces données sont appariées avec* [les autres données contenues dans le SNDS] ».

[1152] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1153] SAUVE J.-M., TABUTEAU D., DECOU-PAOLINI R., VASILIU I., MIGNARD J.-P., BRAS P.-L., GIRARD M., POLTON D., DAUTIEU T., STASSE F., METTENDORFF M., MADDALONE P., SAOUT C., FOMBEUR P., LAUDE A., MARTINEL A., LUCAS J., COMBREXELLE J.-D., « Santé et protection des données », *op. cit.*

de l'année 2019. En lieu et place d'une date plus précise, c'est une période de douze mois qui nous est proposée à l'occasion du colloque organisé par le Conseil d'Etat[1154]. Il est regrettable que cette simple information relative à l'intégration des données manquantes au SNDS à l'horizon 2019 ne soit pas partagée plus ouvertement avec l'ensemble des acteurs concernés. Nous pouvons penser que cette difficulté à communiquer sur un calendrier d'intégration des dernières données dans le SNDS est de nature à renforcer le sentiment d'inachevé, mêlé à un manque de maîtrise, qui émane de l'accès sélectif.

L'incomplétude de l'accès sélectif paraît finalement assumée par les acteurs de la réforme : ces derniers comptaient peut-être sur la finalisation et l'entrée en vigueur des dernières briques juridiques (nous pensons notamment au Règlement général pour la protection des données[1155] entré en vigueur le 25 mai 2018, à la loi relative à la protection des données personnelles adopté le 20 juin 2018, à l'ordonnance du 12 décembre 2018) avant d'user de leurs prérogatives pour parachever la construction du SNDS. Ce retard pris dans la mise en œuvre du système et les vides juridiques qui restent à combler ne doivent pas pour autant occulter le fait que sa pérennité dépend d'autres paramètres qui demeurent incertains.

B) L'incertitude constante du coût du nouvel l'accès sélectif

416. La deuxième critique qui peut être faite à l'encontre du nouvel accès sélectif concerne l'inconnue de son coût pour le bénéficiaire : incertitude toujours existante à l'heure de l'écriture de ces lignes en 2019, plus d'un an et demi après la mise en service du SNDS. L'article L. 1461-5 du code de la santé publique créé par l'article 193 de la loi de modernisation de notre système de santé[1156] précise en effet que l'accès aux données de santé qui n'ont pas fait l'objet d'une mise à disposition du public – ladite mise à disposition étant subordonnée au fait que ces données doivent être assurément non identifiantes et non réidentifiantes – doit être gratuit pour les recherches, études ou évaluations demandées par l'autorité publique, ou pour les recherches menées exclusivement pour les besoins de services publics administratifs. *A contrario*, cela signifie que l'accès sélectif aux données de santé, sans avoir nécessairement vocation à être

[1154] Cette période de 12 mois a été confirmée par Mylène GIRARD, cheffe de la mission accès aux données de santé à la DREES lors du colloque « Santé et protection des données », *op. cit.*

[1155] Règlement 2016/679, *op. cit.*

[1156] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

payant, pourrait le devenir pour tous les bénéficiaires qui ne rentrent pas dans l'une des deux catégories prévues par le code de la santé publique si le besoin s'en fait sentir : le législateur s'est intelligemment ménagé une telle possibilité en rédigeant l'article L. 1461-5 du code de la santé publique. Ainsi, à l'avenir, si un acteur privé souhaite réaliser, pour son compte et à son initiative, une recherche dans le domaine de la santé nécessitant un accès sélectif au SNDS, un coût pourra lui être opposé.

417. La Cour des comptes valide cette logique de construction d'un modèle permettant de financer le SNDS à hauteur de ses ambitions et des usages[1157] : elle justifie cela en mettant d'abord en avant les coûts nécessairement élevés engendrés par le chantier de la mise aux normes de sécurité des gestionnaires du SNDS, mais aussi par le maintien d'un niveau suffisant de sécurité par la mise en place d'audits. Ainsi, dans son rapport[1158], la Cour des comptes fait référence au mécanisme déjà existant du centre d'accès sécurisé aux données à distance (CASD) qui a été créé pour accéder aux données détaillées de l'INSEE. Dans ce cadre, chaque utilisateur qui souhaite accéder à des données mises à disposition de manière sécurisée par l'INSEE prend en charge une partie des coûts induits par la mise aux normes de sécurité des bases de données, en fonction de ses besoins. Ce modèle est avantageux pour la Cour des comptes en ce qu'il permet « *la mutualisation des coûts des infrastructures et des logiciels, seule solution viable financièrement. Car les institutions ne peuvent pas supporter individuellement le coût de la sécurité, qui est en grande partie un coût fixe, peu dépendant de la taille de la plateforme* »[1159]. Cette référence favorable au CASD a été, plus tard, reprise par la Commission des affaires sociales à l'Assemblée nationale dans son rapport relatif aux données du SNIIRAM disponibles dans le SNDS[1160] : « *le rapporteur est convaincu que les réflexions et travaux préliminaires sont suffisamment avancés et que le modèle du CASD est suffisamment éclairant pour que des décisions soient prises dans un délai rapproché, qui permettront sinon de garantir la viabilité économique intrinsèque du SNDS, du moins de couvrir dans des proportions raisonnables une partie de ses coûts, selon des modalités*

[1157] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 113.

[1158] *Ibid.*, p. 110.

[1159] *Ibid.*

[1160] Rapport d'information déposé par la Commission des affaires sociales à l'Assemblée nationale 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, 21 février 2017, p. 123 à 130.

respectueuses à la fois des besoins des gestionnaires et des attentes des utilisateurs »[1161]. Si nous revenons à la mise en œuvre du SNDS, nous ne pouvons que constater l'absence totale de communication des différents acteurs qui ont travaillé à son ouverture (CNAMTS, DREES et INDS en tête) au sujet d'une potentielle mise à contribution – destinée à mutualiser le coût de l'actualisation des normes de sécurité de toutes les bases qui le composent – des bénéficiaires de l'accès aux données.

418. La Cour des comptes s'appuie ensuite sur les coûts de maintenance, de développement et d'enrichissement du SNDS qui justifieraient que l'accès aux données de santé fasse l'objet d'une redevance spécifique. Si un tel dispositif devait exister, il devrait seulement avoir pour objet, d'après le rapport, de couvrir les coûts dans le respect du « *principe général de non enrichissement des administrations et des établissements publics* »[1162]. Pour étayer son raisonnement elle met en avant les exemples internationaux qui proposent régulièrement un accès gratuit de base couplé à divers autres accès payants tels qu'une base de données plus spécifiques dont l'accès fait l'objet d'une redevance forfaitaire, ou des services supplémentaires payants. En Angleterre, aux Etats-Unis, au Québec (Canada) ou encore en Allemagne.

La base de données *Clinical Practice Research Datalink* (CPRD) située en Angleterre permettait, en 2015, un accès annuel complet à sa base pour 250 000 livres (soit 339 300 euros en tenant compte du taux de change du mois de décembre 2015[1163]). Une précision primordiale est apportée par le rapport : la base anglaise CPRD est alimentée par des médecins volontaires qui sont rémunérés pour leur temps passé à transmettre les données : ils gagnaient, en 2015, environ 800 livres par an pour cela (soit environ 1 000 euros). L'objectif de cette base est de trouver l'équilibre financier entre les coûts de gestion et les produits de la vente des données : une véritable logique comptable et financière est mise en œuvre pour assurer la pérennité de l'ensemble du dispositif.

Aux Etats-Unis, la solution retenue par la sécurité sociale fédérale (*Centers for Medicare & Medicaid Services*, ou CMS) consiste à mettre à disposition des utilisateurs de nombreux jeux de données différents. Les premiers jeux de données, les plus simples, sont accessibles

[1161] *Ibid.*, p. 130.

[1162] *Ibid.*, p. 112.

[1163] Toutes les conversions de devises en euros proposées dans cette sous-partie ont pour référence le taux de change en vigueur au 31/12/2015 alors que le rapport de la Cour des comptes était en cours de finalisation.

gratuitement par tous. Le deuxième type de jeux de données, qui recèlent des informations plus complexes, est accessible par tous mais fait l'objet d'un paiement. Le troisième type de jeux de données est, lui, beaucoup plus détaillé et n'est accessibles qu'aux chercheurs : aucune utilisation commerciale directe ne peut en être faite. La Cour des comptes indique que les redevances dues sur les jeux de données standardisées sont extrêmement variables en fonction de la profondeur historique souhaitée et du volume final du fichier. A titre d'exemple, une année entière de données peut ne coûter que 300 dollars (soit 275,55 euros) si les informations demandées sont simples, tandis que cela peut atteindre 100 000 dollars (soit 91 850 euros).

Au Québec, une redevance allant de 500 à 5 500 dollars (soit de 330,80 à 3 638,80 euros) est due, en fonction des données demandées : la moitié sert à financer le personnel chargé de la mise en œuvre de la base de données de santé, l'autre moitié sert à financer les frais informatiques. En Allemagne, c'est un système d'accès premium à des données beaucoup plus vastes qui existe : les clients payent un abonnement spécifique pour avoir le droit d'accéder à davantage de données.

Les différentes solutions préexistantes au niveau international sont intéressantes à connaître car elles déclinent une multitude de possibilités de facturation pour un même objectif : financer le regroupement, la sécurisation et la fourniture de données de santé. Toute la difficulté soulevée par les auteurs du rapport réside dans la bonne tarification du service qui ne doit pas conduire à l'enrichissement des acteurs publics chargés de la gestion des bases de données et de leur mise à disposition. Il n'est malheureusement pas envisageable de transposer, tel quel, l'un ou l'autre de ces schémas : chaque système de santé possède une structure de bases de données différente et un mode de gestion qui lui est propre. L'enjeu véritable réside dans la difficulté à s'inspirer des de tout ou partie des exemples cités en les adaptant aux particularités du SNDS français.

419. Nous ne pouvons clore ce développement sans mettre en exergue l'utilisation, loin d'être innocente, du terme « *appétence* »[1164] par les rédacteurs du rapport pour caractériser la volonté des acteurs privés à obtenir des données de santé. En effet, le document souligne le fait que « *le secteur privé* [est] *disposé à payer des montants élevés pour accéder aux données* », comme si cette potentialité devait être nécessairement exploitée par l'Assurance maladie pour tarifer, le plus cher possible, les redevances relatives à l'accès au SNDS. Cependant, ce type de

[1164] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 113.

raisonnement, s'il doit trouver application en pratique, présente deux risques : le premier concerne l'exclusion des petits acteurs privés qui n'auraient, par leur taille, pas les moyens d'accéder aux jeux de données qui les intéressent, sans tenir compte de l'intérêt public que la recherche qu'ils souhaitent mener pourrait avoir. En d'autres termes, fixer des coûts élevés pour obtenir les données les plus intéressantes reviendrait à réserver la recherche sur les données du SNDS aux acteurs privés les plus importants et à se couper, le cas échéant, de recherches au potentiel prometteur menées par des acteurs privés plus petits qui n'auraient pas les moyens d'acheter les jeux de données requis. Le second risque renvoie au principe rappelé par la Cour des comptes de non enrichissement des administrations : si l'objectif est de proposer le coût d'accès aux données le plus élevé possible et que, malgré ces tarifs, les ventes de données rencontrent un succès important, il n'est pas impossible que le produit de ces ventes aille au-delà de la simple couverture des coûts entrainés par la gestion des bases de données et par la fourniture desdites données. Nous le comprenons, la question de la tarification de la mise à disposition des données de santé du SNDS est très complexe.

C'est probablement en raison de cette complexité que, à la fin de l'année 2018, plus de 14 mois après la mise en fonctionnement de l'accès sélectif, aucun nouveau point d'étape n'a été réalisé concernant la réflexion autour du coût que devront supporter les demandeurs qui sollicitent un accès de leur propre chef. La DREES, la CNIL, ou encore l'INDS restent officiellement silencieux alors que la responsable de la mission accès aux données de santé de la DREES annonçait en décembre 2017 : « *nous avons avancé sur la question du modèle économique et nous travaillons à une tarification qui devrait être affichée en début d'année* »[1165]. Si une décision a été prise depuis lors, elle n'a pas, à notre connaissance, été affichée. De plus, nous ne savons pas si les accès autorisés au SNDS dans le cadre de l'accès sélectif depuis la fin du mois d'août 2017[1166] ont donné lieu à une quelconque facturation. Cette inconnue relative au tarif est source d'incertitudes chez les demandeurs de l'accès sélectif qui n'ont aucun moyen de savoir si, à l'avenir, ils devront s'acquitter d'une quelconque somme d'argent. Le fait que

[1165] SAUVE J.-M., TABUTEAU D., DECOU-PAOLINI R., VASILIU I., MIGNARD J.-P., BRAS P.-L., GIRARD M., POLTON D., DAUTIEU T., STASSE F., METTENDORFF M., MADDALONE P., SAOUT C., FOMBEUR P., LAUDE A., MARTINEL A., LUCAS J., COMBREXELLE J.-D., « Santé et protection des données », *Les entretiens du Conseil d'Etat en droit social*, colloque organisé le 01/12/2017 à Paris, actes non publiés.

[1166] La liste des dossiers de demande d'accès au SNDS étudiés par l'INDS est mise à jour deux fois par mois sur le site de l'Institut à l'adresse suivante : https://www.indsante.fr/fr/acceder-au-tableau-de-suivi-des-dossiers-deposes.

l'hypothèse d'une tarification n'ait pas été officiellement écartée ou embrassée montre à quel point le sujet est sensible.

La question de la tarification est donc un élément crucial de l'accès sélectif pour tous les demandeurs qui ne bénéficient pas, d'après le code de la santé publique, de la gratuité. Le fait que ce sujet soit totalement absent des décrets et arrêtés pris depuis la loi du 26 janvier 2016[1167], sans être un véritable frein à l'utilisation sereine de l'accès sélectif, symbolise le sentiment d'inaboutissement d'un système réformé depuis plus de trois ans.

C) La mise en place ralentie des accès simplifiés

420. Le troisième élément qui est de nature à nous faire douter quant à la complétude de l'accès sélectif concerne les accès simplifiés dont la promesse offerte aux demandeurs d'accès depuis la réforme du 26 janvier 2016[1168] est encore en suspens. En effet, ladite réforme a modifié l'article 54 de la loi relative à l'informatique et aux libertés[1169] : aux termes de cet article, dans sa rédaction issue de la réforme de 2016, les acteurs devaient pouvoir obtenir un accès simplifié au SNDS de trois façons différentes. Soit par le biais d'une déclaration de conformité déposée à l'INDS aux méthodologies de référence élaborées et homologuées par la CNIL. Soit en bénéficiant d'une décision unique de la CNIL autorisant à réaliser plusieurs traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques. Soit en demandant l'accès à des jeux de données agrégées dont la mise à disposition est reconnue conforme à la loi par la CNIL. Les candidats à l'accès aux données de santé avaient donc trois alternatives à la procédure classique d'autorisation préalable permettant d'obtenir des données contenues dans le SNDS.

421. Or, l'année 2018 a donné lieu à l'adoption de la loi du 20 juin 2018 réformant la loi relative à l'informatique et aux libertés[1170] visant à l'adapter au Règlement général relatif à la protection des données[1171] et de l'ordonnance du 12 décembre 2018[1172] qui a entièrement réorganisé les

[1167] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1168] *Ibid.*

[1169] *Supra* n° 413.

[1170] Loi n° 2018-493 du 20 juin 2018, *op. cit.*

[1171] Règlement 2016/679, *op. cit.*

[1172] Ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

dispositions légales. Depuis l'entrée en vigueur de cette réforme, le seul moyen, pour un responsable de traitement de données de santé à caractère personnel dans le domaine de la santé, d'obtenir des données du SNDS dans le cadre de la recherche en santé est de se conformer aux méthodologies de référence mentionnées à l'article 73 de la loi relative à l'informatique et aux libertés[1173]. En effet, ledit article dispose que seuls les traitements conformes à une méthodologie de référence peuvent être mis en œuvre sans obtenir d'autorisation préalable de la CNIL : la simple déclaration de conformité devrait suffire, y compris pour obtenir les données du SNDS qui sont nécessaires à la mise en œuvre du traitement. Cela signifie-t-il pour autant que les autres types d'accès simplifié n'existent plus ? La réponse à cette question est mitigée et doit être donnée en deux temps.

422. D'abord, le mécanisme de décision unique délivrée par la CNIL est toujours d'actualité. Il peut encore être trouvé au point IV de l'article 66 de la loi relative à l'informatique et aux libertés[1174] : sa rédaction n'a quasiment pas évolué si ce n'est que le législateur a remplacé le mot « *commission* » par « *Commission nationale de l'informatique et des libertés* ». Mais l'opportunité de bénéficier d'une décision unique est-elle ouverte aux responsables de traitement qui souhaitent faire de la recherche dans le domaine de la santé en utilisant des données issues du SNDS ? La question mérite d'être posée car l'incertitude demeure. En effet, à première vue, les dispositions prévues par les articles 65 à 71 de la loi relative à l'informatique et aux libertés et qui composent la sous-section 1 de la section 3 du chapitre III de son titre II sont supposées s'appliquer à l'ensemble des traitements de données à caractère personnel dans le domaine de la santé, cela devrait donc inclure les traitements effectués dans le cadre de la recherche en santé[1175].

Pourtant, le législateur a inséré, dans la sous-section 2 suivante de la loi, des dispositions précisant que le seul moyen, pour un traitement ayant pour finalité de faire de la recherche en santé, d'être mis en œuvre sans autorisation préalable de la CNIL est de faire l'objet d'une déclaration de conformité à une méthodologie de référence homologuée[1176]. Cela suppose, à

[1173] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[1174] *Ibid.*

[1175] Rappelons que l'accès aux données du SNDS n'est possible qu'à des fins de recherche, d'étude ou d'évaluation présentant un caractère d'intérêt public aux termes de l'article L. 1460-1 du code de la santé publique.

[1176] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, art. 73, modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

l'inverse, que les procédures simplifiées qui ne sont pas présentes dans le corps de la sous-section 2 susmentionnée ne peuvent pas bénéficier aux traitements ayant pour finalité la recherche en santé et, par extension, aux traitements qui nécessitent un accès aux données du SNDS. Ce raisonnement paraît conforté par le fait que le législateur ait pris la peine de rédiger des dispositions qui se ressemblent fortement, entre les articles 66 (dans la sous-section 1 de la section 3 du chapitre III du titre II) et 73 (dans la sous-section 2 de la section 3 du chapitre III du titre II) de la loi. En revanche, si le législateur entend tout de même faire bénéficier aux traitements ayant pour finalité la recherche en santé et nécessitant potentiellement un accès au SNDS des autres procédures simplifiées que les méthodologies de référence, alors le texte de la loi est fort loin d'être suffisamment clair et intelligible.

423. Ensuite, la faculté de mise à disposition de jeux de données agrégées ou d'échantillons en provenance du SNDS a disparu de la loi relative à l'informatique et aux libertés. Initialement prévue par le point V de son article 54[1177], cette faculté permettait la création d'échantillons et agrégats homologués dont l'accès était soumis au respect de conditions particulières et à des finalités définies au préalable. Dans ce cadre, tout demandeur d'accès désirant utiliser les données dans le cadre de la recherche en santé pouvait obtenir les données souhaitées s'il répondait aux critères prédéfinis par le ou les jeux de données convoités. Mais cette opportunité s'est a été camouflée à l'occasion de la réforme destinée à adapter le droit français au droit européen : désormais, la mise à disposition de jeux de données est subordonnée à la création de référentiels et règlements types[1178], elle est donc moins facile à détecter dans le texte de loi. Il n'est pas certain que le législateur ait sciemment rendu moins lisible cet accès simplifié pourtant potentiellement très utile si les bons jeux de données viennent à être créés. Effectivement, le code de la santé publique continue à faire référence, à son article L. 1462-1, à « *la mise à disposition d'échantillons ou de jeux de données agrégées mentionn*[és] *au V dudit article 54, dans des conditions préalablement homologuées par la Commission nationale de l'informatique et des libertés* »[1179]. Cet article dresse une liste non exhaustive des missions de l'INDS qui fait référence à une rédaction de l'article 54 de la loi relative à l'informatique et aux

[1177] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, art. 54, V, modifié par la loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1178] V. loi n° 78-17 du 6 janvier 1978, *op. cit.*, art. 54 al. 4, modifié par la loi n° 2018-493 du 20 juin 2018, *op. cit.*, et loi n° 78-17 du 6 janvier 1978, *op. cit.*, art. 66 al. 4, modifié par l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit*.

[1179] Article L. 1462-1, 4° du code de la santé publique.

libertés antérieure à la réforme du 20 juin 2018[1180] et de l'ordonnance du 12 décembre 2018[1181]. Il s'agit donc d'un nouveau motif de confusion dans l'appréhension de l'accès sélectif car les mesures insérées dans le code de la santé publique.

424. L'article L. 1462-1 du code de la santé publique a finalement fait l'objet d'une harmonisation en lien avec la nouvelle rédaction de la loi relative à l'informatique et aux libertés grâce à l'ordonnance du 12 décembre 2018[1182]. Cette harmonisation pouvait être pressentie du fait de la publication, par la CNIL, de la délibération homologuant la procédure d'accès simplifié à l'échantillon généraliste des bénéficiaires (EGB)[1183]. Les responsables de traitement qui souhaitent utiliser de telles données peuvent, s'ils respectent les critères fixés par la délibération, déposer un dossier auprès de l'INDS qui a 15 jours pour se prononcer. Si cette délibération est antérieure au vote de la réforme du 20 juin 2018 qui a camouflé les mentions relatives à la mise à disposition de jeux de données en accès simplifié, il n'en demeure pas moins qu'elle est bel et bien applicable car le site internet de l'INDS[1184] communique ouvertement autour de l'accès simplifié à l'EGB. La création de jeux de données issues du SNDS continue donc à faire partie des accès simplifiés, mais elle est désormais subordonnée à la création de référentiels et règlements types. Cela accompagne les méthodologies de référence, dont peuvent bénéficier les demandeurs d'accès au SNDS dans le cadre de la mise en œuvre d'un traitement ayant pour finalité la recherche dans le domaine de la santé.

425. Il ressort des précédents développements que l'articulation du code de la santé publique avec la loi relative à l'informatique et aux libertés devrait faire l'objet d'une harmonisation complète car les dispositions concernant les accès simplifiés au SNDS restent extrêmement floues. Un point supplémentaire attire notre attention et vise la mise en œuvre pratique des mécanismes d'accès simplifié. Ceux-ci permettent à un traitement de données à caractère personnel ayant pour finalité la recherche en santé d'être réalisé sans obtenir l'autorisation de la CNIL : une simple déclaration de conformité, un examen par l'INDS et, le cas échéant, par

[1180] Loi n° 2018-493 du 20 juin 2018, *op. cit*.

[1181] Ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[1182] *Ibid.*

[1183] Délibération n° 2018-134 du 12 avril 2018 portant homologation de conditions de mise à disposition de l'échantillon généraliste des bénéficiaires (EGB) et des bases de données thématiques appelées « datamarts » du Système National d'Information Inter Régimes de l'Assurance Maladie (SNIIRAM).

[1184] V. le site en suivant le lien suivant : https://www.indsante.fr/fr/actualite/nouveau-procedure-dacces-simplifie-legb

le CEREES suffisent dans le cadre de la méthodologie de référence, tandis que pour l'accès à des jeux de données comme l'EGB, un dossier à déposer à l'INDS suffit pour obtenir une autorisation dans les 15 jours sans intervention de la CNIL. Ces deux types d'accès simplifiés doivent sans nul doute permettre de décharger la Commission d'une somme de travail considérable. En revanche, pour les candidats à l'accès sélectif aux données de santé du SNDS, cela ne change que très peu de choses : les critères de sécurité des données à caractère personnel et de respect de la vie privé restent primordiaux, le dépôt de dossiers auprès de l'INDS est toujours requis ; même en cas de déclaration de conformité à une méthodologie de référence, le responsable du traitement est toujours soumis à un délai d'attente car il ne peut commencer la mise en œuvre du traitement qu'une fois qu'il obtient l'accès aux données du SNDS requises.

426. D'après nos précédentes réflexions, seuls deux accès simplifiés sont véritablement opérationnels dans le cadre de l'accès sélectif au SNDS à la fin de l'année 2018 : la conformité aux méthodologies de référence d'une part et la demande de transmission de jeux de données tels que l'EGB d'autre part. S'agissant des méthodologies de référence, une seule d'entre elles est véritablement exploitable par les acteurs publics et privés à but non lucratif afin d'obtenir des données de santé qui composent le SNDS : il s'agit de la méthodologie de référence appelée MR-005 qui a été créée environ 9 mois après l'ouverture des accès sélectifs par délibération de la CNIL en date du 7 juin 2018[1185].

Le seul bénéfice que les accès simplifiés devraient avoir sur l'accès sélectif aux données du SNDS, et qu'il est important de ne pas minimiser, est lié à la réduction globale des délais d'accès étant donné que la CNIL n'a pas à intervenir dans la procédure d'accès. A la fin du mois de novembre 2018, seulement 6 traitements nécessitant un accès à la base PMSI, faisant partie du SNDS, étaient enregistrés par l'INDS dans le répertoire public des études enregistrées sous MR (méthodologie de référence). Ce répertoire n'a commencé à être mis à jour que depuis le mois de juillet 2018 et devrait être de plus en plus fourni au fil du temps. Les acteurs intéressés par l'accès aux données de santé contenues dans le SNDS ont besoin d'un cadre bien défini et clair pour appréhender correctement les opportunités qui leur sont offertes. Un travail conséquent de

[1185] Délibération n° 2018-256 du 7 juin 2018 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).

réorganisation des textes et de pédagogie sur le terrain doivent donc encore être menés pour que le droit relatif à l'accès aux données de santé du SNDS puisse pleinement s'exercer.

427. Il ressort des développements précédents que les autorités françaises n'ont pas attendu que l'accès sélectif soit intégralement opérationnel, dans toutes ses formes, pour le mettre en œuvre. Cette façon d'opérer est, certes, imparfaite et donne l'impression que la réforme n'est pas aboutie – de nombreuses questions liées à des aspects de l'accès sélectif continuent en effet à se poser plus d'un an après son entrée en vigueur – mais elle a le mérite de permettre, à tous les bénéficiaires, de déposer leurs premiers dossiers de demande d'accès aux données de santé du SNDS et de faire émerger les premières pistes d'adaptation et d'amélioration envisageables du dispositif. Sans parler de version d'essai « grandeur nature » de l'accès sélectif, nous pouvons penser que les premiers mois d'existence de l'accès sélectif ont permis d'éprouver les mécaniques prévues par le législateur. L'inconvénient de ce procédé réside dans l'incertitude liée aux capacités d'évolution et d'adaptation des différents acteurs de l'accès sélectif à l'ensemble des mesures dictées par la réforme.

Paragraphe 2 : L'avenir de l'accès sélectif pavé d'incertitudes

428. La nouvelle version de l'accès sélectif est pleine de promesses si nous nous en tenons aux textes qui la définissent. La procédure a vu son encadrement entièrement remanié pour répondre à des critères stricts mais connus de tous[1186] afin de fluidifier la constitution des dossiers de demande d'accès et leur examen par les intervenants successifs. En vérité, le bon fonctionnement du dispositif repose sur des conditions qui devront être vérifiées dans la pratique, mais surtout dans la durée car elles sont confrontées à des incertitudes importantes (A) telles que le respect des délais d'examen des demandes ainsi qu'ils sont prévus par la loi, la viabilité du copilotage du SNDS par la CNAMTS et par l'INDS, mais aussi la capacité de l'INDS et de la CNIL à pleinement mettre en œuvre leur mission de contrôle *a posteriori* des traitements effectués. Par ailleurs, nous ne pouvons omettre de faire part des doutes qui ont été officiellement émis concernant la sécurité des données de santé à caractère personnel contenues dans le SNIIRAM, qui font partie intégrante du SNDS (B).

[1186] *Supra* n° 330 à 336.

A) Les incertitudes durables de l'accès sélectif

429. La première incertitude que nous pouvons soulever sans difficulté concerne la capacité des acteurs à respecter le *tempo* imposé par les textes de loi. Nous l'avons étudié dans le chapitre précédent[1187], la réforme du 26 janvier 2016 a fixé des délais d'examen des dossiers et de délivrance des avis. Ainsi, l'INDS a 7 jours ouvrés pour transmettre tout dossier complet au CEREES. Ce dernier dispose alors d'un mois[1188] pour rendre son avis sur la méthodologie du traitement de données : passé ce mois, son avis, s'il n'a pas été rendu, sera réputé favorable. Dans le même temps, l'INDS, dans le cas où il est saisi par la CNIL ou le ministre chargé de la santé, ou s'il s'est auto-saisi dans la semaine (soit 5 jours ouvrés) qui suit l'avis du CEREES, sur le caractère d'intérêt public que présente un projet de recherche, d'étude ou d'évaluation déposé dans le cadre de la sous-section 2 de la section 3 du chapitre III du titre II de la loi relative à l'informatique et aux libertés[1189], dispose d'un mois pour rendre son avis. Cependant, ni les textes de loi, ni le décret pris en Conseil d'Etat[1190], ne prévoient de mesure en cas de silence de l'INDS après expiration dudit délai. S'agissant du CPP[1191] qui est compétent pour rendre son avis à la place du CEREES en cas de projet de recherches impliquant la personne humaine, il dispose de 45 jours (soit environ 33 jours ouvrés) pour se prononcer[1192] : en revanche, son silence vaut rejet de la demande. Enfin, lorsque le dossier arrive entre les mains de la CNIL, si le texte de la loi réformant l'accès sélectif[1193] n'a pas prévu de délai pour la prise de décision d'autorisation ou de refus du traitement envisagé, la loi relative à la protection des données personnelles[1194] visant à adapter le droit français au Règlement général pour la protection des données[1195] puis l'ordonnance du 12 décembre 2018[1196] précisent qu'elle dispose de 2 mois, renouvelables une seule fois, pour dévoiler le contenu de sa décision. En admettant qu'une demande ait pour objet l'accès à des données dans le cadre d'une recherche impliquant la personne humaine, le temps maximum d'attente du demandeur pour recevoir une réponse,

[1187] *Supra* n° 333 à 336.

[1188] Décret n° 2016-1872 du 26 décembre 2016, *op. cit*.

[1189] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[1190] Décret n° 2016-1872 du 26 décembre 2016, *op. cit*.

[1191] Comité de protection des personnes.

[1192] Art. R. 1123-23 du code de la santé publique.

[1193] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1194] Loi n° 2018-493 du 20 juin 2018, *op. cit*.

[1195] Règlement 2016/679, *op. cit.*

[1196] Ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

dans le cas où tous les intervenants possibles seraient sollicités, ne devrait donc pas dépasser 6 mois et 59 jours (soit 165 jours ouvrés, si l'on considère qu'un mois contient 20 jours ouvrés). Toutefois, s'agissant des demandes d'accès sélectif destiné à effectuer de la recherche n'impliquant pas la personne humaine, le délai maximum ne pourra excéder 6 mois et 14 jours (soit 132 jours ouvrés).

Chacun des intervenants dans le processus d'autorisation d'accès sélectif aux données de santé se voit limité dans la durée pour délivrer son avis ou sa décision. Le respect de ces délais est un enjeu majeur pour la fluidité de l'accès sélectif, mais c'est aussi un point déterminant pour asseoir la légitimité du nouveau mécanisme. En effet, l'intérêt de la réforme est de proposer un cheminement balisé pour l'usager qui assure au demandeur une réponse à sa demande d'accès aux données de santé dans les temps impartis. L'objectif est évidemment de ne plus connaître de délais allant jusqu'à 11 mois[1197] avant d'obtenir une décision de la CNIL. Pourtant, rien ne garantit vraiment que les limites imposées par les textes de loi seront nécessairement respectées : il nous appartient de dresser les conséquences que des retards entraineraient selon que nous nous plaçons du point de vue de l'intervenant (le CEREES, l'INDS, le CPP ou la CNIL), ou de celui du demandeur d'accès (l'acteur public non bénéficiaire de l'accès permanent ou l'acteur privé à but non lucratif).

430. Imaginons d'abord la situation du demandeur qui dépose un dossier. Si son projet implique des recherches sur la personne humaine, il doit passer par le CPP : étant donné que l'absence de décision de ce comité entraine le rejet de la demande, la conséquence est claire pour le demandeur, c'est un retour à la définition du projet. Si son projet n'implique pas la personne humaine, alors sa demande est déposée auprès de l'INDS qui la transmet, une fois que le dossier est complet, au CEREES. Si cet intervenant ne s'est pas prononcé après un mois, son avis est favorable par défaut, ce qui peut constituer un handicap lors de l'examen ultérieur par la CNIL. Il en va de même en cas de recours à l'avis de l'INDS concernant le caractère d'intérêt public de la recherche : si l'avis n'est pas rendu dans les temps, comment cela sera-t-il interprété par la CNIL ? Il est probable que la Commission accordera naturellement plus de crédit à une demande d'accès sélectif ayant reçu un avis positif du CEREES et/ou de l'INDS qu'une demande qui n'aura fait l'objet que d'un avis positif par défaut. Le retard du CEREES ou de l'INDS pourrait donc avoir un effet néfaste sur le devenir de la demande d'accès sélectif.

[1197] *Supra* n° 387.

Cependant, si ces retards risquent de nuire au projet de recherche dans le domaine de la santé, ils ne ralentissent pas la durée de la procédure.

A contrario, si nous nous reportons à l'article 66 de la loi relative à l'informatique et aux libertés[1198], la CNIL devra nécessairement rendre sa décision dans un délai de quatre mois au maximum. Dans le cadre de l'accès sélectif, l'absence de décision est, cette fois-ci, muée en refus par défaut à moins que le ou les avis rendu(s) par le CEREES et, éventuellement, l'INDS, soient expressément favorables. Jusqu'à la fin de l'année 2017 les délais de traitement des dossiers et de transmission à la CNIL ont été respectés d'après la présidente de l'INDS[1199], cependant, aucune mesure ne garantit qu'ils le seront aussi dans les années à venir. Cela signifie que si cela devient nécessaire, le temps d'examen par la CNIL pourrait être étendu sans que les demandeurs de l'accès sélectif ne puissent obtenir l'accélération du processus.

Nous comprenons bien que, malgré le fait que le silence du CEREES soit considéré comme un avis favorable ou que celui de l'INDS ne soit pas officiellement pénalisant, tout dépassement des temps d'examen par un ou plusieurs intervenants de la procédure d'accès sélectif aurait des conséquences préjudiciables sur l'auteur de la demande : cela affectera aussi bien les chances d'autorisation du projet par la CNIL que la viabilité du projet du demandeur si plusieurs mois de retard sont constatés.

431. Supposons maintenant que nous sommes l'un des acteurs intervenant dans la chaîne d'autorisation de l'accès sélectif. Que nous soyons le CEREES ou l'INDS, toute absence d'avis dans les délais impartis, si elle n'a pas de conséquence directe sur le devenir de la demande, pourrait être perçue négativement par les autres autorités mais aussi par les usagers. Effectivement, le silence peut être interprété de plusieurs façons : nous pourrions penser que le personnel n'est pas assez nombreux pour traiter les dossiers, qu'il n'est pas assez bien formé, en résumé, que le comité ou l'institut est submergé par le nombre de demandes qu'il reçoit et qu'il n'est pas apte à faire face aux impératifs de temps.

[1198] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[1199] SAUVE J.-M., TABUTEAU D., DECOU-PAOLINI R., VASILIU I., MIGNARD J.-P., BRAS P.-L., GIRARD M., POLTON D., DAUTIEU T., STASSE F., METTENDORFF M., MADDALONE P., SAOUT C., FOMBEUR P., LAUDE A., MARTINEL A., LUCAS J., COMBREXELLE J.-D., « Santé et protection des données », *op. cit.*

Le raisonnement ne sera pas identique s'agissant du CPP. Son silence valant rejet de la demande, les auteurs du dossier pourraient se sentir lésés de ne pas avoir de motif de rejet et donc de ne pas avoir d'indices leur permettant de requalifier leur projet de recherche dans le domaine de la santé impliquant la personne humaine.

Enfin, la ponctualité de la CNIL dans ses analyses de dossiers est déterminante. Le délai étendu de deux mois, renouvelable une fois, associé au fait que chaque demande a déjà fait l'objet d'un avis du CEREES et, le cas échéant, d'un avis de l'INDS, ne permet à la Commission de connaître aucun retard dans le rendu de ses décisions. Dans le cas où elle en connaîtrait, ces retards seraient probablement interprétés comme une preuve d'incapacité à assurer le bon fonctionnement du dispositif. Pendant les quatre premiers mois d'activités du SNDS, les délais ont bien été respectés d'après D. POLTON[1200], présidente de l'INDS. Mais plusieurs mois après cette déclaration, le constat est plus contrasté. En effet, le tableau de bord des dossiers de demande d'accès sélectif au SNDS actualisé à la date du 6 novembre 2018[1201] montre que les délais maxima prévus par les textes ont pu être dépassés. Le délai moyen d'instruction d'un dossier entre son envoi par l'INDS au CEREES et la décision finale de la CNIL est de 34 jours ouvrés, ce qui est largement conforme aux limites fixées par les textes que nous estimons à 132 jours ouvrés[1202]. Le délai médian, lui, est de 71 jours ouvrés, ce qui reste dans le sillage des délais autorisés. En revanche, le tableau de bord signale que le délai d'examen des dossiers a pu atteindre 188 jours ouvrés, ce qui est bien supérieur à ce que prévoient les dispositions légales et réglementaires. Ce dépassement, certes ponctuel, des délais prévus, démontre que la procédure d'examen des demandes d'accès sélectif peut déjà légèrement s'enrayer : la raison peut notamment provenir de la nature d'un dossier particulièrement ardu à traiter qui demanderait de plus amples réflexions. La réforme du 26 janvier 2016[1203] a pourtant été bâtie pour favoriser un examen rapide et facilité de chaque demande par les services de la CNIL, y compris les demandes les plus complexes : tout l'enjeu est donc de savoir si le rythme imprimé au lancement du SNDS et tenu jusqu'à la fin de l'année 2018 pourra être maintenu, tout en récoltant, dans le même temps, de plus en plus de dossiers en provenance, notamment, du secteur privé.

[1200] *Ibid.*

[1201] Institut national des données de santé, « Worklfow sur les demandes d'utilisation des données du SNDS », 06/11/2018.

[1202] *Supra* n° 429.

[1203] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

432. La solution proposée par le nouvel accès sélectif pour anticiper la hausse du nombre de demandes et éviter l'engorgement des services du CEREES, de l'INDS et de la CNIL consiste d'ailleurs dans la mise en œuvre de procédures simplifiées[1204] qui ont vocation à se développer et dont l'efficacité sera déterminante.

433. La deuxième inconnue du nouveau système d'accès sélectif repose sur la viabilité de son co-pilotage par la CNAMTS et l'INDS. Le rapport de la Cour des comptes[1205] faisait part de ses doutes, sans aucune ambiguïté, concernant le risque de concurrence entre les instances chargées de gérer le SNDS et de la mise à disposition des données. En regrettant la complexification de « *la définition des responsabilités et des compétences du gestionnaire technique qu'est la CNAMTS* » face aux « *organismes, désignés par décret en Conseil d'Etat,* [qui peuvent] *gérer eux-mêmes la mise à disposition effective des données du SNDS* »[1206], les auteurs du rapport prônaient clairement la suprématie d'un acteur – la CNAMTS – dans la gestion globale du SNDS et dans la mise à disposition des données. Ledit décret[1207] est bien paru et indique effectivement que si la CNAMTS est chargée de la mise en œuvre du SNDS, elle peut déléguer à l'INDS, dans le cadre d'une convention, la mission de réaliser les extractions et la mise à disposition effective des données issues du SNDS. La convention doit cependant préciser quel est le service de l'INDS chargé de ces opérations, dans quelles conditions sont suivies les demandes de mise à disposition des données, les extractions réalisées, les personnels habilités à réaliser ces extractions, et quelles mesures de sécurité sont mises en place. Les dispositions prévues par le décret semblent suffisamment précises pour permettre un partage clair de compétences dans le cadre de la gestion du SNDS. Cependant, les facteurs humains et financiers entrent également en ligne de compte et auront nécessairement, dans la pratique, un effet sur la capacité de chacun des intervenants dans la gouvernance du SNDS à assurer sa part de responsabilités.

Après quelques mois d'activité du nouvel accès sélectif, il semble que les craintes de la Cour des comptes ne se soient pas réalisées, mais le dispositif est encore en phase de montée en

[1204] *Supra* n° 420 à 427.

[1205] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 96.

[1206] *Ibid.*

[1207] Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé », JORF n° 0301 du 28/12/2016.

charge et sa viabilité n'a pas encore été totalement mise à l'épreuve. Le projet de loi relatif à l'organisation et à la transformation du système de santé[1208] pourrait, par ailleurs, avoir des conséquences sur le pilotage du SNDS avec la transformation de l'INDS en Plateforme des données de santé dont l'une des missions devrait être de « *réunir, organiser et mettre à disposition les données du système national des données de santé* » d'après l'article 11 dudit projet.

434. Le troisième aléa de l'accès sélectif tel qu'il est mis en œuvre depuis le mois de septembre 2017 vise la capacité de l'INDS et de la CNIL à assumer leur mission de vérifier, *a posteriori,* les traitements mis en œuvre. En effet, la nouvelle procédure est supposée permettre de multiplier les traitements de données de santé à des fins de recherche, d'étude ou d'évaluation par un système d'autorisation préalable, cependant, malgré toutes les précautions prévues pour s'assurer que les traitements soient respectueux de la vie privée des individus et de la loi dans sa globalité, le contrôle des traitements pendant ou après leur mise en œuvre est nécessaire. Souvenons-nous que la CNIL ne fût pas dans la capacité de répondre à toutes les demandes d'accès sélectif avant la réforme[1209] ; cette difficulté caractérisée par un manque de personnel devrait logiquement se répercuter sur la capacité de la Commission à mener à bien sa mission de contrôle *a posteriori* prévue par les articles 8, 2°, g) et 19 de la loi relative à l'informatique et aux libertés[1210]. C'est là l'une des craintes exprimées dans le rapport BRAS qui déplore que « *la CNIL* [n'ait] *jamais procédé à un contrôle a posteriori du SNIIRAM et du respect des autorisations de traitement délivrées, tant en matière d'utilisation que de destruction des données transmises* »[1211]. L'explication principale à cette carence majeure relève, une fois de plus, du manque de moyens humains : en 2013, seules 17 personnes[1212] étaient affectées au contrôle *a posteriori* de tous les traitements relevant du champ de compétence de la CNIL. L'auteur ajoute que cette absence de contrôle postérieur à l'autorisation de traitement « *apparaît comme une faille majeure, qui entache la pertinence des procédures* »[1213]. Il semble

[1208] Projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019.

[1209] *Supra* n° 398.

[1210] Loi n° 78-17 du 6 janvier 1978, *op. cit*., modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[1211] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.*, p. 104.

[1212] *Ibid*., p. 104.

[1213] *Ibid.*, p. 105.

que la Commission ait entendu les craintes exprimées par P.-L. BRAS car plusieurs délibérations successives, datées du 6 juillet 2017[1214], du 25 janvier 2018[1215], et du 12 juillet 2018[1216] ont habilité, pour cinq ans, des listes successives de, respectivement, 89 agents, puis 92 agents, et enfin 99 agents, à effectuer les visites et vérifications prévues par l'article 19 de la loi 6 janvier 1978. Il existe donc aujourd'hui 82 agents de plus qu'en 2013 compétents pour mener à bien la mission de contrôle *a posteriori* de la CNIL.

En complément, l'alinéa 13 de l'article L. 1461-3 du code de la santé publique impose désormais au demandeur d'accès sélectif qui obtient l'autorisation de mener son traitement de données de santé à transmettre à l'INDS « *la méthode, les résultats de l'analyse et les moyens d'en évaluer la validité* » afin de permettre audit groupement d'intérêt public de rendre publics la méthode et les résultats. Cette obligation est un premier pas vers le contrôle de l'utilisation réelle des données de santé communiquées au demandeur. Nous pouvons rester circonspects devant cette mesure en ce que l'obligation de communication qui repose sur le bénéficiaire de l'accès sélectif doit être remplie « *dans un délai raisonnable* » d'après le texte de loi. Cela va potentiellement conduire l'INDS à suivre de près chacun des demandeurs d'accès sélectif ayant reçu une autorisation afin de savoir si sa recherche, son étude ou son analyse des données de santé transmises est terminée, tout cela pour mesurer le caractère raisonnable du délai communication des informations prévues par le code de la santé publique. Cette étape du contrôle de ce qu'il advient véritablement des données de santé obtenues dans le cadre de l'accès sélectif peut aussi être perçue comme une façon de sélectionner les traitements qui peuvent faire l'objet du contrôle de la CNIL, mais son effectivité devra être démontrée dans la pratique.

435. La capacité des intervenants de l'accès sélectif à exercer efficacement leur mission de contrôle des traitements de données de santé sera déterminante pour la confiance des individus dans le SNDS. Si le renforcement des moyens humains dédiés à cette finalité ainsi que des procédures auxquelles sont soumis les bénéficiaires de l'accès sélectif est bien visible dans les

[1214] Délibération n° 2017-197 du 6 juillet 2017 habilitant des agents de la CNIL à procéder à des missions de vérification.

[1215] Délibération n° 2018-026 du 25 janvier 2018 habilitant des agents de la CNIL à procéder à des missions de vérification.

[1216] Délibération n° 2018-290 du 12 juillet 2018 habilitant des agents de la CNIL à procéder à des missions de vérification.

textes, c'est leur concrétisation matérielle qui permettra de caractériser une protection suffisante de la vie privée et le bon usage des données de santé issues du SNDS.

B) La sécurité contestée de l'accès sélectif

436. La bonne mise en œuvre de l'accès sélectif au SNDS est, nous l'avons vu précédemment, soumise à des facteurs variés qui ont chacun un impact sur le fonctionnement du dispositif. Mais, si un seul facteur permettant de stocker et mettre à disposition des données à caractère personnel aussi sensibles devait être retenu, ce serait celui de la sécurité qui s'érige en préalable inconditionnel, telles les fondations du dispositif. Toutes les données de santé destinées à faire partie du SNDS et de l'accès sélectif doivent nécessairement faire l'objet d'une protection qui garantisse le respect de la vie privée des individus qui en sont à l'origine. Comme expliqué au début de cette étude[1217] le système de chiffrement des données de santé à caractère personnel utilisé depuis 2002 par la CNAMTS pour la gestion du SNIIRAM est réutilisé pour le SNDS. Cette protection des données, appelée « *fonction d'occultation des informations nominatives* », ou FOIN, est supposée être irréversible afin d'empêcher de faire une table de correspondance entre les identifiants de départ de chaque donnée et leur numéro d'anonymat. Mais ce mécanisme est vieillissant et fait pâle figure devant les innovations technologiques, telles que les données massives, qui permettent de traiter des volumes de données extrêmement importants et, potentiellement, de réidentifier les individus à partir de données anonymisées censées être sécurisées.

C'est pour cela que la Cour des comptes[1218] et la CNIL[1219] ont toutes deux émis des réserves au sujet du niveau insuffisant de protection des données de santé à caractère personnel. La Cour rappelait ainsi, en 2016, que la CNAMTS est de fait un hébergeur de données de santé au sens des articles L. 1111-8, L. 1121-1 du code de la santé publique et de la loi du 6 janvier 1978 : pourtant, elle n'a pas eu à solliciter l'agrément du ministère de la santé après avis de la CNIL et du comité d'agrément. Pourquoi un tel passe-droit ? Parce que, dit la Cour, « *techniquement, un tel agrément imposerait des mises en conformité dont la caisse nationale estime qu'elles*

[1217] *Supra* n° 139 et 153.

[1218] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 41.

[1219] Délibération n° 2016-316 du 13 octobre 2016, portant avis sur un projet de décret en Conseil d'Etat relatif au Système national des données de santé.

seraient sans doute lourdes et coûteuses, et hors de portée en l'état de ses moyens »[1220]. Malgré le caractère sensible des données gérés par la CNAMTS, la mise à jour du dispositif de sécurité ne semble pas être une priorité absolue : c'est un paradoxe quand on sait que c'est justement la protection de la vie privée qui motive l'existence même de l'accès sélectif au SNDS. Il est malgré tout reconnu[1221] que la CNAMTS travaille, depuis 2013, à la meilleure sécurisation de ses systèmes d'information : un plan d'action sécurité sur le SNDS est censé avoir été mis en œuvre par la CNAMTS depuis 2017 pour aboutir, fin 2019, au lancement d'un nouveau système de sécurité entièrement opérationnel[1222]. Cependant, cet engagement de sécurisation ne semble pas avoir convaincu, outre mesure, la CNIL.

437. En effet, les craintes concernant la sécurité des données du SNIIRAM émises par la Cour des comptes en 2016[1223] ont été confirmées par la CNIL qui a mis en demeure[1224], au début de l'année 2018, la CNAMTS, elle-même responsable du traitement du SNDS et du SNIIRAM, de « *prendre toute mesure pour garantir la sécurité et la confidentialité des données à caractère personnel traitées* ». Cette mise en demeure devait être respectée dans les trois mois, afin d'être conforme au moment de l'entrée en vigueur du RGPD[1225], le 25 mai 2018. C'est un avertissement sans ambiguïté concernant l'adaptation nécessaire et rapide des bases de données administratives en santé aux technologies innovantes, notamment en matière de cryptage. Entre cette mise en demeure et la fin de l'année 2018, aucune communication supplémentaire n'a été diffusée sur cette question : cela signifie potentiellement que la CNAMTS a apporté à la CNIL les éléments suffisants permettant d'attester des travaux en cours pour améliorer la sécurité des données de santé à caractère personnel. Il serait tout de même intéressant qu'une mise à jour de la situation soit officiellement publiée.

[1220] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 41.

[1221] Rapport d'information déposé par la Commission des affaires sociales à l'Assemblée nationale 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, 21 février 2017, p. 71.

[1222] *Ibid.*, p. 72.

[1223] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 41 à 47.

[1224] Décision n° MED-2018-006 du 8 février 2018 mettant en demeure la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés.

[1225] Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016, *op. cit.*

438. Dans la foulée de la mise en demeure de la CNIL, un effet secondaire inattendu mais bénéfique a été observé. Lors des discussions qui ont précédé le vote de la loi du 20 juin 2018[1226] un nouvel article[1227] a été inséré dans le texte. Cet article est entièrement dédié à la mise en place d'un comité d'audit du SNDS. D'abord, nous pouvons penser que cette initiative du législateur n'est pas anodine dans la mesure où c'est juste avant l'ouverture des débats que la CNIL a mis en demeure la CNAMTS, responsable de traitement du SNIIRAM, de « *prendre toute mesure pour garantir la sécurité et la confidentialité des données à caractère personnel traitées* »[1228]. Dans le document rendu public par la CNIL, de nombreux manquements à la sécurité des données à caractère personnel ont été constatés concernant notamment « *la pseudonymisation des données, les procédures de sauvegarde, l'accès aux données par les utilisateurs du SNIIRAM et par des prestataires, la sécurité des postes de travail des utilisateurs du SNIIRAM, les extractions de données individuelles du SNIIRAM ainsi que la mise à disposition d'extractions de données agrégées du SNIIRAM aux partenaires* »[1229]. La force des critiques émises par la Commission ont dû toucher plus d'un parlementaire. Etant donné que le SNIIRAM est désormais partie intégrante du SNDS, la décision du législateur de créer un comité d'audit capable de contrôler tous les systèmes le composant est bienvenue : l'objectif est de garantir un niveau de sécurité optimal pour toutes les données contenues dans le SNDS et potentiellement transmises aux responsables de traitement qui bénéficient d'une autorisation d'accès sélectif. Le décret pris le 1er août 2018[1230] est venu préciser la composition et le fonctionnement de ce comité d'audit qui doit se réunir au moins deux fois chaque année pour fixer les orientations à partir desquelles le président du comité décide des audits à réaliser dans l'année. Les entités qui font l'objet d'un audit doivent nécessairement rendre compte, auprès du président du comité d'audit et des auditeurs, du plan d'action mis en œuvre. Signalons également que le président du comité d'audit rend compte annuellement au ministre chargé des affaires sociales et de la santé ainsi qu'au comité stratégique de la stratégie d'audit du comité d'audit (sic) « *des audits réalisés, du niveau global de maîtrise des opérations, des problèmes*

[1226] Loi n° 2018-493 du 20 juin 2018, *op. cit*.

[1227] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, art. 65, modifié par la loi n° 2018-493 du 20 juin 2018, *op. cit.*, devenu art. 77 avec l' l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit*.

[1228] Décision n° MED-2018-006 du 8 février 2018 mettant en demeure la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés.

[1229] *Ibid.*

[1230] Décret n° 2018-687 du 1er août 2018 pris pour l'application de la 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.

significatifs constatés ainsi que des recommandations formulées pour respecter la législation en vigueur, les référentiels et réduire les risques »[1231]. La création de ce comité n'est donc pas purement cosmétique pour rassurer les individus – et la CNIL – sur la sécurité des données de santé à caractère personnel les concernant : l'objectif est d'opérer un véritable contrôle qualité des mesures de protection des données contenues dans le SNDS par le biais d'audits réalisés par des prestataires indépendants. Il est encore trop tôt pour savoir si l'activité de ce comité donne des résultats probants. Des études ultérieures devront ainsi faire la lumière sur l'impact, s'il existe, de ce comité sur la sécurité des données au sein du SNDS.

439. La pérennité de l'accès sélectif aux données de santé est finalement suspendue au bon fonctionnement des mécanismes permettant aux bénéficiaires de tirer tous les fruits qui leurs sont promis par les textes, mais aussi aux individus dont les données font l'objet d'un traitement d'être assurés que toutes les mesures de contrôle et de vérification sont opérationnelles. Seule une exploitation durable de l'accès sélectif au SNDS permettra de produire une analyse pertinente des résultats obtenus à chacun des niveaux détectés.

440. Nous le comprenons, le nouvel accès sélectif est encore en cours de consolidation : son plein potentiel ne pourra être atteint que dans les années à venir avec l'intégration des ultimes données de santé[1232] prévues par les textes[1233] ; l'apport attendu de réponses à des questions cruciales, comme celle du coût, pour un demandeur privé, de l'accès au SNDS[1234], ou encore la concrétisation des différentes procédure simplifiées[1235]. Ce n'est qu'une fois que ces éléments posés que l'accès sélectif sera stabilisé à *minima* et pourra être pleinement fonctionnel : ce n'est qu'alors que tout un chacun sera en mesure d'en analyser les véritables forces et faiblesses.

[1231] *Ibid.*

[1232] *Supra* n° 414 et 415.

[1233] Art. L. 1461-1 du code de la santé publique.

[1234] *Supra* n° 416 à 419.

[1235] *Supra* n° 420 à 427.

CONCLUSION DU CHAPITRE II

441. Le nouvel accès sélectif aux données de santé entend répondre aux différentes critiques émises à l'encontre du précédent mécanisme. La tâche est importante au regard des imperfections et dysfonctionnements qui ont émaillé les 15 ans d'existence de l'accès sélectif initial. Toutes les difficultés n'ont pu être gommées : certaines contraintes, telle la sécurité des données, sont inhérentes à la nature des données dont il est question et ne peuvent être écartées sans contrepartie. La participation de plusieurs intervenants dans la procédure d'examen des demandes d'accès sélectif demeure nécessaire afin de recueillir l'avis de plusieurs collèges de spécialistes concernant la méthode de traitement envisagée et l'intérêt général. Cela permet à la CNIL de fonder sa décision finale de refus ou d'autorisation plus aisément, sur la base des réflexions émises par les autres instances. Signalons toutefois que l'INDS, transformé en PDS (plateforme des données de santé) dans le nouveau projet de loi relatif à l'organisation et à la transformation du système de santé[1236], perd sa capacité à se prononcer sur l'intérêt public d'un traitement : son rôle est réduit à celui de guichet unique dans le cadre de l'accès sélectif. Avec le projet de loi c'est maintenant le CESREES (remplaçant du CEREES) qui est pleinement compétent pour cela. Le CESREES et la CNIL forment donc un duo chargé de travailler en bonne collaboration pour délivrer les autorisations d'accès aux données de santé contenues dans le SNDS.

442. Face à ces difficultés incompressibles, un problème majeur a pu être résolu. Les retards importants dans la délivrance des accès sélectifs ont été grandement limités grâce à plusieurs actions. La première est la mise à disposition d'un maximum de données anonymisées et ne présentant pas de risque de réidentification. Cela permet de réduire, dans un premier temps, les demandes d'accès sélectif. La seconde action relève de l'amélioration de la formation du personnel des intervenant dans la gestion des données de santé ainsi que le renforcement des équipes concernées.

Pourtant, la version réformée de l'accès sélectif aux données de santé présente encore des imperfections : nous faisons ici référence aux accès simplifiés, encore trop rares, ainsi qu'aux données de santé supposées être disponibles qui sont incomplètes au moment de l'écriture de

[1236] Projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019.

ces lignes. La question du coût de l'accès sélectif aux données de santé reste également mystérieuse car c'est un sujet explosif qui, pour le moment, ne semble pas trouver de réponse.

Ces imperfections du nouvel accès sélectif sont accompagnées par des questionnements sur l'application du dispositif dans le temps. Les intervenants de la procédure arriveront-ils à tenir les délais d'examen si les demandes d'accès augmentent ? L'INDS, devenu PDS, et la CNIL travailleront-ils toujours ensemble dans le cadre d'une collaboration vertueuse pour le bon fonctionnement de l'accès aux données du SNDS ? Le contrôle des traitements effectués avec les données de santé obtenues dans le cadre de l'accès sélectif sera-t-il opérationnel ? Ces questions sont en suspens et ne trouveront de véritable réponse que dans la pratique. Elles ont toutes un facteur en commun : celui de la maîtrise de l'accès aux données de santé, si ce n'est la maîtrise des données elles-mêmes, qui recèle en creux la capacité du système à assurer la protection du droit au respect de la vie privée.

CONCLUSION DU TITRE II

443. Le développement de l'accès sélectif aux données de santé demeure soumis à des conditions très strictes qui paraissent relever d'intérêts contradictoires. Effectivement, d'une part, les autorités affichent clairement leur volonté de rendre accessibles un maximum de données issues du SNDS dans le cadre de l'intérêt public. D'autre part, la priorité donnée à la protection de la vie privée des individus et à la sécurité de leurs données à caractère personnel ralentit nécessairement la mise à disposition des données du SNDS. Les auteurs de la réforme du 26 janvier 2016[1237] se sont alors efforcés de ménager chacun des aspects de l'accès sélectif pour proposer un mécanisme parvenant à allier protection des individus et large accessibilité des données.

444. Cette réforme s'est donc construite à partir de l'analyse préalable des dysfonctionnements de l'accès sélectif, caractérisés à travers divers rapports et comptes-rendus sur le sujet. L'isolement de chaque facteur ayant un impact négatif sur l'accès sélectif permet de faire émerger plus aisément des axes de réforme. L'inadaptation de la structure même de l'accès sélectif à l'usage qui lui est destiné a ainsi été mise en exergue : sa faible utilisation jusqu'en 2015, probablement liée à la répartition floue des compétences entre les acteurs intervenant dans la procédure, constitue un signe fort. Le mauvais fonctionnement de l'accès sélectif semble également être dû à des difficultés internes liées à la complexité de la tâche dévolue aux agents des différents intervenants que sont le CEREES, l'IDS et la CNIL.

445. C'est à partir de ces différents constats que la réforme de l'accès sélectif a été engagées. Il est indéniable que les améliorations apportées sont clairement visibles dans les nouveaux textes. Malgré tout, des incertitudes demeurent et certaines complexités, notamment dans la procédure, semblent ne pas pouvoir être totalement écartées. Il en découle un mécanisme qui ne peut être mis en place que sur plusieurs années, et dont la pose des ultimes briques constitutives n'a été prévue par les acteurs de la réforme qu'à partir l'année 2019 au plus tôt[1238]. Un halo d'incertitudes et d'interrogations entoure donc logiquement le nouvel accès sélectif qui, bien

[1237] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1238] Nous pensons à l'intégration, dans le SNDS des données médico-sociales des maisons départementales des personnes handicapées, des données de remboursement par bénéficiaire transmis par les organismes de complémentaire santé.

que pourvu de nombreuses garanties et de promesses quant à sa fluidité, son accessibilité, et la sécurité des données qu'il met à disposition, doit encore démontrer son plein potentiel.

CONCLUSION DE LA PARTIE II

446. A l'issue de nos réflexions des deux précédents chapitres, nous pouvons émettre l'hypothèse selon laquelle l'accès sélectif tel qu'il a été créé par la réforme du 26 janvier 2016[1239], est la première véritable incursion dans le monde du partage contrôlé des données de santé à grande échelle associé à une démarche protectrice de la vie privée. La dizaine d'années[1240] ayant précédé la réforme n'aurait été qu'un essai peu convaincant de rendre les données du SNIIRAM ou du PMSI accessibles sur demande : le cloisonnement de la procédure, mais surtout l'instabilité des textes et les délais d'examen incertains des dossiers ont démontré l'absence de véritable volonté d'améliorer le système pour le rendre plus accessible[1241].

L'accès sélectif a donc été réformé en suivant une démarche académique : plusieurs rapports ont été réalisés[1242], les fondations du système ont été conservées et remodelées pour parvenir à trouver un compromis plus fonctionnel si nous nous en tenons aux textes. En effet, si le partage de la connaissance est l'objectif diffusé à travers les finalités[1243] du nouveau SNDS[1244], toutes les dispositions qui y sont afférentes traitent avant tout des modalités de la protection de la vie privée par des systèmes d'autorisation préalable mais aussi par des mécanismes de traitement des données personnelles *a priori*. La question de la protection de la vie privée dans le cadre de l'accès sélectif a d'ailleurs fait l'objet d'interrogations doctrinales importantes[1245].

[1239] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1240] *Supra* n° 391 et 392.

[1241] *Supra* n° 358 à 390.

[1242] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.* ; BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé*, *op. cit.* ; GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *Pour une meilleure utilisation des bases de données administratives et médico-administratives nationales pour la santé publique et la recherche*, *op. cit.* ; GORCE G. et PILLET F., Rapport d'information au Sénat, *La protection des données personnelles dans l'open data : une exigence et une opportunité, op. cit. ;* TROJETTE Mohammed Adnène avec le concours de LOMBARD Rémy, Rapport au Premier ministre, *Ouverture des données publiques. Les exceptions au principe de gratuité sont-elles toutes légitimes ?*, juillet 2013, 121 p.

[1243] *Supra* n° 331.

[1244] V. art. L. 1461-1 III du code de la santé publique.

[1245] BOSSI J., « Comment organiser aujourd'hui en France la protection des données de santé », *op. cit.* ; LAUDE A., « De quelques problématiques relatives à l'ouverture des bases de données en santé », *op. cit.* ; PECHILLON E., « L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ? », *op. cit.*

447. C'est en tenant compte des opportunités avancées par les uns et des avertissements lancés par les autres que le nouvel accès sélectif issu de la réforme nous promet des démarches plus simples grâce au principe du guichet unique[1246], une procédure aux délais connus et maîtrisés par chacun des intervenants, la mise en œuvre de procédures annexes simplifiées. Dans les textes, tout se tient et paraît favorable à une exploitation optimisée du SNDS. Cependant, la mise en situation réelle est parfois un passage compliqué pour les réformes et nécessite un regain d'engagement et de bonne volonté de chacune des parties prenantes. En toute objectivité, il semble que les premiers mois d'activité de l'accès sélectif du SNDS se soient déroulés dans des conditions relativement bonnes[1247] et que les modifications apportées par la réforme aient porté leurs fruits malgré des dépassements de délais ponctuels dans l'examen des demandes d'accès. La complexité de l'ensemble du dispositif demeure malgré tout et il ne sera complet, tant dans les données qu'il est censé proposer, que dans les différentes opportunités d'accès qu'il est supposé offrir, que plusieurs mois après sa mise en fonction.

448. Cet accès sélectif constitue la pierre angulaire du SNDS et son bon fonctionnement est crucial pour l'avenir du dispositif. C'est d'autant plus vrai lorsque nous savons que les acteurs privés à but lucratif y sont désormais intégrés après une longue période d'interdiction de principe. L'objet de notre prochaine partie sera par conséquent de comprendre la place des acteurs privés à but lucratif dans l'accès aux données de santé.

[1246] *Supra* n° 333.

[1247] *Supra* n° 429 à 431.

PARTIE III

LA TRANSPARENCE TARDIVE DES DONNÉES DE SANTÉ POUR LES ACTEURS PRIVÉS À BUT LUCRATIF

449. Les deux précédents titres nous ont permis de développer le cadre juridique de l'accès aux données de santé pour les acteurs publics bénéficiaires d'un accès permanent[1248] et pour les acteurs publics (non bénéficiaires d'un accès permanent) ou privés à but non lucratif[1249]. Chacun de ces types d'accès est régi par un dispositif destiné à assurer la protection adéquate des données de santé pour préserver le droit au respect de la vie privée dont les individus producteurs desdites données sont titulaires. Mais un troisième grand ensemble d'acteurs est absent des premiers accès déjà étudiés : il s'agit des acteurs privés à but lucratif parmi lesquels se trouvent, entre autres, les laboratoires de recherche pharmaceutique, mais aussi les entreprises d'assurance. Leur intégration dans le mécanisme d'accès aux données de santé n'a pas été immédiate alors même que ces acteurs sont parfois dotés de moyens humains, techniques et financiers équivalents, sinon supérieurs, aux acteurs publics ou privés à but non lucratifs : leurs capacités de réalisation d'études et de recherches dans le domaine de la santé sont importantes. Cependant, malgré leur apport potentiel dans la maîtrise et la connaissance des données de santé en France, c'est leur nature même qui semble contradictoire avec l'objectif de nécessaire protection de la vie privée. En effet, les acteurs privés à but lucratif sont mus par l'ambition première de créer de la richesse afin de la partager entre leurs membres participants. Il ressort de cet objectif financier que la protection de la vie privée paraît susceptible de passer au second plan si le traitement de certaines données aboutit à un gain pécuniaire. Le droit au respect de la vie privée étant une liberté constitutionnellement protégée[1250], il constitue un

[1248] V. Partie I.

[1249] V. Partie II.

[1250] V. *supra* n° 53 à 62, et notamment Conseil constitutionnel, décision n° 99-416 DC du 23 juillet 1999 *relative à la loi portant création d'une couverture maladie universelle*, JORF n° 172, 28/07/1999 ; Conseil constitutionnel, décision n° 99-419 DC du 9 novembre 1999 *relative à la loi relative au pacte civil de solidarité*, JORF n° 265, 16/11/1999 ; Conseil constitutionnel, décision n° 99-422 DC du 21 décembre 1999 *relative à la loi de financement de la sécurité sociale pour 2000*, JORF n° 302, 30/12/1999 ; BRAIBANT G., *Données personnelles et société de l'information : transposition en droit français de la directive n° 95-46 / rapport au Premier Ministre*, La Documentation française, 1998, p. 20 ; BABUSIAUX C., BREAS L., ESLOUS L., THOUVENIN D., *Rapport,*

obstacle conséquent, mais pas insurmontable comme nous allons l'observer[1251], à l'accès aux données de santé pour les acteurs privés à but lucratif.

450. La problématique spécifique du traitement et de l'accès aux données de santé d'une manière qui respecte le principe du droit au respect de la vie privée s'est posée quelques années avant la création de la grande base SNIIRAM par la loi de financement de la sécurité sociale pour 1999[1252], comme nous l'avons étudié avec précision dans la partie précédente[1253]. Ce qui nous intéresse particulièrement dans le présent titre, c'est de comprendre qu'elle a été, et quelle est aujourd'hui, la place des acteurs privés à but lucratif dans le mécanisme imaginé par le législateur français : tout l'enjeu est de savoir quel raisonnement a été suivi pour intégrer, ou exclure, ces acteurs du système d'accès aux données de santé. Nous allons comprendre que leur position n'a pas toujours été clairement définie par les textes et a fortement évolué en quelques quinze années. Nous nous attacherons donc à démontrer que malgré des dispositions qui semblent découler d'une réflexion sans ambiguïté conduisant à interdire, par principe, l'accès aux données de santé pour les acteurs privés à but lucratif (Titre 1), l'ouverture des données de santé au bénéfice desdits acteurs privés à but lucratif a finalement été accordée, non sans difficultés (Titre 2).

L'accès des assureurs complémentaires aux données de santé des feuilles de soins électroniques, 26 mai 2003, p. 24, 26, 44 ; BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé*, 9 juillet 2014, p. 14.

[1251] *Infra* n° 483 à 506.

[1252] Loi n° 98-1194 du 23 décembre 1998 *de financement de la sécurité sociale pour 1999, op. cit.*

[1253] *Supra* n° 245.

TITRE I

L'INTERDICTION INITIALE D'ACCÈS AUX DONNÉES DE SANTÉ POUR LES ACTEURS PRIVÉS À BUT LUCRATIF

451. Les acteurs privés à but lucratif occupent une place qui a, pendant longtemps, été peu enviable dans le mécanisme de l'accès aux données de santé. Alors qu'un accès permanent[1254], pour des acteurs publics spécifiquement désignés, et un accès sélectif[1255], pour tous les acteurs non bénéficiaires de l'accès permanent, sont prévus dès le premier arrêté[1256] relatif au fonctionnement du SNIIRAM, les opportunités offertes aux acteurs privés à but lucratif restent incertaines dans la pratique[1257]. Ce n'est finalement qu'à partir du deuxième arrêté[1258] relatif à la mise en œuvre du SNIIRAM que le principe d'interdiction stricte d'obtenir des données de santé par le biais de l'accès sélectif a été posé. Nous pourrions penser que cette restriction incontournable découle directement du droit communautaire, aujourd'hui de l'union européenne, et plus particulièrement d'une ou plusieurs dispositions concrètes visant directement les acteurs privés à but lucratif. Pourtant, ce n'est que par déduction que ce principe d'interdiction se forme.

En effet, la directive de 1995[1259], à son article 8, donne une liste des cas dans lesquels « *le traitement des données relatives à la santé* » peut être autorisé par exception. Le point numéro 4 dudit article permet aux Etats membres de « *prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle* » à condition que les garanties appropriées soient assurées. C'est donc à l'initiative des autorités françaises que les acteurs privés à but lucratif ont été exclus sans aucune justification de l'accès aux données de santé du SNIIRAM. Ce manque de pédagogie est dommageable à plus d'un titre comme nous le verrons plus tard[1260].

[1254] V. Partie I.

[1255] V. Partie II.

[1256] Arrêté du 11 avril 2002 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, JORF n° 89, 16/04/2002.

[1257] *Infra* n° 456 à 461.

[1258] Arrêté du 20 juin 2005 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, JORF n° 192, 19/08/2005.

[1259] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[1260] *Infra* n° 514 à 517.

L'exclusion systématique de l'accès aux données de santé signifie-t-elle que les cibles de l'exclusion sont totalement étrangères à l'intérêt public ? Ou bien est-ce que le législateur français n'a pas été en mesure de proposer des garanties appropriées permettant de s'assurer que les acteurs privés à but lucratif ne traitent les données potentiellement accessibles que dans l'intérêt public ? Ces questions ont fait l'objet de débats et de réflexions[1261] intimement liées aux notions de données massives de données ouvertes déjà explorées en introduction de cette étude[1262].

452. Après des années d'interdiction officielle, et de questionnements sur la légitimité d'une telle mesure, la réforme mise en œuvre par la loi du 26 janvier 2016 a finalement défini un tout nouveau mécanisme. Celui-ci précise dans quelles conditions l'accès aux données de santé du nouveau système national des données de santé ou SNDS[1263] est ouvert aux acteurs privés à but lucratif. Nous verrons avec intérêt que certaines interdictions de traitement demeurent afin de garantir aux individus le respect de leur vie privée.

[1261] BERANGER J., « De l'étude des risques à la traduction des enjeux éthiques des Big Data en santé », *Journal International de Bioéthique*, 2017/3, vol. 28, p. 15-25 ; CASTETS-RENARD C., « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data », Revue Lamy de Droit de l'Immatériel, 01/10/2014, supplément au n° 108, p. 38-45 ; Comité Stratégique de Filière des Industries et Technologies de santé (CSF), « Promouvoir une démarche active visant à faciliter l'accès aux données de santé à des fins de santé publique, de recherche et de développement industriel », *Rapport du groupe CSF mesure 1-5*, 29/03/2017, 82 p. ; GOURGUES G., MAZEAUD A., « Peut-on délibérer du Big Data en santé sans controverser ? Retour sur l'expérience d'un atelier citoyen français », *Revue française des affaires sociales*, 2017/4, p. 95-115 ; MENDOZA-CAMINADE A., « Big data et données de santé : quelles régulations juridiques ? », *Revue Lamy Droit de l'immatériel*, 01/06/2016, n° 127 ; PECHILLON E., « L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ? », *L'information psychiatrique*, 8/2015, volume 91, p. 645-649 **;** RIAL-SEBBAG E., « La gouvernance des Big data utilisées en santé, un enjeu national et international », *Journal International de Bioéthique*, 2017/3, vol. 28, p. 39-50 ; VACARIE I., « La finalité des traitements de données de santé », *RGDM*, 30/09/2004, n° 4, p. 27-34.

[1262] *Supra* n° 68 à 81.

[1263] Le SNDS contient les données des bases de données relatives aux soins de ville contenues dans le SNIIRAM, les données relatives aux activités des établissements de soins contenues dans l'ATIH, des données concernant les causes de décès stockées dans le CépiDc, et devrait à terme, en 2019, contenir les données sur les maisons départementales de personnes handicapées issues de la Caisse nationale de solidarité pour l'autonomie (CNSA) ainsi que les données relatives à l'activité des complémentaires santé provenant de l'échantillon représentatif des données de remboursement par bénéficiaires transmis directement par les organismes de complémentaire santé. Le projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019 prévoit également l'ajout de nouvelles données dans le SNDS : « *Les données destinées aux professionnels et organismes de santé recueillies à l'occasion des activités mentionnées au I de l'article L. 1111-8 du* [code de la santé publique] *donnant lieu à la prise en charge des frais de santé en matière de maladie ou de maternité mentionnée à l'article L. 160-1 du code de la sécurité sociale et à la prise en charge des prestations mentionnées à l'article L. 431-1 du même code en matière d'accidents du travail et de maladies professionnelles* » et les « *données à caractère personnel des enquêtes dans le domaine de la santé, lorsque ces données sont appariées avec* [les autres données contenues dans le SNDS] ».

453. L'objet de ce chapitre est donc de comprendre dans un premier temps toute l'étendue du raisonnement qui a motivé la décision des autorités françaises d'interdire aux acteurs privés à but lucratif d'accéder aux données de santé (Chapitre 1). Nous pourrons alors dérouler le fil des événements qui ont finalement conduit le législateur à ouvrir l'accès selon des mesures suffisamment contraignantes pour ne pas faire peser de risque trop important sur la vie privée des personnes (Chapitre 2).

CHAPITRE I
LA FERMETURE DE L'ACCÈS AUX DONNÉES DE SANTÉ POUR LE RESPECT DE LA VIE PRIVÉE

454. L'interdiction d'accès aux données de santé opposée aux acteurs privés à but lucratif n'a pas été définie directement par la loi relative à l'informatique et aux libertés[1264]. La transposition de la directive communautaire de 1995[1265] par la loi du 6 août 2004[1266] aurait pourtant pu représenter une occasion de le faire, mais cette opportunité n'a pas été saisie par le législateur, préférant laisser le soin au pouvoir réglementaire de préciser le contenu de l'interdiction par arrêté. Dès lors, il est intéressant de comprendre comment une mesure aussi radicale a été prise (Section 1) pour étudier ensuite les rares possibilités offertes, en théorie, aux acteurs privés à but lucratif pour accéder à des données de santé dans le but de les traiter (Section 2).

SECTION 1 : LE CHANGEMENT DE PARADAGIME DE L'ACCÈS AUX DONNÉES DE SANTÉ

455. En envisageant la création de la base de données de santé SNIIRAM en 1998[1267], le législateur ne semble pas avoir immédiatement pensé interdire l'accès à des acteurs prédéfinis. Les modalités de gestion du système sont effectivement destinées à être définies par arrêté, pris après avis motivé de la CNIL. Pourtant, cette mesure restrictive est survenue au cours des premières années d'existence du dispositif. Dès lors, il est important de connaître l'évolution de la liberté laissée aux acteurs privés à but lucratif dans l'accès et le traitement des données de santé jusqu'à la déclaration d'interdiction (§1) et d'étudier les différents fondements juridiques et éthiques qui ont guidé cette décision (§2).

Paragraphe 1 : La flexibilité première de l'accès aux données de santé

[1264] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[1265] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[1266] 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.*

[1267] Loi n° 98-1194 du 23 décembre 1998 *de financement de la sécurité sociale pour 1999, op. cit.*

456. Les opportunités offertes aux acteurs privés à but lucratif dans le cadre du traitement des données de santé n'ont pas toujours été restreintes. Il est d'ailleurs surprenant de remarquer que les dispositions légales en vigueur dans le courant des années 1990 ont beaucoup évolué sans pour autant viser spécifiquement le secteur privé à but lucratif.

457. Dès le 3 juillet 1994, un chapitre V bis a donc été intégré à la loi relative à l'informatique et aux libertés[1268] afin d'encadrer la recherche dans le domaine de la santé par le biais du traitement de données nominatives. Lorsque l'on prend le temps d'étudier les dispositions prévues à cette époque il est impossible de ne pas remarquer que les modalités de traitement des données sont destinées à tous les acteurs, sans distinction de leur appartenance au secteur public ou privé, sans accorder d'importance à leur caractère lucratif ou non. Cet état de fait est intrigant quand nous savons que ces critères vont devenir le moyen privilégié permettant de définir des catégories d'autorisation d'accès aux données de santé. Si la loi ne précise pas les notions d'organisme privé ou public, le décret[1269] qui la met en œuvre prend soin de le faire. Mais cette dichotomie n'est pas proposée comme un critère duquel découlerait des mesures spécifiques : il s'agit simplement d'une information de forme. Le texte du décret nous informe que la procédure d'autorisation préalable de mise en œuvre d'un traitement de données nominatives à des fins de recherche dans le domaine de la santé est ouverte aussi bien aux organismes publics qu'aux organismes privés, y compris ceux qui ont un but lucratif.

458. Tous les acteurs, aussi bien publics que privés, sont donc initialement admis à demander l'autorisation de réaliser un traitement de données dans le cadre de recherches en santé. Les acteurs privés à but lucratif sont soumis à la même procédure que les acteurs publics ou que les acteurs privés à but non lucratif. Toutefois, la possibilité de réaliser des traitements de données personnelles dans le cadre de recherches dans le domaine de la santé[1270] ne leur est offerte qu'après un contrôle préalable strict par le CCTIRS et la CNIL. Ces deux examens doivent ainsi

[1268] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 94-548 du 1 juillet 1994 *relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, JORF, n° 152, 02/07/1994.

[1269] Décret n° 95-682 du 9 mai 1995 *pris pour l'application du chapitre V bis de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et modifiant le décret n° 78-774 du 17 juillet 1978*, JORF n° 0110, 11/05/1995.

[1270] D'après le document de SERRE J.-L., « Le CCTIRS : passé et présent. L'INDS & le CEREES : futur », *ADELF*, 09/09/2016, le CCTIRS recevait en moyenne 250 dossiers par an dans les années 1990, puis de 600 à 800 dans les années 2000, et de 900 à 1 100 dans les années 2010. Parmi ces dossiers, 30% en moyenne proviennent de laboratoires privés qui sont à but lucratif.

conduire à n'autoriser que les traitements qui ne comportent pas de risque pour le droit au respect de la vie privée des individus. Une précision capitale doit être apportée : cette faculté de traiter des données de santé pour le secteur privé à but lucratif ne concerne que des données qui ne proviennent pas de bases de données administratives en santé. La question spécifique de l'autorisation de traitement de données issues desdites bases ne s'est posée que quelques années après le décret du 9 mai 1995.

459. Avec l'entrée en vigueur de la loi de financement de la sécurité sociale pour 1999[1271] créant, à son article 21, le SNIIRAM, aucune précision n'est donnée quant à un traitement spécial réservé aux acteurs privés à but lucratifs pour accéder aux données de santé : rien, dans le texte de loi, ne laisse penser que l'accès au SNIIRAM fera l'objet d'accès permanents, sélectifs, ou d'interdictions d'accès. Tout reste à définir et l'ensemble du dispositif entourant cette grande base de données n'est que conjectures à cet instant. La loi du 27 juillet 1999[1272] est venue apporter une première piste de réponse, encore floue pour le secteur privé à but lucratif, en créant le chapitre V ter de la loi relative à l'informatique et aux libertés[1273] qui concerne le « *traitement des données personnelles de santé à des fins d'évaluation ou d'analyse des activités de soins et de prévention* ». Ce chapitre porte sur la faculté de transmettre, en vue d'un traitement, les données d'activités des établissements de santé publics ou privés, celles des dossiers médicaux tenus par les professionnels de santé libéraux, et surtout, celles qui sont issues des systèmes d'information des caisses d'assurance maladie : cette mention est, sans aucun doute, une référence expresse au SNIIRAM qui vient d'être créé. Il y est posé le principe selon lequel, en vertu de la protection de la vie privée des individus, seules les données qui se présentent sous « *la forme de statistiques agrégées ou de données par patient constituées de telle sorte que les personnes concernées ne puissent être identifiées* »[1274] peuvent être transmises et traitées.

[1271] Loi n° 98-1194 du 23 décembre 1998, *op. cit.*

[1272] Loi n° 99-641 du 27 juillet 1999 *portant création d'une couverture maladie universelle*, JORF n° 0172, 28/07/1999.

[1273] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 99-641 du 27 juillet 1999, *op. cit.*

[1274] Art. 40-12 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 99-641 du 27 juillet 1999, *op. cit.*

Toutefois, la CNIL peut être amenée à autoriser un traitement de données identifiantes dès lors que celles-ci ne comportent ni le nom, ni le prénom, ni le NIR[1275] des personnes. Dans un tel cas, la loi développe la procédure qui doit être suivie pour obtenir, ou non, l'autorisation de traitement de telles données de santé. Mais le texte de loi n'opère aucune distinction selon que le dépositaire de la demande de traitement est une personne publique ou privée à but lucratif : tous les demandeurs semblent faire l'objet de la même sévérité de la part de la Commission. Si un traitement est autorisé, c'est qu'il ne comporte pas de risque d'atteinte à la vie privée de l'individu et que les garanties apportées par le demandeur sont suffisantes. Malgré cela, l'article 40-15 de la loi[1276] prend soin de préciser que les personnes qui mettent en œuvre les traitements finalement autorisés, qui ont accès aux données traitées ou aux résultats, sont tenues au secret professionnel. De plus, les traitements ne peuvent pas servir à rechercher ou à identifier des personnes. Enfin, la publication des résultats des traitements autorisés par la CNIL ne peut avoir lieu que s'il est strictement impossible d'identifier les personnes dont les données ont été recueillies. Ces précisions commencent progressivement à répondre directement à quelques craintes d'atteinte au droit au respect de la vie privée dont des acteurs privés à but lucratif pourraient être à l'origine : il pourrait par exemple s'agir de l'identification d'individus atteints de pathologies particulières à des fins de prospection commerciale par un laboratoire pharmaceutique.

Avec cette nouvelle procédure d'accès à des données de santé en vue d'un traitement, le législateur entend alors anticiper la parution de l'arrêté organisant le fonctionnement du SNIIRAM. Les précautions nécessaires à la protection de la vie privée sont prises avec l'examen préalable de la demande par la CNIL : celle-ci est notamment amenée à vérifier que la demande reçue est conforme soit aux missions, soit à l'objet social du demandeur ; que le recours aux données personnelles demandées est nécessaire et que le traitement envisagé est pertinent.

460. Presque tous les éléments permettant de demander un accès aux informations contenues dans les bases de données administratives en santé de l'assurance maladie étaient donc réunis dès l'année 1999. Il ne manquait plus que la parution du premier arrêté relatif à la mise en œuvre

[1275] Numéro d'inscription au répertoire national d'identification des personnes physiques.

[1276] Art. 40-12 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 99-641 du 27 juillet 1999, *op. cit.*

du SNIIRAM qui a finalement été dévoilé trois années plus tard, le 11 avril 2002[1277]. Ce texte dresse la liste des finalités des traitements mis en œuvre dans le cadre du SNIIRAM, des données nécessaires à cela, mais surtout des destinataires des données, aussi appelés bénéficiaires d'un accès permanent[1278]. Plus intéressant encore, le dernier alinéa de l'article 4 de l'arrêté vise tous les demandeurs potentiels qui ne figurent pas sur la liste des bénéficiaires de l'accès permanent[1279] : assez avares en détails, les quelques lignes indiquent que toute personne peut demander à accéder aux « *données individuelles relatives aux bénéficiaires* » en déposant un dossier dans le cadre de la procédure prévue par le chapitre V ter de la loi relative à l'informatique et aux libertés, décrite précédemment[1280]. En théorie, les acteurs privés à but lucratif sont donc parfaitement admis à demander et obtenir, si leur dossier est validé par la CNIL, l'accès aux données de santé du SNIIRAM. Insistons sur l'aspect théorique de ce raisonnement car, comme le signale C. BABUSIAUX dans son rapport[1281] rendu en 2003, les organismes d'assurance maladie complémentaire qui devaient certainement convoiter l'obtention de données de santé issues du SNIIRAM, n'avaient toujours pas déposé de demande auprès de la Commission, alors même que « *cet accès* [était] *juridiquement possible* ».

461. Malheureusement pour les organismes privés à but lucratif, cette première version du système d'accès aux données de santé qui leur laisse une liberté certaine a rapidement été transformée en interdiction complète d'accès. Nous reviendrons dans le prochain titre[1282] sur les raisons de ce revirement de conception.

Paragraphe 2 : L'interdiction expresse d'accéder aux données de santé

[1277] Arrêté du 11 avril 2002, *op. cit*.

[1278] Sur l'accès permanent, v. Partie I.

[1279] Arrêté du 11 avril 2002, *op. cit*., art. 4, dernier alinéa : « *Toute autre demande d'accès à des données individuelles relatives aux bénéficiaires devra faire l'objet d'une demande d'autorisation auprès de la CNIL dans les conditions prévues aux articles 40-11 à 40-15 de la loi du 6 janvier 1978 susvisée* ».

[1280] *Supra* n° 459.

[1281] BABUSIAUX C., BREAS L., ESLOUS L., THOUVENIN D., *Rapport, L'accès des assureurs complémentaires aux données de santé des feuilles de soins électroniques, op. cit.*, p. 19.

[1282] *Infra* n° 513 à 522.

462. Trois ans après le premier arrêté[1283] relatif au SNIIRAM, un second arrêté[1284] est paru. Cet arrêté a drastiquement durci les mesures de demande d'accès aux données de santé à des fins de recherche. Alors que le texte initial ouvrait l'opportunité d'accéder aux données de santé à tous les acteurs non bénéficiaires d'un accès permanent, l'arrêté publié en 2005 est totalement inverse et opère deux nouvelles distinctions.

La première est la désignation directe des types d'acteurs qui peuvent être admis à déposer une demande de traitement pour les informations contenues dans le SNIIRAM. Sont regroupés « *tout autre organisme de recherche, des universités, écoles ou autres structures d'enseignement liés à la recherche que ceux* [mentionnés par le paragraphe 5 de l'article 4 du décret] ». Cela exclut d'emblée toutes les entreprises dont l'objet social n'entre pas dans le cadre de l'une des activités citées par l'arrêté. En revanche certaines entreprises, parmi lesquelles nous pouvons citer de manière non exhaustive les laboratoires de recherche privés ou les écoles et universités privées, sont encore légitimes à demander l'accès aux données de santé du SNIIRAM en vue d'un traitement.

Cependant, la deuxième distinction assène un coup d'arrêt ferme aux velléités que nous venons d'exprimer. Il est précisé que « *aucun organisme de recherche, université, école ou autre structure d'enseignement lié à la recherche poursuivant un but lucratif ne peut accéder aux informations* [nécessaires à l'établissement du SNIIRAM] ». Par ces mots, l'arrêté du 20 juin 2005 exclut, sans exception aucune, tous les organismes privés à but lucratif, quels qu'ils soient, de la procédure d'accès sélectif aux données de santé. Les nouvelles mesures sont donc très restrictives et rétrécissent considérablement le champ des possibles entrouvert par l'arrêté initial du 11 avril 2002. Une question légitime peut se poser au regard de cette nouvelle conception de l'accès sélectif aux données de santé, complètement interdit aux acteurs privés à but lucratif : quel est l'événement a pu motiver un tel bouleversement ? La réponse se trouve du côté de la directive communautaire de 1995[1285].

463. Effectivement, la directive 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 des

[1283] Arrêté du 11 avril 2002, *op. cit*.

[1284] Arrêté du 20 juin 2005, *op. cit*.

[1285] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

données a été transposée par la loi du 6 août 2004[1286]. Cette transposition a eu deux impacts concrets sur l'organisation du SNIIRAM et des accès potentiels aux données qu'il contient. L'impact principal de la transposition est l'intégration, à l'article 8 de la loi relative à l'informatique et aux libertés[1287], de la notion de données « *relatives à la santé* » comme étant une donnée nécessitant une protection particulière. C'est la première fois[1288] que la donnée de santé est reconnue comme une donnée sensible : cette reconnaissance s'accompagne d'une conséquence de taille, l'interdiction de traitement devient le principe, reléguant l'autorisation de traitement au rang d'exception. Parmi les exceptions à la stricte interdiction de traitement figurent les recherches dans le domaine de la santé menées dans le cadre du chapitre V bis[1289] de la loi relative à l'informatique et aux libertés, devenu chapitre IX à l'issue de la transposition de la directive de 1995[1290]. Par cette transposition, le législateur a donc mesuré l'importance que revêt la protection des données de santé dont le traitement peut impacter le droit au respect de la vie privée des individus. Il nous semble qu'un véritable lien existe entre cette prise de conscience par législateur et la réécriture de l'arrêté relatif à la mise en œuvre du SNIIRAM afin d'exclure de l'accès sélectif les acteurs privés à but lucratif. Cette réécriture constitue le deuxième impact de la transposition de la directive de 1995[1291] qui se cristallise dans la publication de l'arrêté du 20 juin 2005[1292] qui exclut totalement les acteurs privés à but lucratif de l'accès aux données de santé sans que le raisonnement suivi pour expliquer cette décision ne soit clairement exposé.

464. Il est vrai que la directive de 1995[1293] laisse aux Etats membres le soin de définir les dérogations à l'interdiction de traitement de données sensibles, dont font partie les données de santé à caractère personnel, « *lorsqu'un motif d'intérêt public important le justifie dans des domaines tels que la santé publique et la protection sociale* […] *et tels que la recherche scientifique et les statistiques publiques ; qu'il leur incombe, toutefois, de prévoir les garanties*

[1286] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[1287] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1288] JOB J.-M., « La loi "Informatique et libertés" et les données de santé », *Revue Lamy droit de l'immatériel*, 01/01/2008, n° 34, p. 86-94.

[1289] V. *supra* n° 457.

[1290] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[1291] *Ibid.*

[1292] Arrêté du 20 juin 2005, *op. cit.*

[1293] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

appropriées et spécifiques aux fins de protéger les droits fondamentaux et la vie privée des personnes » [1294]. Ainsi, les dérogations au principe d'interdiction de traitement prévues par l'article 8 de la directive, transposé à l'article 8 de la loi relative à l'informatique et aux libertés[1295], auraient pu être augmentées par l'Etat français au profit des organismes privé à but lucratif à la condition que les garanties appropriées et que le motif d'intérêt public aient été suffisamment importants[1296]. Une exception supplémentaire a bien été intégrée en droit français avec la loi du 6 août 2004[1297], mais elle ne concerne que les traitements statistiques réalisés par l'INSEE ou l'un des services statistiques ministériels tels que la DARES ou la DREES[1298].

465. Le fait que le législateur n'ait pas souhaité proposer un accès aux acteurs privés à but lucratif peut être interprété de différentes manières. Nous pouvons d'abord discerner dans cette décision un aveu important de la part des autorités françaises : la directive précise qu'une exception au principe d'interdiction de traitement des données de santé peut être prévue pour un « *motif d'intérêt public important* ». Dès lors nous pouvons supposer que les rédacteurs de la loi du 6 août 2004[1299] et ceux de l'arrêté du 20 juin 2005[1300] considéraient que la réalisation de traitements à l'aide des données du SNIIRAM ne comportait pas un intérêt public suffisamment important pour justifier que des acteurs privés à but lucratif puissent participer à cette mission. Nous pouvons ensuite poursuivre un raisonnement différent, pas forcément exclusif de la première hypothèse, selon lequel les acteurs privés à but lucratif n'ont pas été invités à accéder aux données de santé du SNIIRAM, même de façon limitée et contrôlée, en raison de l'incapacité des autorités à apporter les « *garanties appropriées* » permettant d'assurer le droit au respect de la vie privée des individus. Sans cette assurance que le traitement des données de santé ne puisse pas aboutir à une violation de ce droit, il aurait été décidé de fermer totalement l'accès aux données du SNIIRAM pour les acteurs privés à but lucratif.

[1294] *Ibid.*, considérant 34.

[1295] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1296] *Ibid.* art. 8, paragraphe 4 : « *sous réserve de garanties appropriées, les Etats membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle* ».

[1297] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[1298] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, art. 8, paragraphe II, 7°, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit*.

[1299] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[1300] Arrêté du 20 juin 2005, *op. cit*.

Ce second raisonnement comprend malgré tout une limite intéressante car l'arrêté du 20 juin 2005[1301] permet à certains acteurs de bénéficier de l'accès sélectif[1302] aux données sous condition de suivre une procédure ayant pour objet de garantir le droit au respect de la vie privée : cela signifie que, pour les bénéficiaires de cet accès sélectif, les garanties appropriées ont pu être définies. Dans le même temps, il découle de l'arrêté que ces garanties, qui semblent être suffisantes pour les acteurs listés limitativement, ne sont pas assez solides pour permettre aux acteurs privés à but lucratif de devenir, eux-aussi, bénéficiaires de l'accès sélectif. Ce constat peut être considéré comme étant une marque de méfiance de l'Etat vis-à-vis de la capacité des acteurs privés à but lucratif à s'inscrire dans une démarche d'intérêt général en mettant leurs moyens de recherche et d'analyse des données au service de l'intérêt public. Ces acteurs seraient, en d'autres termes, trop attirés par leur intérêt de créer de la richesse pour résister à la mise en œuvre d'une entreprise d'exploitation des données de santé obtenues, irrespectueuse de la vie privée des individus : cela pourrait par exemple être un système de réidentification systématique des personnes[1303]. Les motivations sur lesquelles reposent l'exclusion des acteurs privés à but lucratif de l'accès aux données de santé sont clairement fondées sur la crainte de ne pas pouvoir assurer le droit au respect à la vie privée, toutefois, il conviendra d'explorer ultérieurement[1304] les critiques qui pourraient être formulées à l'égard de la décision de ne pas bâtir dès 2005 un régime spécifique et encadré pour l'accès aux données de santé du SNIIRAM au bénéfice des organismes privés à but lucratif.

466. C'est donc à partir de l'année 2005 que l'accès aux données de santé du SNIIRAM a été strictement fermé aux acteurs privés à but lucratif. Cette interdiction d'accès a, malgré sa sévérité, été accompagnée de quelques possibilités de mettre en œuvre, directement ou indirectement, des traitements, sous une surveillance accrue.

[1301] *Ibid.*

[1302] Sur l'analyse de l'accès sélectif aux données de santé, v. Partie II.

[1303] Ce type d'opération a été considéré comme « *très peu probable* » par P.-L. BRAS dans son rapport remis en 2013, v. *Rapport sur la gouvernance et l'utilisation des données de santé*, septembre 2013, p. 28.

[1304] *Infra* n° 512 à 535.

SECTION 2 : LES RARES EXCEPTIONS À L'INTERDICTION D'ACCÉDER AUX DONNÉES DE SANTÉ

467. La fermeture de l'accès aux données de santé pour les acteurs privés à but lucratif a laissé subsister quelques rares opportunités de bénéficier de la richesse de ces données. En effet, une méthode non prévue par les textes a émergé dans la pratique, les organismes privés à but lucratif privés d'accès aux données de santé issues du SNIIRAM ont fait appel à des tiers (§1). Par ailleurs, le contenu de l'arrêté fixant la liste des bénéficiaires de l'accès permanent a évolué pour inclure des catégories précises d'acteurs privés pouvant avoir un but lucratif (§2).

Paragraphe 1 : La possibilité de l'accès sélectif par procuration

468. La lecture de l'arrêté relatif à la mise en œuvre du SNIIRAM du 20 juin 2005[1305] est claire quant à l'interdiction des acteurs à but lucratif de bénéficier de l'accès sélectif[1306]. Toutefois, s'il est impossible, pour ces organismes, d'obtenir une autorisation de traitement de données issues du SNIIRAM par le biais de la procédure d'accès sélectif, rien ne semble leur bloquer une voie annexe : celle du recours à un organisme tiers, tel un laboratoire public de recherche, faisant partie des acteurs autorisés à déposer une demande auprès de l'IDS. Cette opportunité n'est pas écrite *stricto sensu* dans l'arrêté mais peut être devinée entre les quelques lignes du dernier alinéa de l'article 4 de l'arrêté qui précise que le « *traitement des informations énumérées à l'article 3 demandé par tout autre organisme de recherche, des universités, écoles ou autres structures d'enseignement liés à la recherche que ceux mentionnés au paragraphe précédent est soumis à l'approbation du conseil d'administration de l'Institut des données de santé. Aucun organisme de recherche, université, école ou autre structure d'enseignement lié à la recherche poursuivant un but lucratif ne peut accéder aux informations de l'article 3* »[1307]. Autrement dit, les organismes privés à but lucratif ne peuvent pas obtenir directement des données du SNIIRAM pour réaliser un traitement, mais ils peuvent mandater un organisme public ou privé à but non lucratif bénéficiaire de l'accès sélectif pour obtenir des données de santé et réaliser le traitement souhaité. Permettre à un acteur privé à but lucratif de commanditer une recherche réutilisant des données de santé provenant du SNIIRAM semble conforme à l'esprit de l'arrêté pris par le directeur de la sécurité sociale. En effet, cela ne met pas

[1305] Arrêté du 20 juin 2005, *op. cit.*

[1306] *Supra* n° 462.

[1307] Arrêté du 20 juin 2005, *op. cit.*, art. 4, dernier alinéa.

directement entre les mains de l'organisme ostracisé les données sensibles, ce qui limite, en théorie, le risque que celles-ci soient réutilisées de manière à enfreindre le droit au respect de la vie privée. De plus, l'organisme tiers qui réalise obtient les données et réalise le traitement reste soumis à la procédure stricte de l'accès sélectif.

469. Lors de la recherche de plus amples informations concernant ce moyen, pour les organismes privés à but lucratif, de faire réaliser des études réutilisant des données de santé du SNIIRAM, il est apparu que très peu d'auteurs se sont véritablement intéressés à la mise en œuvre de cet accès sélectif par procuration. En vérité, nous ne trouvons mention de cette faculté qu'à travers de rares documents comme le rapport de P.-L. BRAS de 2013[1308], le rapport de la Cour des comptes rendu en mars 2016[1309], ou les rapports au Parlement de l'Institut des données de santé[1310]. Nous pouvons déplorer que ces quelques références au recours à un tiers restent distantes du cœur du sujet et ne comportent pas d'analyse profonde des problématiques qu'une telle contrainte peut faire surgir[1311]. Toutefois, certaines tournures de phrases et schémas de rédaction nous donnent des indications sur la perception que les auteurs ont de ce moyen, non prévu par les textes, de traiter des données de santé issues du SNIIRAM.

Ainsi, le rapport de l'Institut des données de santé indique que pour réaliser des études sur les données de santé, les organismes privés à but lucratif ont recours à « *des stratégies de contournement peu propices à la transparence dans la mesure où* […] [ils] *peuvent faire appel à un organisme autorisé à utiliser les données du SNIIRAM pour réaliser leurs études* »[1312]. L'Institut, qui a une place centrale dans le processus d'accès sélectif[1313], paraît considérer que le recours à un tiers par les acteurs privés à but lucratif est un acte à la portée négative. L'usage du mot « *contournement* » apporte une connotation péjorative qui nous porte à croire que l'IDS regrette qu'une telle mesure puisse être mise en œuvre alors qu'elle n'est, en soi, pas prévue par les textes. Effectivement, la procédure d'accès sélectif a été mise en place pour connaître

[1308] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, septembre 2013, 128 p.

[1309] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *Communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale*, 03/2016, 167 p.

[1310] V. notamment Institut des données de santé, « Enjeux et étapes », *Rapport au Parlement*, 2010, 66 p.

[1311] V. notre étude des difficultés pratiques liées à l'accès sélectif par procuration auquel les acteurs privés à but lucratif ont pu avoir recours, *infra* n° 538.

[1312] Institut des données de santé, « Enjeux et étapes », *Rapport au Parlement*, *op. cit.*, p. 18.

[1313] *Supra* n° 258.

l'identité des acteurs qui demandent et obtiennent des données du SNIIRAM, pour les contrôler, pour tisser des liens de confiance avec eux, mais aussi pour savoir de quelles données ils ont besoin et pour quelles finalités. Or, le fait que les organismes privés à but lucratif missionnent un tiers pour demander l'accès sélectif, l'obtenir et réaliser le traitement, fausse, dans une certaine mesure, l'objectif initial d'interaction entre l'IDS et les acteurs souhaitant traiter des données de santé. Nous verrons prochainement[1314] que cette prise de conscience a conduit l'Institut à modifier sa politique en matière d'examen des dossiers déposés par les acteurs privés à but lucratif.

Quelques années plus tard, P.-L. BRAS fait, dans son rapport, une référence rapide à ce qui s'apparente à de la sous-traitance d'accès aux données du SNIIRAM. Il précise que « *l'arrêté SNIIRAM exclut d'emblée les demandeurs privés à but lucratif* […] *ce qui n'empêche pas que les demandes commanditées par un laboratoire pharmaceutique mais présentées par un laboratoire de recherche public soient recevables* »[1315]. L'auteur du rapport ne formule aucun commentaire supplémentaire à propos de cette pratique qui, sans être contraire au principe d'interdiction d'accès prévu par l'arrêté du 20 juin 2005, permet aux organismes privés à but lucratif de faire réaliser les traitements que les dispositions légales et réglementaires leur interdisent de mettre en œuvre.

La Cour des comptes adopte peu ou prou le même raisonnement que l'IDS dans son rapport dévoilé en 2016. Elle y précise que malgré l'interdiction d'accès aux données du SNIIRAM pour les organismes privés à but lucratif, des « *contournements sont possibles par l'intermédiation des équipes de recherche publique, répondant à une commande privée, par exemple dans le secteur du médicament* »[1316]. Par cette phrase, la pratique de l'accès sélectif par procuration est perçue non pas comme un acte illégal, mais comme un acte qui sort volontairement de la procédure visée par arrêté et par la loi. Sans vraiment approuver ou critiquer cette possibilité, la Cour des comptes, en parlant de « *contournements* », pointe du doigt le vide juridique qui la rend possible.

[1314] *Infra* n° 486 et 487.

[1315] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 36.

[1316] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 54.

Il ressort de ces différentes références à la sous-traitance de l'accès sélectif par les organismes privés à but lucratif que la situation, bien qu'exorbitante de droit commun, n'a pas suscité de réels commentaires ou discussions collectives. Il s'agit d'un état de fait, constaté par les auteurs successifs, qui a d'abord trouvé une véritable proposition d'évolution dans la pratique[1317].

470. Outre cette faculté, pour les organismes privés à but lucratif, de commanditer la réalisation d'un travail de recherche nécessitant des données issues du SNIIRAM auprès d'un organisme habilité par arrêté, il ne faut pas oublier que la possibilité de traiter des données de santé ne provenant pas de cette base de données est déjà offerte à tous ces acteurs. A titre d'exemple, ni le chapitre IX, ni le chapitre X de la loi relative à l'informatique et aux libertés[1318] modifiée par la loi du 6 août 2004[1319] ne comportent d'interdiction empêchant les acteurs privés à but lucratif de déposer un dossier afin d'effectuer des recherches dans le domaine de la santé : les procédures d'examen par le CCTIRS et par la CNIL, déjà décryptées dans notre étude[1320], sont globales et ne proposent pas de dispositions particulières propres à la nature de l'acteur qui dépose une demande de traitement.

471. Il est aussi étonnant, comme l'a remarqué la Cour des comptes dans son rapport[1321], que les acteurs privés à but lucratif puissent accéder, selon la procédure ordinaire d'autorisation préalable par la CNIL, aux données du PMSI qui contient toutes les données de santé liées à l'activité hospitalière en France. Ces données sont potentiellement aussi sensibles que les données issues du SNIIRAM, pourtant l'accès à ces données et leur étude peut parfaitement être sollicité par des organismes privés à but lucratif comme le rappelait l'IDS dans son rapport de 2015[1322]. Nous pouvons aussi souligner le fait que si l'accès aux données agrégées du SNIIRAM est interdit aux organismes privés à but lucratif, l'accès aux données agrégées du PMSI est, lui, autorisé. Celles-ci sont directement accessibles sur un site internet[1323] ouvert à tous et regroupant des informations statistiques non identifiantes et ne comportant pas de risque

[1317] *Infra* n° 485 à 488.

[1318] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1319] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[1320] *Supra* n° 302 à 310.

[1321] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit*., p. 54.

[1322] Institut des données de santé, « Ouverture, qualité, partage : des avancées », *Rapport au Parlement*, 2015, p. 33.

[1323] La version actuellement en ligne est www.scansante.fr.

de réidentification. La question de la sur-protection des données du SNIIRAM, dans le système antérieur à la réforme du 26 janvier 2016[1324], mérite d'être posée et nous nous attacherons à apporter des éléments de réponse dans le prochain titre[1325].

472. Une autre subtilité réside au troisième paragraphe de l'article 8 de la loi relative à l'informatique et aux libertés issu de la réforme de l'année 2016. Ce paragraphe indiquait que « *si les données à caractère personnel* [relatives à la santé] *sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements* […] *les dispositions des chapitres IX et X ne sont pas applicables* »[1326]. Cette exception a été modifiée courant 2018 pour être plus largement entendue : « *N'entrent pas dans le champ de l'interdiction* […] *les données à caractère personnel* […] *qui sont appelées à faire l'objet, à bref délai, d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés* »[1327]. Cela signifie en substance que si des données sensibles sont anonymisées selon un moyen approuvé par la CNIL, un organisme privé à but lucratif peut être autorisé par cette dernière à réaliser un traitement selon une procédure moins contraignante que celle qui a trait aux recherches dans le domaine de la santé. La possibilité du recours, par les acteurs privés à but lucratif, à cette exception prévue par la loi a d'ailleurs fait l'objet d'un contentieux qu'il conviendra d'examiner en détail ultérieurement[1328]. Signalons que cette faculté de traiter des données de santé issues des bases de données médico-administratives si celles-ci font l'objet d'un processus d'anonymisation à bref délai a été supprimé par l'ordonnance du 12 décembre 2018[1329]. En effet, cette exception se révèle finalement contraire au Règlement général relatif à la protection des données[1330].

[1324] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1325] *Infra* n° 518 à 522.

[1326] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, art. 8, III, modifiée par la loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1327] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, art. 8, III, modifiée par la loi n° 2018-493 du 20 juin 2018, *op. cit*.

[1328] *Infra* n° 490 à 492.

[1329] Ordonnance n° 2018-1125 du 12 décembre 2018 *prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel*, JORF n° 0288 du 13/12/2018.

[1330] Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*.

473. Pour bénéficier *a minima* des connaissances découlant du traitement des données de santé issues du SNIIRAM, les acteurs privés à but lucratif ont donc dû faire appel à des acteurs autorisés par arrêté. Cette démarche, non prévue par les textes semble avoir été acceptée comme un moindre mal, à défaut d'être classique. Mais elle démontre surtout que le secteur privé à but lucratif n'est pas de nature à accepter cette interdiction pure et simple alors que, dans le même temps, des opportunités de traitement lui sont offertes sur des données provenant d'autres bases comme le PMSI. Une toute petite faille a alors vu le jour en 2011 avec l'apparition d'une nouvelle catégorie de bénéficiaires de l'accès permanent dans l'arrêté relatif à la mise en œuvre du SNIIRAM.

Paragraphe 2 : L'ouverture prudente à de rares acteurs privés

474. Nous savons que de nombreux arrêtés relatifs à la mise en œuvre du SNIIRAM ont été pris entre 2005 et 2016[1331]. Si celui de 2005 a bien exclu tous les organismes privés à but lucratif d'un quelconque accès aux données, une évolution a tout de même été constatée au profit d'une sous-catégorie d'acteurs qui a été directement autorisée par arrêté à obtenir et traiter certaines données. Il s'agit d'une part des membres de l'UNOCAM (Union nationale des organismes d'assurance maladie complémentaire) qui sont la FNMF (Fédération nationale de la mutualité française), la FFA (Fédération française de l'assurance), le CTIP (Centre technique des institutions de prévoyance), l'instance de gestion du régime local d'assurance maladie complémentaire obligatoire d'Alsace et de la Moselle, ainsi que la FNIM (Fédération nationale indépendante des mutuelles) ; d'autre part des organismes complémentaires membres des fédérations constitutives de l'UNOCAM qui sont tous les organismes complémentaires d'assurance maladie que sont les mutuelles, les entreprises d'assurances et les institutions de prévoyance.

C'est l'arrêté daté du 1er décembre 2011[1332] relatif à la mise en œuvre du SNIIRAM qui est venu ajouter cette opportunité. Les membres de l'UNOCAM ont accès à toutes les informations disponibles uniquement sous la forme de statistiques agrégées, ou bien sous forme individualisée concernant l'échantillon généraliste des bénéficiaires (EGB), à l'exclusion des

[1331] *Supra* n° 104 à 113.

[1332] Arrêté du 1er décembre 2011 *relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie*, JORF n° 0019, 22/01/2012.

données identifiant les professionnels de santé. De leur côté, les organismes complémentaires membres des fédérations constitutives de l'UNOCAM sont bénéficiaires d'un accès à toutes les données sous forme de statistiques agrégées, à l'exclusion de l'EGB et de toute donnée d'identification des bénéficiaires de l'assurance maladie et des professionnels de santé.

475. Une première observation importante peut être livrée : si tous ces acteurs sont bel et bien des personnes morales de droit privé, un seul d'entre eux a véritablement un but lucratif. En premier lieu, toutes les fédérations membres de l'UNOCAM n'ont pas un but lucratif, leur objectif est de représenter et défendre les intérêts de leurs adhérents. Ensuite, si nous nous intéressons à la nature des différents types d'organismes assureurs qui constituent ces fédérations, nous comprenons rapidement qu'ils sont de trois sortes : les mutuelles, les institutions de prévoyance, et les entreprises d'assurances. Les mutuelles sont des « *personnes morales de droit privé à but non lucratif* », comme le précise le code de la mutualité[1333]. Nous pouvons signaler qu'il existe aussi les mutuelles d'assurance qui restent des « *personnes morales de droit privé ayant un objet non commercial* » tout en étant régies par le code des assurances[1334]. Les institutions de prévoyance sont, elles aussi, des « *personnes morales de droit privé ayant un but non lucratif* » d'après le code de la sécurité sociale[1335]. Mais, à l'opposé, se trouvent les entreprises d'assurance qui sont des sociétés anonymes[1336] et qui ont, par conséquent, un but lucratif. Ce sont finalement les entreprises d'assurances qui sont les plus favorablement touchées par l'arrêté de la fin de l'année 2011 car elles passent du statut d'acteur totalement exclu à celui de bénéficiaire d'un accès permanent. La création de ce nouvel accès permanent a été considéré comme « *un signal fort de la part de l'Assurance Maladie Obligatoire* »[1337] permettant de dynamiser le partage de données avec l'UNOCAM et les fédérations d'assureurs en complémentaire santé. Cette nouvelle opportunité est toutefois soumise à certaines conditions.

476. Le bénéfice de l'accès permanent aux données du SNIIRAM pour les membres de l'UNOCAM et les adhérents aux fédérations constitutives de l'UNOCAM est subordonné à la

[1333] Code de la mutualité, art. L. 111-1, I, al. 1.

[1334] Code des assurances, art. L. 322-26-1, al. 1.

[1335] Code de la sécurité sociale, art. L. 931-1, al. 1.

[1336] Code de la sécurité sociale, Partie législative, Livre III, Titre II, Chapitre II, Section II.

[1337] Institut des données de santé, « Enjeux et étapes », *op. cit*., p. 28.

signature d'une charte d'engagements pour la mise en commun de données de remboursement agrégées ou individuelles anonymisées[1338]. Seuls les organismes signataires peuvent bénéficier de l'accès aux données décrites par arrêté. Cette charte acte l'ouverture des données telles qu'elles sont visées par l'arrêté de 2011 aux membres de l'UNOCAM et aux adhérents de ces membres. Plusieurs conditions sont fixées par cette charte : ainsi, les membres de l'UNOCAM ne peuvent accéder aux données de l'EGB du SNIIRAM que dans la mesure où ils contribuent aux données de remboursement sur le périmètre de l'EGB. D'autre part, l'accès aux données agrégées (aussi appelées datamarts) est subordonné au fait que les organismes d'assurance maladie complémentaire soient contributeurs de données de remboursement dans le cadre du projet appelé MONACO[1339]. Ce projet a été initié par l'IRDES et l'IDS en juillet 2008 afin de tester la faisabilité d'un appariement entre les données de l'UNOCAM et celles de l'assurance maladie obligatoire. La CNIL a ensuite donné son autorisation le 15 juillet 2010 pour une mise en œuvre à partir du milieu de l'année 2011. Si nous envisageons la situation du point de vue d'une entreprise d'assurance à cette période, il lui suffisait de mettre en place la transmission de ses propres données pour pouvoir accéder aux données des datamarts du SNIIRAM. C'est, en quelque sorte, un cercle vertueux de partage de données de santé traitées pour ne pas être réidentifiantes : le projet MONACO qui a servi de base à l'accès des organismes de complémentaire santé à certaines données du SNIIRAM est fondé sur une réciprocité des contributions, profitable à tous les acteurs.

477. La charte signée par l'UNOCAM, ses membres, et leurs adhérents, comprend trois engagements spécifiques qui doivent être respectés. A titre liminaire, nous pouvons souligner que la présence des entreprises d'assurances, qui sont des acteurs privés à but lucratif, parmi les adhérents des membres de l'UNOCAM, a très probablement conduit à renforcer le contenu de la charte afin de prévenir tout risque d'atteinte au respect de la vie privée. De ce fait, les institutions de prévoyance et les mutuelles sont soumises aux mêmes critères stricts malgré leur caractère privé à but non lucratif.

[1338] VAN ROEKEGHEM F., GIN F., LIGER D., COHEN-SOLAL J.-M., LEQUOY J.-F., FAURE J.-L., Charte d'engagements entre l'Assurance Maladie Obligatoire et les assureurs maladie complémentaires pour le partage et la mise en commun des données de remboursement agrégées ou individuelles anonymisées issues de leurs systèmes d'information, 07/10/2010, 4 p.

[1339] MONACO signifie Méthodes, Outils, Normes, pour la mise en commun de données entre les Assureurs maladie Complémentaires et Obligatoires.

Le premier engagement concerne la protection de la vie privée et exige que les signataires utilisent les données du SNIIRAM rendues accessibles « *à des fins de gestion du risque ou pour répondre à des préoccupations de santé publique* »[1340]. En complément, les membres de l'UNOCAM, qui ont aussi accès à l'EGB, ne sont autorisés à utiliser les données qui en sont issues que dans un but de statistiques, d'analyses et d'études portant sur la gestion du risque maladie ou pour répondre à des préoccupations de santé publique. Pour vérifier que cette limite de traitement n'est pas outrepassée, les membres de l'UNOCAM doivent aussi garantir que l'utilisation qu'ils font des données dudit EGB est auditable : c'est-à-dire qu'une documentation suffisante doit être enregistrée et stockée pour permettre de vérifier que le traitement des données issues de l'EGB ne va pas au-delà des autorisations permises par la charte.

Les deuxième et troisième engagements relèvent du même esprit. Est d'abord exigé, d'une part, le partage des données des organismes d'assurance maladie complémentaire contributeurs du projet MONACO avec l'assurance maladie obligatoire ; d'autre part, la mise en commun des données de remboursement anonymisées individuelles collectées par les membres de l'UNOCAM pour constituer l'échantillon commun correspondant à l'EGB. Enfin, les membres de l'UNOCAM doivent aussi mettre à disposition toutes les données de remboursement anonymisées issues de leur système d'information. La notion de partage maîtrisé et sécurisé entre assurance maladie obligatoire et assurance maladie complémentaire prend ici tout son sens.

En parallèle de ces engagements tous les acteurs signataires de la charte doivent respecter les conventions d'utilisation et de conditions de service relatives aux droits et devoirs des producteurs et utilisateurs du SNIIRAM, ainsi que la charte de déontologie[1341] de l'Institut des données de santé. Nous voyons bien que l'accès des organismes complémentaires d'assurance maladie, dont font partie certains organismes privés à but lucratif, n'a pas été ouvert sans précaution. L'autorisation est délivrée à la condition que des finalités bien précises soient respectées, telles que la gestion du risque ou la santé publique, et une obligation de réciprocité

[1340] VAN ROEKEGHEM F., GIN F., LIGER D., COHEN-SOLAL J.-M., LEQUOY J.-F., FAURE J.-L., Charte d'engagements entre l'Assurance Maladie Obligatoire et les assureurs maladie complémentaires pour le partage et la mise en commun des données de remboursement agrégées ou individuelles anonymisées issues de leurs systèmes d'information, 07/10/2010, p. 3.

[1341] Assemblée générale de l'Institut des données de santé, Charte de déontologie, 12/12/2008.

dans le partage des données de santé dans un cadre protecteur de la vie privée est posée. Cet encadrement théorique est prometteur et implique que le moindre écart de conduite de la part de l'un des bénéficiaires de cet accès permanent peut donner lieu à la suspension de l'accès.

478. Un élément essentiel doit être souligné pour comprendre l'importance de cet accès. Dès l'arrêté relatif au SNIIRAM de 2005[1342], l'accès sélectif n'a été ouvert qu'aux organismes de recherches, universités, écoles ou autres structures d'enseignement ne poursuivant pas un but lucratif[1343]. Autrement dit, une lecture stricte de l'arrêté laisse penser que tous les organismes à but non lucratif, qui ne rentrent pas dans l'une des catégories prévues par le texte, n'ont même pas l'opportunité de déposer un dossier pour bénéficier de l'accès sélectif. Dès lors, nous pouvons estimer que les membres de l'UNOCAM, les mutuelles et les institutions de prévoyances, qui sont des organismes privés à but non lucratif bénéficiaires de l'accès permanent aux données agrégées du SNIIRAM depuis l'arrêté de 2011, sont exclus d'office de l'accès sélectif au motif que leur objet principal n'est pas de faire de la recherche. Ils subiraient donc la même exclusion que les entreprises d'assurance, qui sont des organismes privés à but lucratif : cette interdiction qui dépasse alors le cadre du but lucratif ou non est discutable comme nous le verrons ultérieurement[1344]. En dehors de l'accès permanent qui leur est proposé, tous ces acteurs sont donc, par principe, privés de toute autre opportunité d'obtenir et traiter des données supplémentaires.

479. La fermeture du SNIIRAM à tous les acteurs privés à but lucratif, mais aussi à tous les acteurs à but non lucratif qui n'ont pas pour objet de faire de la recherche ou d'enseigner, est très stricte et supporte de rares exceptions. Les organismes participant au fonctionnement de l'accès sélectif se sont peu à peu mobilisés pour explorer les pistes d'évolution et permettre au législateur et au pouvoir réglementaire de réfléchir à une réforme réussissant à combiner la sécurité des données et la protection de la vie privée avec la plus grande ouverture possible aux données de santé.

[1342] Arrêté du 20 juin 2005, *op. cit.*

[1343] *Supra* n° 255.

[1344] *Infra* n° 514 à 517.

CONCLUSION DU CHAPITRE I

480. Les acteurs privés à but lucratif ont rapidement été mis à l'écart de l'accès aux données de santé. Le législateur ne les a pas immédiatement exclus du dispositif lors de la création du premier accès au SNIIRAM. En théorie, les acteurs privés à but lucratif, dont font partie les laboratoires pharmaceutiques ou les organismes assureurs, étaient admis à solliciter un accès aux données personnelles de santé afin d'effectuer un traitement. La CNIL devait nécessairement délivrer une autorisation préalable afin de garantir le respect des dispositions légales et réglementaires relatives. C'est finalement avec l'arrêté de 2005[1345] que le secteur privé à but lucratif a été intégralement radié de l'accès aux données de santé jusqu'à ce que la loi du 26 janvier 2016[1346] intervienne. L'interdiction totale d'accès semble être motivée par l'absence de garanties suffisantes pour la protection des données qui pourraient être rendues accessibles. C'est la crainte d'un détournement dans l'utilisation des données de santé par les acteurs privés à but lucratif qui émerge. Ces acteurs sont alors perçus, à tort diront certains, comme incapables de poursuivre une logique d'intérêt général : en suivant ce raisonnement, le cadre qui permet aux bénéficiaires de l'accès sélectif aux données de santé n'est donc pas adapté au comportement des acteurs privés à but lucratif. La méfiance du législateur à l'égard de ces acteurs qui ne seraient mus que par leur intérêt privé se traduit alors par une interdiction totale d'accès aux données des bases médico-administratives.

481. L'interdiction d'accès aux données de santé comporte toutefois une exception strictement identifiée. Ainsi, les organismes de complémentaire santé membres des fédérations constitutives de l'UNOCAM – dont font partie les entreprises d'assurance – ont pu, à partir de la fin de l'année 2011[1347], accéder en permanence aux données de santé sous forme de statistiques agrégées.

482. Au-delà de cette maigre exception, l'exclusion péremptoire du dispositif d'accès aux données de santé domine. Malgré tout, les acteurs privés à but lucratif ont su trouver quelques moyens de tirer parti de l'accès sélectif aux données de santé. La possibilité de faire déposer un dossier de demande d'accès par un tiers, lui-même soumis à la procédure d'accès sélectif, en

[1345] Arrêté du 20 juin 2005, *op. cit.*

[1346] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1347] Arrêté du 1er décembre 2011, *op. cit.*

vue de réaliser un traitement s'est montrée incontournable. Bien que peu de sources permettent de savoir si le secteur privé à but lucratif s'est accommodé de cette situation, cela représentait le seul moyen pour eux de faire réaliser un traitement à partir de données de santé à caractère personnel provenant du SNIIRAM. En sus de cette possibilité, il convient de rappeler que l'accès aux données du PMSI n'était, lui, pas soumis à une telle interdiction, ce que la Cour des comptes n'a pas manqué de souligner[1348]. Les acteurs privés à but lucratif pouvaient accéder aux informations en se conformant à la procédure d'autorisation préalable classique par la CNIL. Cette situation inconfortable s'est finalement transformée avec la réforme du 26 janvier 216[1349].

[1348] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit*.

[1349] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

CHAPITRE II
L'OUVERTURE ATTENDUE DE L'ACCÈS AUX DONNÉES DE SANTÉ DANS LE RESPECT DE LA VIE PRIVÉE

483. Entre 2005, année d'interdiction d'accès aux données de santé pour les organismes privés à but lucratif et 2016, année de la réforme créant le SNDS, les réflexions entourant l'élargissement de l'accès sélectif ont été nombreuses afin de savoir jusqu'à quel point l'évolution vers l'ouverture pouvait se faire sans basculer dans une atteinte à la vie privée (Section 1). L'aboutissement de ces réflexions a été la loi du 26 janvier 2016[1350] modifiée peu de temps après par la loi du 20 juin 2018[1351] adaptant les nouvelles dispositions nationales à celles du Règlement général relatif à la protection des données[1352] et qui a servi de base à l'ordonnance du 12 décembre 2018[1353] (Section 2).

SECTION 1 : LES ARGUMENTS EN FAVEUR DE L'ACCÈS AUX DONNÉES DE SANTÉ

484. L'interdiction totale d'accès aux données de santé pour les organismes privés à but lucratif n'est pas un mécanisme entièrement satisfaisant pour la doctrine mais aussi pour les acteurs intervenant dans le cadre du système, notamment l'IDS. Au cours des années de pratique d'un accès sélectif entièrement réservé aux acteurs publics et privés à but non lucratif, plusieurs réflexions et initiatives sur un élargissement de l'accès ont été menées (§1). Ces initiatives ont conduit à la production d'un contentieux rare mais instructif pour mieux comprendre l'élan de la réforme de 2016 (§2).

Paragraphe 1 : Les acteurs institutionnels favorables à l'ouverture au secteur privé à but lucratif

485. Les prises de position entourant l'accès des acteurs privés à but lucratif aux données de santé du SNIIRAM ont mis un certain temps à se développer. Rappelons le contexte de mise en

[1350] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1351] Loi n° 2018-493 du 20 juin 2018 *relative à la protection des données personnelles*, JORF n° 0141, 21/06/2018.

[1352] Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*.

[1353] Ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

œuvre des accès aux données : l'arrêté du 11 avril 2002[1354] a défini la première version des accès potentiels incluant les acteurs privés à but lucratif[1355]. Puis l'arrêté du 20 juin 2005[1356] a remodelé les dispositions en réservant l'accès sélectif aux acteurs publics et privés à but non lucratif. Dans le même temps, le texte a indiqué que toute demande devait passer par un nouvel interlocuteur : l'IDS. Or, nous le savons[1357], l'IDS n'a été mis en place qu'au cours de l'année 2007[1358] et il n'est véritablement entré en fonction que dans le courant de l'année 2008[1359] : ce n'est qu'à partir du moment où cet acteur clef a commencé à recevoir des demandes d'accès provenant de tous les demandeurs potentiels que des schémas d'évolution ont pu voir le jour. Mais l'IDS n'a pas reçu que des demandes émanant d'acteurs autorisés par arrêté à solliciter un accès : certaines demandes sont parfois provenues d'acteurs privés à but lucratif désireux de faire bouger les lignes de l'arrêté.

486. Dans son rapport daté de 2010[1360], l'IDS consacre un segment entier de son argumentation aux demandes d'accès déposées par les acteurs privés à but lucratif dans le cadre du chapitre X de la loi relative à l'informatique et aux libertés[1361] afin d'effectuer des recherches à l'aide de données de santé issues du SNIIRAM. Le document fait notamment état des demandes reçues entre 2009 et 2010 de la part de nombreux bureaux d'études, qui sont des organismes privés à but lucratif, souhaitant effectuer des recherches pour le compte de leurs clients. D'après le tableau recensant les dossiers traités par l'IDS[1362], nous comptons 5 demandes émanant de 3 bureaux d'études : une seule en 2009 et 4 en 2010. Les 3 bureaux d'études sont IMS Health, CEMKA-EVAL et STATESIA. Leurs demandes pouvaient porter sur l'élaboration « *d'un modèle de forfait à la pathologie à partir d'une étude internationale* », sur l'élaboration « *de données synthétiques sur les niveaux de prix de l'offre de soins* », ou encore sur les « *approches*

[1354] Arrêté du 11 avril 2002, *op. cit*.

[1355] *Supra* n° 460.

[1356] Arrêté du 20 juin 2005, *op. cit*.

[1357] *Supra* n° 165 et 214 à 215.

[1358] Arrêté du 30 avril 2007, *op. cit*.

[1359] L'IDS a reçu ses trois premières demandes d'accès en 2008 : l'une provenant des Hospices civils de Lyon et déposée le 14 janvier 2008, l'autre adressée par l'Unité 912 de l'INSERM le 25 juillet 2008, la dernière envoyée par l'Unité 780 de l'INSERM le 4 août 2008.

[1360] Institut des données de santé, « Enjeux et étapes », *op. cit.*, p. 18.

[1361] Chapitre X de la loi n° 78-17 du 6 janvier 1978, *op. cit*., modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1362] Institut des données de santé, « Workflow sur les demandes d'utilisation des données du SNIIRAM », 03/05/2017.

possibles de la prévalence de syndromes coronariens aigus (SCA) et [l'] *étude de la prise en charge de ces derniers* » En recevant ces demandes, les membres de l'IDS semblent avoir pris conscience que le mécanisme de l'accès sélectif tel qu'il existait alors pouvait avoir une nature contreproductive et conduire à « *des contradictions et des incohérences* ». En effet, recevoir ces demandes leur a permis de prendre conscience qu'exclure toute une catégorie d'acteurs en raison de leur objectif lucratif entre potentiellement en opposition avec le principe d'amélioration de la connaissance de la santé et des systèmes de soins inhérent au SNIIRAM[1363]. Ce n'est donc plus la finalité qui est prise en compte mais bien la nature du demandeur qui, par son activité, serait irrémédiablement amené à chercher à tirer profit des données de santé obtenues au mépris du principe de protection de la vie privée des individus. Ce raisonnement est suffisamment déséquilibré pour que les membres de l'IDS eux-mêmes reconnaissent qu'une évolution est envisageable. A ce titre, plusieurs actions ont été menées dès l'année 2010.

En premier lieu, le rapport précise que des « *représentants des industries de santé* », sans que nous ne sachions véritablement lesquelles, ont été auditionnés pour connaître leurs besoins dans le cadre de l'accès sélectif : il en ressort que c'est principalement pour réaliser des études pré et post autorisation de mise sur le marché (AMM) de produits pharmaceutiques à la demande des autorités sanitaires. L'accès aux données du SNIIRAM serait donc véritablement utile et apporterait une plus-value intéressante aux organismes privés à but lucratif pour leur mise en conformité avec leurs obligations légales.

La seconde initiative est hautement symbolique car elle a consisté à saisir pour avis à la fois le comité d'experts[1364] de l'IDS et surtout la CNIL pour une demande de conseil au sujet d'une

[1363] L'article 2 de l'arrêté relatif à la mise en œuvre du SNIIRAM pose les finalités des traitements réalisés à partir des données qu'il contient parmi lesquelles nous retrouvons l'amélioration de la qualité des soins, la contribution à la meilleure gestion de l'assurance maladie, la contribution à la meilleure gestion des politiques de santé, la transmission aux prestataires de soins les informations pertinentes relatives à leur activité, à leurs recettes et à leurs prescriptions.

[1364] La composition du comité d'experts de l'IDS, avant sa dissolution en vue de la création de l'INDS, est la suivante : Annick ALPEROVITCH (directrice de recherche à l'INSERM, membre du Comité Consultatif National d'Ethique), Pascal AUQUIER (professeur à la faculté de Médecine de Marseille directeur de l'EA2279, Responsable du service de santé publique et de l'information médicale, CHU de Marseille), Brigitte DORMONT (professeur à l'université Paris Dauphine, responsable de la Chaire Santé de la Fondation du Risque), Martial FRAYSSE (Président du conseil régional des pharmaciens d'Ile de France, membre du Conseil National de l'Ordre des Pharmaciens), Jean-Pierre LE GLÉAU (inspecteur général de l'INSEE, chef du département de la coordination statistique), Claude LE PEN (professeur, université Paris-Dauphine), Jacques LUCAS (Vice-Président du Conseil National de l'Ordre des Médecins), René PADIEU (inspecteur général honoraire de l'INSEE, président de la commission de déontologie de la société française de statistiques), Gérard DE POUVOURVILLE (professeur titulaire de la chaire Economie et Gestion de la Santé à l'ESSEC), Catherine QUANTIN (professeur à la faculté

requête déposée par la société IMS Health le 20 novembre 2009[1365]. La CNIL, dans sa réponse du 8 juin 2010[1366] à la demande de l'IDS, prend une position tout à fait intéressante. Elle note l'analyse du dossier par le comité d'experts qui considère que « *la finalité de l'étude est en rapport avec l'amélioration de la connaissance de la santé et des systèmes de soins* » et que « *l'accès aux données du SNIIRAM à des fins d'études et de recherche devrait être élargi aux organismes quel que soit leur statut* ». Le comité observe également que l'accès aux données agrégées du SNIIRAM et à l'EGB « *devrait être facilité ainsi que les conditions de mise à disposition des données de santé par l'IDS* ». En d'autres termes, d'après les experts de l'IDS, si la finalité de la recherche est conforme aux objectifs d'amélioration des connaissances en santé, et à la condition que toutes les précautions soient prises pour assurer le respect de la vie privée des individus, les organismes privés à but lucratif devraient pouvoir déposer des dossiers auprès de l'IDS en vue d'accéder aux données agrégées du SNIIRAM.

La CNIL n'émet pas d'opposition à cette proposition d'ouvrir l'accès aux données agrégées pour les acteurs privés à but lucratif mais s'oppose à celle de l'EGB qui comporterait un risque trop important de réidentification. De plus, bien que la réponse de la Commission ne soit pas défavorable à une évolution de l'arrêté relatif au SNIIRAM, elle rappelle qu'en 2010, l'état du droit ne permet pas d'autoriser la société IMS Health à obtenir un accès sélectif, même si la finalité de l'étude envisagée permet d'améliorer la connaissance de la santé et des systèmes de soins. Il serait alors nécessaire de modifier la législation en vigueur encadrant l'accès aux données, puis réviser les normes de sécurité encadrant les données rendues accessibles aux acteurs privés à but lucratif. Cette réponse de la CNIL montre à quel point l'ouverture des données de santé au-delà du secteur non lucratif fait face à plusieurs barrières : celle du temps nécessaire à la révision des dispositions légales, et celle de la technique utile à la vérification de la bonne sécurité des données de santé. Il est donc clair que la réflexion engagée par l'IDS ne constitue que le frémissement d'une ouverture des données aux organismes privés à but lucratif. Le conseil apporté par la CNIL n'est pas surprenant à cet égard : elle délivre un accord

---

de Médecine de Dijon, responsable du service de bio statistique et informatique médicale, CHU de Dijon), Roxane SILBERMAN (directrice de recherche au CNRS Ecole d'Economie de Paris, Secrétaire générale du Comité de Concertation pour les Données en Sciences Humaines et Sociales CCDSHS).

[1365] Institut des données de santé, « Workflow sur les demandes d'utilisation des données du SNIIRAM », *op. cit.* La requête portait sur l'accès aux données agrégées, au tableau de bord et à l'EGB afin de réaliser une étude sur « les facteurs impactant le parcours de soins des patients souffrant de douleur chronique et leur prise en charge en France ». Déposée le 20 novembre 2009, cette demande à reçu une réponse négative le 25 juin 2010.

[1366] Institut des données de santé, « Enjeux et étapes », *op. cit.*, p. 44.

de principe à l'accès aux données de santé agrégées ne comportant aucun risque de réidentification, mais indique dans le même temps que cet accès ne peut avoir lieu que sous des conditions qui ne sauraient être remplies avant plusieurs années pour la simple raison qu'une réforme législative est nécessaire : nous savons aujourd'hui qu'à partir de cet avis, près de 6 années se sont écoulées avant que cette proposition n'aboutisse à travers la loi relative à la modernisation de notre système de santé[1367].

487. Les évolutions de cette doctrine de pensée ont finalement abouti aux 5 premières autorisations d'accès au bénéfice des acteurs à but lucratif le 18 janvier 2017. Chacune de ces approbations de traitement a été émise sous réserve (malheureusement le tableau fourni par l'IDS ne donne aucune information sur la nature et le contenu des réserves émises). Les organismes bénéficiaires de ces approbations sont Santéclair (société spécialisée dans les réseaux de soins et travaillant avec des organismes complémentaires d'assurance maladie comme Allianz, MAAF, MMA ou la Mutuelle Générale de la Police), Observia (bureau d'études spécialisé dans la e-santé) et Celtipharm devenu Openhealth (bureau d'études spécialisé dans l'analyse des données de santé). Les 5 demandes ayant reçu une autorisation correspondent à des études sur des données entrant dans un large périmètre, citons par exemple l'étude relative à la « *caractérisation du parcours de soins en amont de séjours hospitaliers* » ou encore celle relative au « *suivi de la consommation des benzodiazépines et antidépresseurs en France* ». Soulignons par ailleurs que d'autres demandes, émanant d'acteurs privés à but lucratif, ont été refusées le même jour par l'IDS. C'est le cas de MAAF Santé qui souhaitait traiter des données du SNIIRAM dans le cadre de deux études détaillées : la première concernait la consommation de soins et des restes à charge des patients en ALD, la seconde visait l'analyse longitudinale des composantes du reste à charge des patients. Il est probable que cette volonté de réaliser des études détaillées représentait une possible réidentification des individus et comportait donc un risque élevé pour la protection de la vie privée. Cela démontre que l'IDS est resté très prudent dans la délivrance des accès aux données de santé, alors même que le nouveau mécanisme, plus ouvert, était sur le point d'entrer en vigueur avec l'installation de l'INDS[1368]. Finalement, la dernière vague de rendus de décisions a eu lieu le 11 avril 2017 et contient aussi son lot d'approbations avec cinq autorisations d'accès délivrés à des organismes privés à but lucratif.

[1367] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1368] *Supra* n° 333.

488. Nous pourrions croire que ces décisions résultent uniquement de l'évolution doctrinale et idéologique concernant l'opportunité d'ouvrir l'accès sélectif aux acteurs privés à but lucratif. Pourtant, l'étude de la jurisprudence montre que le juge a également joué un rôle déterminant dans l'accessibilité des données de santé.

Paragraphe 2 : Les prémices jurisprudentiels favorables au secteur privé à but lucratif

489. Le vent d'ouverture des bases de données de santé provenant des initiatives menées par l'IDS et la CNIL a été appuyé une jurisprudence hautement importante. Bien que cette jurisprudence ait été rendue assez tardivement, en 2014, elle a permis de confirmer que les directions envisagées pour faire évoluer l'accès aux données de santé étaient fondées juridiquement.

490. La première jurisprudence que nous proposons d'analyser est celle rendue par le Conseil d'Etat le 26 mai 2014[1369]. Les faits dont traite cette décision remontent à l'année 2011, plus précisément au 8 septembre. En effet, c'est ce jour que la CNIL a délivré, au bénéfice de Celtipharm, une entreprise privée à but lucratif spécialisée dans les études en santé, une autorisation[1370] de mettre en œuvre un traitement de données à caractère personnel afin de procéder à la réalisation d'une étude épidémiologique. Les modalités de l'autorisation sont très intéressantes car cette dernière repose principalement sur l'anonymisation à bref délai des données issues des feuilles de soins électroniques[1371]. Cette autorisation n'a pas été délivrée sur le fondement du chapitre X de la loi relative à l'informatique et aux libertés[1372] car la société ne demande pas d'accéder aux données provenant du SNIIRAM. En revanche, elle souhaite pouvoir traiter des données provenant directement de feuilles de soins électroniques, c'est donc le III de l'article 8 de ladite loi[1373] qui sert de fondement juridique.

[1369] Conseil d'Etat, 10e et 9e sous-sections réunies, 26 mai 2014, n° 354903, recueil Lebon, Société IMS Health c/ CNIL.

[1370] Délibération n° 2011-246 du 8 septembre 2011 autorisant la mise en œuvre par la société Celtipharm d'un traitement de données à caractère personnel ayant pour finalité la réalisation d'études épidémiologiques à partir de données issues des feuilles de soins électroniques anonymisées à bref délai.

[1371] Fondement aujourd'hui supprimé depuis l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[1372] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*, chapitre X.

[1373] *Ibid.*, art. 8, III : « *Si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la*

Cette autorisation démontre que les acteurs privés à but lucratif peuvent mettre en œuvre des traitements de données personnelles de santé avec l'aval de la CNIL : il en découle que les garanties nécessaires à la protection de la vie privée des individus (patients et professionnels) sont apportées. Effectivement, lorsque l'on explore le contenu de la délibération du 8 septembre 2011, nous pouvons apprécier le résumé des caractéristiques du traitement envisagé par la société Celtipharm.

Outre la description détaillée des finalités du traitement envisagé, la délibération rendue par le Commission développe avec précision les catégories de données amenées à être traitées : font notamment partie du traitement autorisé des données relatives à la pharmacie émettrice de la feuille de soins électronique, des données sur le patient (y compris son identifiant anonyme unique, ses mois et année de naissance), des données sur le prescripteur (dont l'identifiant anonyme unique du prescripteur, sa spécialité, sa condition d'exercice, l'origine de la prescription de l'acte et la date de la prescription de l'acte). Il est directement notifié que le NIR, le jour de naissance, le rang de naissance et le numéro de complémentaire santé qui figurent sur la feuille de soins électronique ne sont utilisés que pour créer un identifiant anonyme et supprimés à bref délai. Cette formule est importante car elle fait le lien directement avec le paragraphe III de l'article 8 de la loi relative à l'informatique et aux libertés sur lequel repose le traitement : le procédé d'anonymisation à bref délai est conçu pour assurer la protection de la vie privée des individus, professionnels comme particuliers, dont les données de santé à caractère personnel font l'objet d'un traitement.

Les mesures liées à la mise en place des informations nécessairement délivrées aux individus sont également décrites dans la délibération de la CNIL. Conformément à l'obligation d'information qui découle de l'article 32 de la loi relative à l'informatique et aux libertés[1374], chaque individu dont les données font l'objet d'un traitement doit être informé des caractéristiques du traitement[1375] et de ses droits. Dans le cadre du traitement mis en œuvre par

Commission nationale de l'informatique et des libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25. Les dispositions des chapitres IX et X ne sont pas applicables ».

[1374] Art. 32 de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit*.

[1375] Ces caractéristiques sont multiples, nous trouvons notamment l'identité du responsable du traitement, la finalité du traitement, le caractère obligatoire ou facultatif de la fourniture des données, les destinataires ou catégories de destinataires des données, les droits dont dispose l'individu sur le traitement.

Celtipharm, c'est par voie d'affichettes présentes dans les pharmacies participant à la collecte des données que les individus sont informés. En complément, une plateforme téléphonique avec un numéro vert[1376] ainsi qu'une adresse électronique sont créés pour permettre à toute personne de demander des compléments d'informations.

La partie la plus importante dans le descriptif du traitement mis en œuvre par la société Celtipharm et autorisé par la CNIL est celle qui concerne la description de l'anonymisation des données et de la sécurité du processus. Ainsi, nous apprenons qu'avant de faire l'objet d'un quelconque traitement, toutes les données personnelles de santé font plusieurs fois l'objet d'une « *anonymisation irréversible à clé secrète de type FOIN*[1377] » : les données d'identification du patient passent deux fois de suite à travers ce procédé, la première est faite par les « *organismes concentrateurs techniques* » (OCT), la seconde par la société Celtipharm elle-même. Sans la clé de décryptage gardée secrète par les OCT, la société, responsable du traitement, se trouve dans l'incapacité d'inverser le processus d'anonymisation, ce qui garantit la protection de la vie privée. Pour les données d'identification des professionnels de santé, elles sont d'abord délivrées chiffrées par le GIE SESAM Vitale[1378]. Des clés de déchiffrement sont ensuite fournies à Celtipharm pour pouvoir déchiffrer les données afin de leur délivrer un nouvel identifiant par un système de type FOIN. Des précisions sont aussi apportées sur la sécurité des secrets cryptographiques détenus par Celtipharm : ces informations sont contenues sur supports individuels nécessitant un quorum minimum de 3 personnes pour pouvoir les activer. De plus, pour répondre aux critères de sécurité requis, tous les accès au système d'informations permettant le traitement sont tracés et des audits de sécurité réguliers sont effectués. Nous le constatons, si la CNIL donne l'autorisation à un organisme privé à but lucratif de traiter des données personnelles de santé, c'est à des conditions strictes et prévues par la loi.

491. Pourtant, une autre entreprise, la société IMS Health, a demandé l'annulation pour excès de pouvoir de la délibération de la CNIL autorisant le traitement. Bien que cette demande

[1376] Le fait qu'un numéro vert, donc gratuit, soit mis en place montre que le responsable du traitement donne véritablement les moyens aux individus d'obtenir plus d'information.

[1377] Le FOIN est la fonction d'occultation des informations nominatives utilisée pour chiffrer les données personnelles de santé contenues dans le SNIIRAM. V. *supra* n° 139.

[1378] Le GIE SESAM-Vitale a été créé en 1993 par les régimes général, agricole et des professions indépendantes de l'Assurances Maladie Obligatoire. C'est ce GIE qui a développé la carte vitale en France dès 1994 pour une démocratisation à l'ensemble des assurés français en 1998.

semble avant tout motivée par des raisons concurrentielles[1379], plusieurs arguments sont portés devant le Conseil d'Etat, lequel répond, point par point[1380], pour finalement appuyer la légalité de la délibération de la CNIL. Le Conseil d'Etat reconnaît d'une part le fondement légal de l'autorisation qui combine les articles 8, III, 25, I, 1° et 6, 2° de la loi relative à l'informatique et aux libertés[1381] ; d'autre part, il reconnaît la légitimité du traitement envisagé au regard de sa compatibilité avec la finalité du traitement pour lequel elles ont été initialement recueillies. Dès lors que le traitement prévu par la société Celtipharm a pour objectif d'améliorer la connaissance concernant la consommation de produits de santé et qu'il comporte une phase d'anonymisation, il est légitime, indépendamment du caractère éventuellement marchand de l'étude. Soulignons également que par sa décision, le Conseil d'Etat a confirmé que la CNIL est habilitée à autoriser des traitements de données incluant le NIR sans qu'il soit nécessaire qu'une autorisation préalable par décret en Conseil d'Etat soit délivrée. En effet, avec la réforme du 6 août 2004[1382], si l'article 27 de la loi relative à l'informatique et aux libertés[1383] porte toujours sur l'autorisation préalable par décret en Conseil d'Etat des traitements de données contenant le NIR[1384], un nouvel article est inséré, l'article 25, I, 6° qui précise que la CNIL peut aussi autoriser des traitements de données parmi lesquelles figure le NIR.

492. La décision du Conseil d'Etat est donc hautement significative pour tous les acteurs privés à but lucratif qui, dans le cadre de leur activité participant à une meilleure connaissance du système de santé et comportant un intérêt public, souhaitent traiter des données de santé à caractère personnel. Bien que le palier de l'accès aux données du SNIIRAM ne soit pas encore franchi, cette jurisprudence permet à tous les acteurs privés à but lucratif de savoir qu'ils ont l'opportunité de réaliser des recherches en traitant des données de santé à caractère personnel dans des conditions encadrées et sécurisées. Cette nouvelle interprétation, plus favorable au secteur privé à but lucratif, a indéniablement participé à l'ouverture plus sereine des esprits sur

[1379] CAPRIOLI Eric A., « Le Conseil d'Etat valide l'autorisation de la CNIL relative au traitement statistique de données de santé anonymisées au profit d'une entreprise privée », *Communication Commerce Electronique*, 01/07/2014, n° 7-8, p. 40-43.

[1380] *Ibid.* pour un commentaire détaillé de la décision du Conseil d'Etat.

[1381] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1382] Loi n° 2004-801 du 6 août 2004, *op. cit*.

[1383] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1384] Tous les traitements mis en œuvre pour le compte de l'Etat, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public, qui portent sur des données comprenant le NIR doivent être autorisés par décret en Conseil d'Etat d'après l'article 27, I, 1° de la loi *ibid.*

ce sujet sensible en vue de la présentation, de la discussion et du vote de la réforme qui a abouti à la loi du 26 janvier 2016[1385].

SECTION 2 : LE REVIREMENT DE LA LOI ET DU JUGE EN FAVEUR DE L'OUVERTURE DES DONNÉES DE SANTÉ

493. L'année 2016 est une année charnière pour l'accès des acteurs privés à but lucratif aux données de santé de l'assurance maladie. Elle est importante à deux égards : elle est d'abord reconnue pour être l'année d'adoption de la réforme créant le SNDS et modifiant en profondeur la procédure d'accès aux données de santé[1386]. Mais c'est également une année symbolique pour les acteurs privés à but lucratif qui ont vu le juge administratif mettre à mal le principe d'interdiction d'accès sélectif aux données du SNIIRAM dont ils faisaient l'objet. Nous analyserons donc en priorité le contenu de la loi du 26 janvier 2016[1387] dédié aux acteurs privés à but lucratif (§1), puis nous étudierons la décision du Conseil d'Etat[1388] qui a été délivrée quelques mois après l'adoption de la réforme (§2).

Paragraphe 1 : La consécration légale de l'autorisation d'accès aux données de santé

494. Le début de l'année 2016 a donné lieu à l'adoption de la réforme du système d'accès aux données de santé avec la loi de modernisation de notre système de santé[1389]. Le texte semble être arrivé à point nommé lorsque nous connaissons le contexte de cette année avec la parution du rapport hautement critique de la Cour des comptes[1390] sur le fonctionnement du dispositif d'accès aux données du SNIIRAM, mais également avec la décision du Conseil d'Etat[1391] du 20 mai 2016 que nous étudierons prochainement[1392]. Ce texte de loi est l'aboutissement de plusieurs années de réflexions, de rapports, de discussions autour des moyens pouvant être mis en œuvre pour favoriser l'utilisation des données de santé à caractère personnel contenues dans

[1385] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1386] *Ibid*.

[1387] *Ibid.*

[1388] Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, recueil Lebon, Celtipharm.

[1389] *Ibid*.

[1390] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit*.

[1391] Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, *op. cit*.

[1392] *Infra* n° 501 à 504.

le SNIIRAM tout en assurant une protection adéquate permettant de respecter le droit au respect de la vie privée des individus. Le législateur procède alors à la mise en place d'un tout nouveau système en modifiant la loi relative à l'informatique et aux libertés[1393] et en créant de nouveaux articles au sein du code de la santé publique. Les acteurs privés à but lucratif ont probablement découvert avec grand intérêt le contenu de la loi et des décrets qui en découlent[1394]. En effet, alors que les arrêtés relatifs à la mise en œuvre du SNIIRAM interdisaient, depuis l'arrêté du 20 juin 2005[1395], l'accès sélectif au secteur privé à but lucratif, aucun des nouveaux textes, y compris le décret qui définit le fonctionnement du SNDS et dresse la liste des bénéficiaires de l'accès permanent[1396], ne prévoit une telle interdiction. Ce silence doit être interprété comme une autorisation étendue de profiter de la nouvelle procédure d'accès sélectif aux données du SNDS sans qu'aucune exclusion ne soit possible sur le seul fondement du but lucratif du demandeur. Cette ouverture ne signifie pas pour autant qu'aucune précaution n'est mise en place par le législateur : l'étude des dispositions insérées dans le code de la santé publique apporte de nombreux enseignements concernant les restrictions auxquelles sont soumises tous les acteurs amenés à traiter des données provenant du SNDS. Certaines de ces mesures visent, par ailleurs, directement des activités qui relèvent du secteur privé à but lucratif.

495. Un nouveau titre est ainsi inséré dans le livre IV dédié à l'administration générale de la santé, de la première partie du code de la santé publique dénommée « *Protection générale de la santé* ». Il s'agit du titre VI intitulé « *Mise à disposition des données de santé* ». Cette initiative est hautement symbolique en ce qu'elle inscrit directement dans la loi les principes relatifs à la mise à disposition des données de santé. Ainsi, dès l'article L. 1460-1 du code de la santé publique, les finalités potentielles des données de santé à caractère personnel recueillies « *à titre obligatoire et destinées aux services ou aux établissements publics de l'Etat ou des collectivités territoriales ou aux organismes de sécurité sociale* » sont clairement prévues afin d'autoriser les « *traitements à des fins de recherche, d'étude ou d'évaluation présentant un caractère d'intérêt public* ». Par cette précision, le législateur crée une base légale à la réutilisation des données notamment contenues dans le SNIIRAM désormais intégré dans le

[1393] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[1394] V. le décret n° 2016-1871 du 26 décembre 2016 *relatif au traitement de données à caractère personnel dénommé « système national des données de santé »*, JORF n° 0301, 28/12/2016 et le décret n° 2016-1872 du 26 décembre 2016 *modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, JORF n° 0301, 28/12/2016.

[1395] Arrêté du 20 juin 2005, *op. cit.*

[1396] Décret n° 2016-1871 du 26 décembre 2016, *op. cit.*

nouveau SNDS[1397] dans un cadre qui reste contraignant car seules des finalités listées de manière exhaustive justifient de tels traitements.

496. Une fois ces principes posés à titre liminaire, le code de la santé publique modifié par la loi de modernisation de notre système de santé[1398] dresse, à l'article L. 1461-1, le type de données contenues dans le SNDS, les finalités de ce dernier et, plus important encore, les mesures de sécurités qui s'imposent pour tout traitement de données qui sont issues du système. Les paragraphes IV et V de l'article L. 1461-1 du code de la santé publique disposent en effet que toutes les personnes qui accèdent aux données du SNDS sont soumises au secret professionnel[1399] dont la violation peut donner lieu à une condamnation à un an d'emprisonnement et 15 000 euros d'amende[1400]. Ils précisent également que la confidentialité, l'intégrité des données, et la traçabilité des accès et des traitements réalisés doivent être assurées[1401] conformément à un référentiel défini par arrêté du ministère des affaires sociales et de la santé[1402].

Cependant, trois points supplémentaires font particulièrement écho aux activités potentielles des acteurs privés à but lucratif. Le premier point exige que le traitement des données contenues dans le SNDS ne conduise, à aucun moment, à prendre une décision à l'encontre d'une personne physique identifiée[1403] : cela rejoint le principe selon lequel les traitements doivent avant tout être mus par une finalité d'intérêt public. Le deuxième point interdit formellement aux traitements réalisés à partir des données du SNDS d'avoir pour finalité de promouvoir des « *produits à finalité sanitaire destinés à l'homme et des produits à finalité cosmétique* » auprès des professionnels de santé ou des établissements de santé[1404]. Quant au troisième point, il interdit de traiter les données du SNDS afin d'exclure des garanties d'un contrat d'assurance ou de modifier le montant de « *cotisations ou de primes d'assurance d'un individu ou d'un*

[1397] Pour la liste des bases de données de santé regroupées dans le SNDS, v. *supra* n° 414.

[1398] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1399] Art. L. 1461-1, IV, 2° du code de la santé publique.

[1400] Art. 226-13 du code pénal.

[1401] Art. L. 1461-1, IV, 3° du code de la santé publique.

[1402] Arrêté du 22 mars 2017 *relatif au référentiel de sécurité applicable au Système national des données de santé*, JORF, n° 0071, 24/03/2017.

[1403] Art. L. 1461-1, IV, 1° du code de la santé publique.

[1404] Art. L. 1461-1, V, 1° du code de la santé publique.

groupe d'individus présentant un même risque »[1405]. Bien que la loi dispose avec clarté que seule une finalité d'intérêt public permet de traiter des données du SNDS, le législateur a souhaité ôter toute forme d'ambiguïté dont auraient pu se prévaloir certains organismes privés à but lucratif. Les laboratoires pharmaceutiques, les fabricants de cosmétiques et les organismes assureurs sont directement visés par les interdictions insérées dans le code de la santé publique.

497. En complément de ces finalités interdites, d'autres restrictions s'imposent aux acteurs privés à but lucratif. Le paragraphe 2 de l'article L. 1461-3 du code de la santé publique[1406] dispose que les organismes privés à but lucratif qui produisent ou commercialisent des médicaments ou des cosmétiques ainsi que les organismes de crédit, les organismes assureurs ou les intermédiaires d'assurance, doivent remplir une condition particulière pour être autorisés à obtenir et traiter des données provenant du SNDS. Cette condition est, au choix, soit l'apport de la preuve que le traitement appelé à être mis en œuvre empêche toute utilisation des données pour l'une des deux finalités interdites précitées[1407] ; soit le recours à un laboratoire de recherches ou un bureau d'études, peu importe qu'il soit public ou privé, pour effectuer le traitement. Le laboratoire ou le bureau d'études choisi doit cependant s'engager auprès de la CNIL à être conforme au référentiel publié par arrêté du ministère des affaires sociales et de la santé. Bien que cela ne soit pas directement indiqué dans le texte de l'arrêté du 22 mars 2017[1408] créant le référentiel de sécurité applicable au SNDS, nous pouvons légitimement penser que la mention « *Vu le code de la santé publique, notamment son article L. 1461-1* » permet d'inclure les dispositions de l'article L. 1461-3 du même code dans le *visa*. Nous comprenons donc que, si tous les acteurs privés à but lucratif sont désormais admis à bénéficier de l'accès sélectif dans l'optique de réaliser un traitement ayant une finalité d'intérêt public, certains d'entre eux, qui sont tout de même les plus susceptibles de trouver une utilité pratique dans le traitement des données proposées, sont soumis à des mesures particulièrement restrictives afin de prévenir au maximum toute atteinte au droit au respect de la vie privée.

Nous pouvons souligner que le recours à un sous-traitant pour réaliser un traitement de données de santé à caractère personnel issues du SNDS est ici entièrement légitimé par le législateur.

[1405] Art. L. 1461-1, V, 2° du code de la santé publique.

[1406] Art. L. 1461-3, II, 1° et 2° du code de la santé publique.

[1407] *Supra* n° 496.

[1408] Arrêté du 22 mars 2017 *relatif au référentiel de sécurité applicable au Système national des données de santé*, *op. cit*.

Pourtant, cette démarche était clairement identifiée comme un moyen détourné de traiter des données de santé dans l'ancien système[1409].

498. Le respect de ces mesures constitue l'un des piliers incontournables de l'accès aux données aux SNDS pour le secteur privé à but lucratif. L'autre pilier est matérialisé dans la procédure d'accès sélectif, entièrement remaniée par la réforme. Comme nous l'avons déjà étudié dans la partie précédente[1410], l'accès sélectif repose désormais intégralement sur la sous-section 2 de la section 3 du chapitre 3 du titre II de la loi relative à l'informatique et aux libertés[1411] (nouvelle numérotation du chapitre IX) et l'ancien chapitre X de ladite loi a été abrogé. Cette uniformisation, destinée à simplifier le processus d'accès aux données de santé, a également donné lieu à la création de l'INDS comme guichet unique auprès duquel déposer les dossiers de demande d'accès au SNDS. Sans qu'il soit nécessaire de revenir sur l'intégralité du nouveau dispositif, il est important de mettre en exergue le rapport de confiance qui existe entre ses différentes parties prenantes. En effet, une fois les conditions requises réunies et l'examen de la demande d'accès préalable passé, les acteurs privés à but lucratif sont libres de procéder au traitement de données de santé à caractère personnel pour lequel ils ont obtenu une autorisation. Jusqu'à ce que les résultats du traitement et les moyens d'en analyser la validité soient communiqués à l'INDS à l'issue de la recherche, comme prévu par l'article L. 1461-3 du code de la santé publique[1412], le responsable du traitement est finalement libre de réaliser le traitement pour lequel il a obtenu l'autorisation. Le législateur compte sur la bonne volonté des bénéficiaires de l'accès sélectif qui doivent se borner à ne procéder qu'au traitement prévu par le dossier ayant obtenu un feu vert de la part de la CNIL à l'issue de la procédure d'autorisation préalable. En d'autres termes, si un acteur privé à but lucratif décide d'outrepasser les limites fixées par la loi, les autorités ne pourront s'en rendre compte qu'une fois que la violation aura eu lieu. La position des organismes privés à but lucratif est, sur ce point, limpide d'après les déclarations de M. GIRARD[1413] lors d'un entretien réalisé en décembre 2016 : ceux-ci souhaitent que « *des sanctions claires et exemplaires soient prononcées à l'encontre de ceux qui iront sur des finalités interdites* ». En outre, les multiples séances d'informations effectuées,

[1409] *Supra* n° 468 et 469.

[1410] *Supra* n° 331.

[1411] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par l'ordonnance 2018-1125 du 12 décembre 2018, *op. cit.*

[1412] Art. L. 1461-3, II, b) du code de la santé publique.

[1413] Mylène GIRARD est cheffe de la mission « *accès aux données de santé* » à la DREES depuis le mois de mai 2016.

à l'initiative de la DREES, avec les représentants du secteur privé à but lucratif ont permis de faire passer le message selon lequel, à la moindre constatation d'une utilisation frauduleuse des données de santé du SNDS par une entreprise, la procédure d'accès pourrait être totalement fermée dans l'attente d'analyser les éventuels dysfonctionnements et les solutions permettant d'y remédier.

499. Il ressort de tout cela que les acteurs privés à but lucratif sont encore différenciés, d'une certaine façon, dans leur accès aux données de santé car ils font l'objet d'un traitement particulier. Le SNDS leur est désormais accessible mais des conditions supplémentaires leur sont imposées dans une finalité objective de protection de la vie privée des individus sur lesquels portent les données traitées. Les résultats attendus de ce bouleversement résident avant tout dans la production d'études, de plus en plus nombreuses, permettant d'améliorer les connaissances de notre système de santé.

500. Outre l'adoption de la réforme du 26 janvier 2016, un autre événement important a eu lieu au cours de cette année : il s'agit de la décision du Conseil d'Etat du 20 mai 2016[1414] rendue en faveur de l'ouverture de l'accès sélectif aux données de santé du SNIIRAM pour les acteurs privés à but lucratif.

Paragraphe 2 : La consécration jurisprudentielle de l'autorisation d'accès aux données de santé

501. Nous avons étudié, dans la section précédente[1415], la jurisprudence du Conseil d'Etat favorable à ce que les acteurs privés à but lucratif puissent réaliser des traitements de données à caractère personnel dans un cadre contrôlé par la CNIL et à la condition d'effectuer une anonymisation à court terme des données sensibles. Une autre jurisprudence du Conseil d'Etat a apporté un vent de nouveauté, bien tardif, dans le domaine de l'accès aux données de santé. Il s'agit de l'arrêt rendu par le Conseil d'Etat le 20 mai 2016[1416], soit près de 4 mois après l'adoption de la loi de modernisation de notre système de santé[1417], impliquant une fois de plus la société Celtipharm. Celle-ci avait enjoint à la ministre des affaires sociales et de la santé

[1414] Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, *op. cit*.

[1415] *Supra* n° 489 à 492.

[1416] Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, *op. cit*.

[1417] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

d'abroger les dispositions du 3° du III de l'article 4 de l'arrêté du 19 juillet 2013 relatif à la mise en œuvre du SNIIRAM interdisant l'accès aux données de santé pour les organismes privés à but lucratif. Cette demande d'abrogation est datée du 19 juillet 2014. Or, la ministre a gardé le silence et n'a jamais répondu à la requête de la société Celtipharm. Cette dernière a donc demandé l'annulation pour excès de pouvoir de la décision de rejet implicite découlant de ce silence. Le raisonnement du Conseil d'Etat est alors très intéressant à suivre.

502. L'arrêt du 20 mai 2016 s'attache à décortiquer le rôle de la ministre des affaires sociales et de la santé dans la rédaction de l'arrêté relatif à la mise en œuvre du SNIIRAM. Comme indiqué à son article 1er, ledit arrêté a uniquement pour objet d'approuver « *le protocole du 8 juin 2012 et ses annexes définissant les modalités de gestion et de renseignement du Système national d'information interrégimes de l'assurance maladie (SNIIRAM)* »[1418]. Puis les articles 2 à 7 n'ont pour objet que de définir « *les finalités du traitement ainsi mis en œuvre, la liste des informations nécessaires, rassemblées dans une base de données nationale, les destinataires de ces informations* […] »[1419]. Cependant, le Conseil d'Etat s'arrête particulièrement sur l'avant-dernière disposition du 3° du III de l'article 4 de l'arrêté du 19 juillet 2013 : ce sont précisément les mesures qui interdisent aux acteurs privés à but lucratif l'accès aux données du SNIIRAM. Le juge considère que la ministre des affaires sociales et de la santé a outrepassé ses compétences en allant plus loin que la simple approbation des modalités de gestion et de renseignement du SNIIRAM qui comprennent bien la définition des destinataires potentiels des données qu'il contient.

Pourtant, la ministre des affaires sociales et de la santé amène plusieurs arguments en soutien de sa défense. Elle estime d'abord que l'interdiction d'accès aux données du SNIIRAM pour les acteurs privés à but lucratif est parfaitement déductible des dispositions contenues dans l'annexe II du protocole du 8 juin 2012[1420] qui établit notamment la liste des autorités compétentes, pour chaque utilisateur de données du SNIIRAM, à traiter des données qui en sont issues : cette interdiction serait, d'après la ministre des affaires sociales et de la santé, l'interprétation logique du protocole. Elle argue également de l'application transparente de

[1418] Arrêté du 19 juillet 2013 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, JORF n° 0187, 13/08/2013, art. 1.

[1419] Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, *op. cit*.

[1420] Protocole inter-régimes du 8 juin 2012 *relatif au système national d'information interrégime de l'assurance maladie*, BO Santé – Protection sociale – Solidarité n° 2013/8, 15/09/2013.

l'article 3.5 dudit protocole qui « *prévoit la fixation par arrêté ministériel des destinataires des informations contenues dans le SNIIRAM* »[1421], ce qui aurait pour conséquence de créer une base légale suffisante pour lui permettre de sélectionner les organismes pouvant avoir accès aux données du SNIIRAM.

503. Le Conseil d'Etat contredit, sur ces deux arguments, la ministre des affaires sociales et de la santé. En effet, il souligne qu'il n'est pas possible de déduire de l'annexe II du protocole du 8 juin 2012 une interdiction quelconque d'accès aux données du SNIIRAM pour les acteurs privés à but lucratif : cette annexe n'a pour objet que « *d'identifier pour certains utilisateurs, l'autorité compétente pour accéder aux informations contenues dans le SNIIRAM* »[1422]. Le juge en déduit que l'annexe II n'a pas vocation à exclure tous les acteurs non listés d'une possibilité d'accéder aux données par le biais de l'accès sélectif. C'est donc la ministre qui a elle-même décidé de fixer une nouvelle règle non prévue par le protocole.

Par ailleurs, le juge porte son attention sur l'article 3.5 du protocole qui aurait conféré à la ministre des affaires sociales et de la santé la compétence pour déterminer les organismes habilités à accéder aux données du SNIIRAM. Cet article indique que « *les destinataires des informations contenues dans le système national d'information interrégime de l'assurance maladie sont fixés par arrêté ministériel, à raison de leurs fonctions et selon les règles d'habilitation détaillées à l'annexe II du protocole* »[1423]. Il est vrai que la lecture combinée de cet article et de l'annexe II à laquelle il est fait référence peuvent laisser penser que c'est un arrêté ministériel qui définit les personnes autorisées ou non à obtenir des données du SNIIRAM. Pourtant le Conseil d'Etat est catégorique sur ce point, une telle disposition présente dans le protocole n'est pas de nature à constituer un fondement légal à la compétence de la ministre. A la suite de ce constat, le juge poursuit son raisonnement afin de vérifier si un autre fondement légal existe, notamment à travers le chapitre X de la loi relative à l'informatique et aux libertés[1424].

[1421] Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, *op. cit*., paragraphe 5.

[1422] *Ibid*., paragraphe 5.

[1423] Protocole inter-régimes du 8 juin 2012, *op. cit.*, article 3.5.

[1424] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

Par son analyse, le Conseil d'Etat confirme que les dispositions légales en vigueur « *ne restreignent pas la qualité des personnes susceptibles de solliciter, à des fins d'évaluation des pratiques de soins et de prévention, la communication d'informations issues du SNIIRAM* »[1425]. Le juge reconnaît bien que la loi impose à la CNIL de contrôler les garanties présentées par les demandeurs d'accès avant de procéder à toute communication, mais il remarque, dans le même temps, que si toutes les conditions sont remplies, la loi, qu'il s'agisse de la loi relative à l'informatique et aux libertés[1426] ou du code de la sécurité sociale[1427], ne s'oppose à aucun moment à ce que les organismes ayant un but lucratif soient exclus de toute opportunité d'autorisation.

504. Il ressort de ces deux points de la décision du Conseil d'Etat que le ministre chargé des affaires sociales et de la santé a ajouté, dès l'arrêté du 20 juin 2005[1428], sans véritable fondement juridique, l'interdiction de déposer une demande d'obtention de données du SNIIRAM dans le cadre de l'accès sélectif. Effectivement, souvenons-nous que l'arrêté initial du 11 avril 2002[1429] ne comprenait pas une telle interdiction. Ni le protocole du 15 octobre 2001[1430], ni son avenant du 16 mai 2005[1431], tous deux approuvés par les arrêtés relatifs à la mise en œuvre du SNIIRAM, ne prévoient d'interdiction d'accès à l'encontre des organismes privés à but lucratif. Dès lors, le Conseil d'Etat décide deux choses : le refus implicite de la ministre des affaires sociales et de la santé d'abroger l'arrêté du 19 juillet 2013 dans sa partie relative à l'exclusion des organismes privés à but lucratif de l'accès aux données du SNIIRAM est annulé. Puis, plus important encore, le juge laisse un délai de 4 mois, à compter de la notification de la décision, à la ministre des affaires sociales et de la santé pour abroger les dispositions litigieuses de l'arrêté. Nous pouvons donc raisonnablement croire que la date limite d'abrogation desdites mesures a été fixée à la fin du mois de septembre 2016. Pourtant, ce n'est pas avant la parution, au Journal officiel daté du 19 octobre 2016, de l'arrêté relatif à la mise en œuvre du SNIIRAM

[1425] Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, *op. cit*., paragraphe 7.

[1426] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1427] Art. L. 161-28-1 du code de la sécurité sociale relatif au protocole définissant les modalités de gestion et de renseignement du SNIIRAM.

[1428] Arrêté du 20 juin 2005, *op. cit.*

[1429] *Supra* n° 460.

[1430] Protocole inter-régimes du 15 octobre 2001 *relatif au système national d'information interrégime de l'assurance maladie*, BO Santé – Protection sociale – Solidarité n° 2002/14 du 7 avril 2002.

[1431] Avenant n° 1 du 16 mai 2005 au protocole inter-régimes du 15 octobre 2001 *relatif au système national d'information interrégime de l'assurance maladie*, BO Santé – Protection sociale – Solidarité n° 2005/10, 15/11/2005.

du 6 octobre 2016[1432] que l'injonction d'abrogation a été appliquée. La ministre de la santé a finalement accepté de modifier le dernier alinéa du 3°, du III, de l'article 4 de l'arrêté afin qu'il adopte une rédaction plus ouverte vis-à-vis du secteur privé à but lucratif : cette nouvelle rédaction permet ainsi à « *tout autre organisme de recherche, des universités, écoles ou autres structures d'enseignement liés à la recherche que ceux mentionnés au paragraphe précédent* » de déposer une demande d'accès sélectif. L'objet lucratif ou non n'est donc plus un facteur déterminant.

L'intervention du Conseil d'Etat a été interprétée par la presse comme « *une secousse* [qui] *a bousculé le monde très verrouillé des données de santé* »[1433]. Pourtant, cette prise de position du juge administratif devrait être perçue comme la continuité de la jurisprudence du 26 mai 2014[1434] plutôt que comme une révolution. Comme certains auteurs l'ont écrit, il s'agit là d'un « *nouveau message envoyé dans le sens d'une ouverture accrue des données de ce SNIIRAM, quelques semaines seulement après un rapport critique de la Cour des comptes* [1435] *sur l'utilisation des données du SNIIRAM appelant, également, à une libération sous contrôle de ces données* »[1436]. La publication du rapport de la Cour des comptes et celle de la décision du Conseil d'Etat, quelques mois seulement après le vote de la réforme[1437] créant le SNDS et prévoyant une ouverture contrôlée à tous les demandeurs, tendent à démontrer que les acteurs privés à but lucratif n'auraient pas été en mesure de supporter plus longtemps leur exclusion. En cette année 2016, les esprits des français semblaient fin prêts à l'ouverture des données du SNIIRAM.

[1432] Arrêté du 6 octobre 2016 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, JORF n° 0244, 19/10/2016.

[1433] THIBERT C., « Les données personnelles de santé accessibles aux assurances et laboratoires », *Le Figaro*, 30/05/2016.

[1434] Conseil d'Etat, 10e et 9e sous-sections réunies, 26 mai 2014, n° 354903, *op. cit.*

[1435] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*

[1436] PERRIN G., « Données de santé : le Conseil d'Etat repose la question de l'ouverture », *Argus de l'Assurance*, 23/05/2016.

[1437] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

CONCLUSION DU CHAPITRE II

505. L'interdiction d'accès aux données de santé dont ont été la cible les acteurs privés à but lucratif s'est progressivement transformée en autorisation par une intégration dans le processus d'accès sélectif. Dès 2010[1438], l'IDS souligne que des bureaux d'études souhaiteraient réaliser des traitements de données de santé issues du SNIIRAM et présentant un intérêt public : mais leur caractère d'acteur privé à but lucratif les exclut d'emblée. La CNIL aussi a eu l'occasion de se prononcer sur un dossier[1439] émanant d'un bureau d'études en 2010. Elle reconnait que l'accès aux SNIIRAM à des fins de recherche devrait être élargi à tous les organismes. Pourtant, ce n'est pas avant l'année 2017 que les premières véritables autorisations d'accès au bénéfice des acteurs privés à but lucratif ont été délivrées.

En parallèle de cette évolution de pensée, l'intervention du juge a probablement intercédé en faveur d'un changement plus rapide. En effet, l'entreprise Celtipharm a été autorisée par le Conseil d'Etat, en 2014[1440], à réaliser un traitement à partir de données provenant de feuilles de soins numérisées : bien que l'autorisation délivrée ne repose pas sur les mesures liées à l'accès sélectif, il s'agit d'un premier pas vers l'élargissement de l'accès aux données de santé.

506. L'année charnière de l'ouverture pour les acteurs privés à but lucratif est 2016. La réforme du 26 janvier 2016[1441] est l'aboutissement de plusieurs années de réflexions pour construire un système qui permette d'ouvrir l'accès aux données de santé au secteur privé à but lucratif tout en apportant les garanties nécessaires à la protection de la vie privée des individus. Deux finalités interdites inscrites dans le code de la santé publique visent alors spécifiquement les laboratoires pharmaceutiques et les organismes assureurs. Le Conseil d'Etat a également apporté sa pierre à l'édifice en mai 2016[1442] en indiquant que le pouvoir réglementaire n'a pas la compétence pour exclure les acteurs privés à but lucratif de l'accès aux données de santé du SNIIRAM. Ainsi, l'interdiction d'accès posée par arrêté dès 2005 n'a jamais été fondée en droit. Bien que cette décision soit prise après le vote de la réforme qui ouvre justement l'accès sélectif

[1438] Institut des données de santé, « Enjeux et étapes », *op. cit.*

[1439] *Ibid.*

[1440] Conseil d'Etat, 10e et 9e sous-sections réunies, 26 mai 2014, n° 354903, *op. cit.*

[1441] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1442] Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, *op. cit.*

aux données de santé au secteur privé à but lucratif, elle apporte un soutien supplémentaire aux partisans de l'élargissement des accès.

CONCLUSION DU TITRE I

507. L'entrée en fonctionnement du nouvel accès sélectif incluant les acteurs privés à but lucratif a finalement eu lieu à la fin du mois d'août 2017[1443]. Depuis lors, tout acteur peut déposer une demande d'accès aux données du SNDS auprès de l'INDS, dans le respect des normes de sécurité prévues par la loi. Ce qui a changé avec cette réforme du 26 janvier 2016[1444], ce n'est pas réellement la protection des données de santé à caractère personnel, c'est la manière dont le tri est effectué entre les données pouvant être diffusées et celles qui ne peuvent pas l'être. Le législateur a doté le système de santé de nouveaux acteurs ayant, en théorie, les compétences et les capacités pour mener à bien leur mission de mise à disposition des données de santé dans un cadre sécurisé et fonctionnel. Cela permet à la fois de respecter la vie privée des individus, particuliers aussi bien que professionnels, et de favoriser l'amélioration de la connaissance du système de santé par la multiplication des recherches rendues possibles grâce à la nouvelle procédure d'accès sélectif.

508. Nous pouvons cependant considérer que cette évolution est bien tardive compte tenu de la place croissante qu'occupent les traitements de données depuis le début des années 2000[1445]. L'ouverture des données de santé au secteur privé à but lucratif est le résultat de plusieurs années d'échanges, parfois conflictuels[1446], entre les responsables des bases de données administratives et les acteurs privés concernés. Une discussion peut notamment être tenue à propos de l'argument de l'utilisation nécessairement vertueuse des données lorsqu'elles sont traitées uniquement par des acteurs publics. D'autres questions peuvent aussi se poser concernant le coût que devrait avoir l'accès aux données de santé ou bien la meilleure sécurité des données lorsqu'elles sont conservées par l'administration. Ces sujets, non exhaustifs, font l'objet de notre prochain chapitre dédié à l'accès des acteurs privés à but lucratif aux données de santé.

[1443] *Supr*a n° 336.

[1444] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1445] La CNIL reconnaissait dès l'année 2001 que les sites internet dédiés à la santé se multipliaient déjà de façon exponentielle, v. BOSSI J., « La circulation des données de santé », *RGDM*, 2004, n° 4, p. 55-64.

[1446] Initiative transparence santé, « Liberté pour les données de santé », *Manifeste*, 2013.

TITRE II

L'AUTORISATION PROGRESSIVE D'ACCÈS AUX DONNÉES DE SANTÉ POUR LES ACTEURS PRIVÉS À BUT LUCRATIF

509. L'accès à la base de données de santé SNIIRAM a longtemps été conçu avec l'interdiction, par principe, d'accès au détriment des acteurs privés à but lucratif. Cette fermeture catégorique de l'accès est un principe qui a dominé pendant plus de 10 ans (depuis l'arrêté de 2005[1447] posant le principe d'interdiction, jusqu'au vote de la réforme du 26 janvier 2016[1448]). Nous l'avons abordé précédemment dans cette étude[1449], le droit européen[1450], alors encore appelé droit communautaire, et le droit français[1451] interdisent par principe le traitement des données de santé. C'est l'autorisation de traitement qui est exceptionnelle. Il en découle que l'accès aux données de santé de l'assurance maladie contenues dans le SNIIRAM relève un caractère exceptionnel. Toutefois, les autorités nationales françaises se sont engagées, dès les premières années d'activité du dispositif, dans la voie de l'interdiction totale d'accès au SNIIRAM pour le secteur privé à but lucratif alors même que de nombreux autres acteurs publics, ou privés à but non lucratif, disposaient d'un accès soumis à autorisation préalable[1452], voire permanent[1453] pour certains.

510. Toutes les réflexions étaient alors tournées vers le sujet de la protection des données de santé à caractère personnel[1454] et, par extension, des individus qui en étaient à l'origine. Mais

[1447] Arrêté du 20 juin 2005, *op. cit.*

[1448] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1449] *Supra* n° 60.

[1450] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[1451] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[1452] V. Partie II.

[1453] V. Partie I.

[1454] BESLAY N., « Les applications de données médicales personnelles : approche juridique pratique », *RGDM*, 2004, n° 4, p. 35-40 ; BEYNEIX I., « Le traitement des données personnelles par les entreprises : big data et vie privée, état des lieux », *JCP G*, 09/11/2015, n° 46-47, p. 2113-2119 ; BOSSI J., « Comment organiser aujourd'hui en France la protection des données de santé », *RDSS*, 01/03/2010, n° 2, p. 208 ; CASTETS-RENARD C., « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data », *Revue Lamy de Droit de l'Immatériel*, 01/10/2014, supplément au n° 108, p. 38-45 ; CHEMTOB-CONCE M.-C., « La protection des données de santé à caractère personnel », *RGDM*, 01/06/2003, n° 10, p. 111-126 ; DAUBECH L., « La collecte des données de santé », *RGDM*, 2004, n° 4, p. 41-54 ; VACARIE I., « La finalité des traitements de données de santé », *RGDM*, 30/09/2004, n° 4, p. 27-34.

la plupart de ces réflexions s'attachaient directement à la possibilité de traiter des données de santé à caractère personnel sans approcher le système d'accès aux données contenues dans le SNIIRAM. Pourtant, la faculté d'obtenir des données provenant des bases de données administratives en santé est nécessairement affectée par les questions de sécurité et de protection. La doctrine ne semble pas s'être intéressée aux raisons de fond qui ont conduit le pouvoir réglementaire français à fermer totalement aux acteurs privés à but lucratif l'accès aux données de santé alors même que cette décision était parfaitement contraire au droit : en effet, dans une décision du 20 mai 2016[1455], le Conseil d'Etat a affirmé que la ministre des affaires sociales et de la santé n'avait pas les compétences pour interdire, par arrêtés successivement pris entre 2005 et 2013, l'accès du SNIIRAM aux acteurs privés à but lucratif à des fins d'évaluation des pratiques de soins et de prévention[1456]. Remarquons que pendant toutes ces années, personne n'a formellement contesté le refus d'autorisation posée par le pouvoir réglementaire. Il semblerait que, malgré l'absence, aujourd'hui avérée, de fondement légal, la fermeture des données de santé ait été considérée comme une fatalité ne pouvant pas être remise en cause sans faire peser de risque irrépressible sur la vie privée des individus.

511. Il est donc opportun de s'intéresser aux raisonnements qui ont été tenus et suivis en majorité dans le but de justifier l'exclusion du secteur privé à but lucratif de toute possibilité d'accès, et nous verrons dans quelles mesure ces raisonnements présentent des faiblesses. Le recul qui est le nôtre aujourd'hui nous permet de remettre en question les justifications de l'interdiction d'accès afin de mieux comprendre pourquoi cette interdiction s'est aujourd'hui transformée en autorisation de principe, sous conditions. Nous observerons d'abord l'instabilité des arguments permettant l'exclusion des acteurs privés à but lucratif (Chapitre 1), puis nous évoquerons les modalités d'adaptation et d'acceptation du nouveau principe d'admission du secteur privé à but lucratif dans le mécanisme d'accès sélectif aux données de santé (Chapitre 2).

[1455] Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, *op. cit*.

[1456] Pour l'étude complète de la décision, v. *supra* n° 501 à 504.

CHAPITRE I
L'ACCÈS AUX DONNÉES DE SANTÉ REFUSÉ SANS MOTIF CONCRET

512. Dans la présente section, notre objectif est de déterminer dans quelle mesure les arguments mis en avant pour interdire, dès 2005, l'accès des acteurs privés à but lucratif au SNIIRAM sont suffisamment ou insuffisamment fondés. Nous commencerons simplement par décrypter le manque de traçabilité des réflexions qui ont abouti à la fermeture de l'accès aux données de santé (Section 1), puis nous analyserons l'influence qu'a certainement pu avoir le développement des phénomènes des données ouvertes et des données massives (Section 2) sur les décisions ministérielles.

SECTION 1 : L'INTROUVABLE JUSTIFICATION DU REFUS D'AUTORISATION D'ACCÈS

513. Il est nécessaire d'avoir une approche pédagogique pour aborder ce paragraphe convenablement. Il est évident que les justifications de l'interdiction d'accès au SNIIRAM pour les acteurs privés à but lucratif doivent être discutées sur le plan juridique. Ce qui nous intéresse dans le cas présent, ce sont également les justifications matérielles apportées par le ministre de la santé et des solidarités à partir de l'arrêté de 2005[1457]. Nous allons constater que la décision de mettre à l'écart le secteur privé à but lucratif laisse filtrer une impression d'arbitraire (§1), tandis que l'argument sécuritaire qui pourrait être à l'origine de la décision du ministre reste discutable (§2).

Paragraphe 1 : Le caractère arbitraire du refus d'autorisation d'accès

514. Nous savons que le premier arrêté relatif à la mise en œuvre du SNIIRAM[1458] daté de 2002 ne comportait aucune distinction entre les acteurs à but lucratif ou non[1459] : tous les acteurs non bénéficiaires d'un accès permanent pouvaient déposer une demande auprès de la CNIL en vue d'obtenir des données. Cependant, dans la pratique, aucune demande d'accès provenant d'un acteur privé à but lucratif n'a été recensée. Si aucune raison concrète n'est proposée par les

[1457] Arrêté du 20 juin 2005, *op. cit.*

[1458] Arrêté du 11 avril 2002, *op. cit*.

[1459] *Supra* n° 460.

rapports qui évoquent cette possibilité d'accès théorique[1460], nous pouvons supposer que les conditions matérielles n'étaient, en réalité, pas réunies pour que l'accès aux données de santé soit effectif pour le secteur privé à but lucratif à partir de 2002. Ceci étant précisé, aucune raison explicite apparente ne nous permet de comprendre pourquoi un revirement a été mis en œuvre. En effet, l'arrêté du 20 juin 2005[1461] a créé l'interdiction d'accès au détriment des acteurs privés à but lucratif, interdiction qui a duré jusqu'à la réforme du 26 janvier 2016[1462], dont la mise en œuvre réelle n'a commencé qu'à partir du 28 août 2017[1463]. Bien que nous sachions déjà que le pouvoir réglementaire n'avait pas la compétence juridique pour insérer une telle interdiction dans l'arrêté[1464], il est important de comprendre comment et pourquoi cette décision a été prise. Un ou des rapports ont-ils été remis ? Un audit a-t-il été réalisé pour savoir si les gestionnaires du SNIIRAM étaient, ou non, en mesure de mettre à disposition des données de manière sécurisée ? Quel fondement juridique a été mis en avant pour justifier la mise à l'écart du secteur privé à but lucratif ?

515. Ces questions semblent aller de soi tant la mesure est radicale et a limité drastiquement les opportunités offertes aux acteurs privés à but lucratif. Pourtant, malgré des recherches conséquentes portant sur les travaux qui ont mené à la décision d'interdiction, aucun élément traitant directement de l'accès aux données de santé du SNIIRAM et apportant une réponse tangible n'a été recueilli. Seuls quelques documents abordent, de façon annexe, le sujet de l'accès des acteurs privés à but lucratif aux données de santé. Cela ne signifie pas pour autant qu'il n'y a pas de commentaire à apporter. Bien au contraire, cette absence de résultat dans nos recherches est révélatrice du caractère arbitraire de la décision du ministre de la santé et des solidarités. Effectivement, si nous observons les documents officiels disponibles avant la prise de l'arrêté, deux documents attirent particulièrement l'attention : le rapport relatif à l'accès des assureurs aux feuilles de soins daté de 2003[1465] ainsi qu'un avis plus ancien de la Commission européenne au sujet de l'utilisation des données personnelles de santé en date de 1999[1466].

[1460] BABUSIAUX C., BREAS L., ESLOUS L., THOUVENIN D., *Rapport, L'accès des assureurs complémentaires aux données de santé des feuilles de soins électroniques,* 26 mai 2003, p. 92.

[1461] Arrêté du 20 juin 2005, *op. cit.*

[1462] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1463] *Supra* n° 409.

[1464] *Supra* n° 504.

[1465] BABUSIAUX C., BREAS L., ESLOUS L., THOUVENIN D., *Rapport, L'accès des assureurs complémentaires aux données de santé des feuilles de soins électroniques*, *op. cit.*

[1466] Commission européenne, *Avis n° 13 du 30 juillet 1999 : Aspects éthiques de l'utilisation des données*

Dans l'avis rendu par la Commission européenne[1467], il est fait référence aux opportunités qui doivent être offertes aux acteurs privés à but lucratif, notamment les employeurs et organismes assureurs qui « *peuvent obtenir des informations sur l'état de santé de leurs clients ou de leurs salariés* », mais une limite est posée : « *ils ne doivent en aucun cas pouvoir avoir directement accès aux dossiers médicaux des intéressés* »[1468]. L'avis insiste également sur le principe de finalité légitime qui doit exister entre la collecte des données et leur traitement. Est-ce cet avis qui a motivé l'interdiction d'accès au SNIIRAM insérée dans l'arrêté de 2005[1469] ? Force est de constater que non. Les données auxquelles auraient pu accéder les organismes privés à but lucratif n'auraient évidemment pas eu de caractère identifiant ou réidentifiant conformément à l'ancien article 64 de la loi relative à l'informatique, aux fichiers et aux libertés[1470]. Il n'existait donc pas de risque que les organismes privés à but lucratif accèdent aux dossiers médicaux des individus. Par ailleurs, la finalité de l'accès aux données du SNIIRAM serait entrée dans le cadre de l'accès sélectif, qui repose sur l'ancien chapitre X de la loi relative à l'informatique, aux fichiers et aux libertés[1471] et dont la finalité affichée est l'évaluation ou de l'analyse des pratiques de soins ou de prévention. Cela correspond parfaitement aux finalités du SNIIRAM qui sont notamment l'amélioration de la qualité des soins, la contribution à une meilleure gestion de l'assurance maladie, ou encore la contribution à une meilleure gestion des politiques de santé[1472]. La lecture de l'avis donné par la Commission européenne ne donne, à aucun moment, d'arguments visant à exclure totalement les acteurs privés à but lucratif de l'accès à des données de santé non identifiantes et non réidentifiantes. La seule recommandation d'interdiction clairement établie concerne l'accès de ces acteurs au dossier médical des individus : ce qui est formellement rendu impossible dans le cadre de l'accès sélectif aux données du SNIIRAM auquel auraient pu prétendre les acteurs privés à but lucratif. Il ne semble

personnelles de santé dans la société de l'information, Journal international de bioéthique, 2001/3, vol. 12, p. 113-117.

[1467] *Ibid.*

[1468] *Ibid*., p. 4.

[1469] Arrêté du 20 juin 2005, *op. cit.*

[1470] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit*., art. 64 : « [la CNIL] *vérifie que les données à caractère personnel dont le traitement est envisagé ne comportent ni le nom, ni le prénom des personnes concernées, ni leur numéro d'inscription au Répertoire national d'identification des personnes physiques* ».

[1471] *Ibid.*, chap. X.

[1472] Il s'agit des finalités mises à jour par l'arrêté du 20 juin 2005, *op. cit*. Les finalités prévues par l'arrêté initial du 11 avril 2002, *op. cit*., étaient moins détaillées v. *supra* n° 95.

donc pas que ce texte soit à l'origine de la décision prise par le ministre de la santé et des solidarités dans son arrêté de 2005.

Le rapport relatif à l'accès des organismes de complémentaire santé aux feuilles de soins électroniques[1473] recèle peut-être plus d'indices. En effet, le document concerne tous les organismes assureurs complémentaires qui comprennent, comme nous l'avons détaillé dans le titre précédent[1474], des entreprises d'assurance qui sont des acteurs privés à but lucratif, mais également des mutuelles ainsi que des institutions de prévoyances et qui sont, elles, des organismes privés à but non lucratif. Le chapitre 6 du rapport est même spécialement dédié à l'étude de l'ouverture de l'accès de ces organismes aux données anonymisées du SNIIRAM « *à des fins d'analyse statistique, d'ajustement de leur offre et de contribution à la gestion du risque* »[1475]. Les auteurs du rapport précisent que les organismes de complémentaire santé sont prêts à alimenter le SNIIRAM en contrepartie d'un accès ouvert aux données dont ils ont besoin pour améliorer leur activité : nous pouvons considérer que cet objectif peut s'inscrire dans la finalité d'amélioration de la gestion des politiques de santé, prévue par l'arrêté de 2005[1476], notamment par la surveillance de la consommation de soins ou bien par le suivi et l'évaluation de la santé des patients et leurs conséquences sur la consommation de soins. De plus, le rapport indique spécifiquement que « *l'accès des assureurs complémentaires au SNIIRAM est techniquement possible dès 2004 et* [que] *les trois caisses nationales y ont donné leur accord dans le cadre de la présente mission* ». Toutefois, nous savons déjà[1477] que cette volonté démontrée d'ouvrir le SNIIRAM aux organismes de complémentaire santé que sont les entreprises d'assurance, organismes privés à but lucratif, les mutuelles et les institutions de prévoyance, organismes privés à but non lucratif, si elle était présente dès 2003, ne s'est concrétisée qu'avec la parution de l'arrêté du 1er décembre 2011[1478] : malgré un besoin et des solutions apportées dès le début des années 2000, 8 ans ont dû s'écouler pour que le projet d'ouverture d'accès voie finalement le jour. Cette ouverture, très encadrée et limitée aux seuls

[1473] BABUSIAUX C., BREAS L., ESLOUS L., THOUVENIN D., *Rapport, L'accès des assureurs complémentaires aux données de santé des feuilles de soins électroniques*, *op. cit*.

[1474] *Supra* n° 475.

[1475] BABUSIAUX C., BREAS L., ESLOUS L., THOUVENIN D., *Rapport, L'accès des assureurs complémentaires aux données de santé des feuilles de soins électroniques, op. cit.*, p. 91-92.

[1476] Arrêté du 20 juin 2005, *op. cit.*

[1477] *Supra* n° 474 à 479.

[1478] Arrêté du 1er décembre 2011, *op. cit*.

organismes de complémentaire santé, incluant des acteurs privés à but lucratif, n'est pas une autorisation d'accès sélectif aux données de santé et fait l'objet d'une analyse nuancée dans le titre précédant[1479]. Bien que ce rapport ne vise pas l'ensemble des acteurs privés à but lucratif, nous comprenons qu'il prône l'exact inverse d'une fermeture du SNIIRAM : au contraire, c'est son ouverture, certes limitée à une catégorie précise de bénéficiaires que sont les organismes de complémentaire santé, qui est conseillée. Il en ressort que ce n'est pas dans ce document que le ministre de la santé et des solidarités a puisé son inspiration pour introduire, dans l'arrêté de 2005[1480], l'interdiction totale d'accès à l'attention du secteur privé à but lucratif.

516. Si nous ne trouvons pas de réponses à nos questions dans les travaux liés à la notion d'accès aux données de santé, il est probable que nous en trouvions dans les travaux de préparation de l'arrêté qui a créé l'interdiction d'accès au SNIIRAM. Deux documents attirent, à ce titre, notre attention : l'avenant du 16 mai 2005 au protocole du 15 octobre 2001 définissant les modalités de gestion et de renseignement du SNIIRAM[1481] et l'avis de la CNIL du 14 juin 2005.

L'avenant du 16 mai 2005 au protocole du 15 octobre 2001[1482] est intéressant à lire car il est le fondement de la publication de l'arrêté de 2005[1483]. Or, sa lecture nous apprend qu'il ne modifie que la liste des acteurs bénéficiaires d'un accès garanti au SNIIRAM. Parmi eux figurent 4 acteurs publics[1484] dont l'accès est soumis à autorisation de la CNIL dans le cadre du chapitre X de la loi relative à l'informatique aux fichiers et aux libertés[1485] : il est d'ailleurs surprenant de remarquer que l'arrêté a transformé cet accès sélectif prévu par le protocole en accès permanent pour ces 4 acteurs[1486]. En revanche, l'avenant au protocole ne prévoit aucunement

[1479] *Supra* n° 474 à 479.

[1480] Arrêté du 20 juin 2005, *op. cit.*

[1481] Avenant n° 1 du 16 mai 2005 au protocole inter-régimes du 15 octobre 2001 *relatif au système national d'information interrégime de l'assurance maladie,* BO Santé – Protection sociale – Solidarité n° 2005/10 du 15/11/2005.

[1482] *Ibid.*

[1483] Arrêté du 20 juin 2005, *op. cit.*

[1484] Il s'agit des chercheurs de l'Institut de recherche et de documentation en économie de la santé (IRDES), des agents du centre technique d'appui et de formation des centres d'examen de santé, des chercheurs de l'Institut national de la santé et de la recherche médicale (INSERM), des chercheurs du Centre national de la recherche scientifique (CNRS).

[1485] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1486] Arrêté du 20 juin 2005, *op. cit.*, art. 4, 5°.

de créer ou de promouvoir l'interdiction pour les acteurs privés à but lucratif de bénéficier de l'accès sélectif. Ce document n'est donc pas non plus la source qui a poussé le ministre de la santé et des solidarités à prendre sa décision.

Qu'en est-il de l'avis rendu par la CNIL le 14 juin 2005 d'après le *visa* présent en tête de l'arrêté de 2005 ? Rappelons que l'article L. 161-28-1 du code de la sécurité sociale dispose que l'arrêté approuvant le protocole relatif aux modalités de gestion et de renseignement du SNIIRAM doit être pris « *après avis motivé de la Commission nationale de l'informatique et des libertés* ». Dès lors, il est opportun d'examiner l'avis rendu le 14 juin 2005 pour en connaître le contenu et les éventuels commentaires qui auraient pu viser les acteurs privés à but lucratif. Etonnamment, cet avis ne semble pas exister[1487] ! Est-ce un dysfonctionnement ou une erreur dans la date inscrite dans l'arrêté ? Il semblerait bien que non : il n'existe aucune trace d'un avis rendu par la CNIL en 2005 à propos du projet d'arrêté relatif aux modalités de mise en œuvre et de gestion du SNIIRAM. Ni la base de données Légifrance[1488], ni le site internet de la CNIL[1489] ne contiennent d'avis rendu au cours de l'année 2005 en lien avec l'arrêté du 20 juin 2005. Chose encore plus étrange, si nous consultons le rapport annuel de la CNIL retraçant l'intégralité de son activité sur l'ensemble de l'année 2005[1490], la liste des délibérations adoptées en 2005 qui figure en annexe[1491] est vierge de toute délibération portant avis sur un quelconque projet d'arrêté du ministère de la santé et des solidarités. Deux observations peuvent être apportées à cette lacune documentaire. La première est le basculement potentiel de l'arrêté de 2005 dans l'illégalité pour défaut de procédure. Sans l'avis préalable de la CNIL prévu par l'article L. 161-28-1 du code de la sécurité sociale, la décision prise par le ministre de la santé et des solidarités perd sa base légale. La seconde nous amène à penser que le pouvoir réglementaire a décidé, seul, de fermer l'accès au SNIIRAM pour les acteurs privés à but lucratif.

[1487] Nous avons contacté les services de la CNIL à plusieurs reprises des mois de mai à juillet 2018 pour en savoir plus sur cet avis du 14 juin 2005, sans obtenir de réponse.

[1488] www.legifrance.gouv.fr

[1489] www.cnil.fr

[1490] Commission nationale de l'informatique et des libertés, « 26e rapport d'activité 2005 », *La documentation française*, 2006, 125 p.

[1491] *Ibid.*, p.109-122.

517. Il en ressort que l'hypothèse du caractère arbitraire de cette interdiction insérée dans l'arrêté de 2005 est confortée par l'analyse du contexte de l'époque. Cela ne signifie pas pour autant qu'il aurait fallu intégrer les acteurs privés à but lucratif dans le mécanisme d'accès sélectif sans réflexion préalable. Cependant, le mode opératoire est hautement contestable et des discussions concrètes sur le sujet auraient dû voir le jour et donner lieu à une décision transparente : il en aurait peut-être résulté une ouverture du SNIIRAM plus précoce que celle que nous avons connue avec la réforme du 26 janvier 2016[1492]. Maintenant que nous avons étudié les potentielles influences officielles sur la décision d'interdiction d'accès, il est nécessaire de s'intéresser à l'argument qui a probablement conduit le ministre de la santé et des affaires sociales à prendre une telle décision : celui de la sécurité des données et de la protection de la vie privée des individus.

Paragraphe 2 : L'argument sécuritaire discutable du refus d'autorisation d'accès

518. La question de la sécurité des données personnelles de santé est dans tous les esprits dès lors que l'on évoque la possibilité d'utiliser ces données dans un traitement automatisé. Dès le début des année 2000, en vue de la transposition en droit français de la directive du 24 octobre 1995[1493], le débat entourant cette problématique capitale est né avec, en son cœur, la volonté de respecter « *les droits des personnes dont les données personnelles de santé sont collectées – risques d'utilisation détournée, risques de violation de la vie privée* »[1494]. L'un des autres points sensibles concerne également « *l'indépendance professionnelle et morale des médecins* »[1495]. Lorsque le pouvoir réglementaire a pris la décision de fermer l'accès au SNIIRAM pour les acteurs privés à but lucratif, la protection de la vie privée des particuliers ainsi que de l'activité des professionnels de santé par la sécurisation des données de santé à caractère personnel était déjà centrale dans le débat sur la numérisation de la santé. Etant donné que nous n'avons pas trouvé d'argumentaire issu de documents officiels[1496], tels que des rapports ou avis, il est probable que le ministre de la santé et des solidarités ait trouvé une justification à sa prise de position en se basant sur les incertitudes qui pouvaient graviter autour de la sécurité des données

[1492] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1493] Directive 95/46/CE du 24 octobre 1995, *op. cit.*

[1494] BESLAY N., « Les applications de données médicales personnelles : approche juridique pratique », *RGDM*, 2004, n° 4, p. 35-40.

[1495] CHEMTOB-CONCE M.-C., « La protection des données de santé à caractère personnel », *RGDM*, 01/06/2003, n° 10, p. 111-126.

[1496] *Supra* n° 514 à 517.

transmises aux acteurs privés à but lucratif. Le développement qui va suivre consiste alors à étudier le bien-fondé d'une telle hypothèse et d'en débusquer les failles par une analyse du droit positif et de cas d'école concrets.

519. Nous nous sommes attachés à étudier le contenu des publications parues avant l'arrêté du 20 juin 2005[1497]. Ces documents portent notamment sur les applications de données médicales personnelles[1498], l'exploitation des données de santé[1499], ou encore la finalité des traitements de données de santé[1500]. Si aucun texte ne porte précisément sur l'accès aux données de santé à caractère personnel contenues dans le SNIIRAM, la question de la sécurité des données est diffuse dans chacun des raisonnements tenus. En matière d'applications de données de santé, convoitées par les acteurs privés à but lucratif, N. BESLAY présentait ainsi, en 2004, les mesures de protection des données requises comme le chiffrement des données ou la mise en place d'outils de traçabilité[1501]. La réflexion proposée n'intègre à aucun moment de distinction entre acteurs selon leur nature ou leur caractère lucratif ou non : les mêmes mesures de sécurité s'imposent à chacun d'entre eux. La même année, I. VACARIE s'est intéressée à l'autorisation de traiter des données de santé fondée sur la finalité de traitement. Elle revient dans son étude sur l'évocation des mesures de sécurité examinées dans le cadre de la procédure prévue en cas de recherche dans le domaine de la santé et parle de la nécessité de valider les « *solutions techniques retenues pour la protection des informations : codages, sécurité des systèmes etc…* »[1502].

Un élément est flagrant dans l'ensemble de ces publications : les questions relatives à la sécurité des données, si elles sont systématiquement évoquées, sont à chaque fois rapidement évacuées par des références techniques à des modalités pratiques de protection des informations. Etrangement, la question de savoir à partir de quel moment cette protection est suffisante n'est jamais abordée par les auteurs. Pourtant, il s'agit d'un point clef de l'interdiction d'accès pour les acteurs privés à but lucratif : si le SNIIRAM leur a été entièrement fermé pendant tant

[1497] Arrêté du 20 juin 2005, *op. cit.*

[1498] BESLAY N., « Les applications de données médicales personnelles : approche juridique pratique », *op. cit*.

[1499] KHODOSS H., « L'exploitation des données de santé », *RGDM*, 30/09/2004, n° 4, p. 65-76.

[1500] VACARIE I., « La finalité des traitements de données de santé », *RGDM*, 30/09/2004, n° 4, p. 27-34.

[1501] BESLAY N., « Les applications de données médicales personnelles : approche juridique pratique », *op. cit.*, p. 38.

[1502] VACARIE I., « La finalité des traitements de données de santé », *op. cit.*, p. 34.

d'années, cela devrait nécessairement être justifié par des failles potentielles qui auraient été détectées dans les mesures destinées à sécuriser les données de santé à caractère personnel. Seul ce type de danger pesant sur les données serait de nature à apporter un fondement à l'interdiction d'accès.

520. Si l'on se reporte aux modalités d'accès au SNIIRAM qui correspondent alors au chapitre X de la loi relative à l'informatique et aux libertés[1503], aujourd'hui abrogé, il était prévu que, au cours de la procédure, la CNIL vérifie que « *les données personnelles dont le traitement est envisagé ne comportent ni le nom ni le prénom des personnes concernées ni leur numéro d'inscription au Répertoire national d'identification des personnes physiques* »[1504]. De plus, seules peuvent être communiquées aux acteurs qui en font la demandent, des données « *sous la forme de statistiques agrégées ou de données par patient constituées de telle sorte que les personnes concernées ne puissent être identifiées* »[1505]. Partant de là, toutes les données de santé qui sortent du SNIIRAM pour être communiquées dans le cadre d'un accès sélectif sont suffisamment protégées pour ne pas risquer de compromettre la vie privée des individus et les professionnels. Si toutes les conditions sont réunies par le demandeur, il doit pouvoir obtenir les données de santé dont il fait la demande, qu'il soit à but lucratif ou non : la loi n'opère aucune distinction entre les deux. Il nous semble donc difficile de considérer que malgré toutes ces précautions, les acteurs privés à but lucratif soient mis à l'écart en raison d'un problème de sécurité dans des données qui sont censées avoir été traitées pour ne pas être réidentifiantes.

Cette réflexion amène une interrogation supplémentaire concernant le déséquilibre que crée de l'interdiction d'accès. En effet, comment un problème de sécurité dans les données pourrait-il justifier l'interdiction d'accès pour les acteurs privés à but lucratif alors que les acteurs publics et privés à but non lucratif bénéficient de l'accès sélectif ? La question est légitime car si c'est bien l'argument sécuritaire qui a été retenu pour prendre l'arrêté du 20 juin 2005[1506], cela implique que les acteurs privés à but lucratif ont d'une part, plus de moyens d'exploiter les failles éventuelles que les autres acteurs, d'autre part, une ambition incontrôlable de se servir des données de santé récoltées pour violer le droit au respect de la vie privée des individus. Ce

[1503] Loi n° 78-17 du 6 janvier 1978, *op. cit.,* modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.,* chap. X.

[1504] CHEMTOB-CONCE M.-C., « La protection des données de santé à caractère personnel », *op. cit.*, p.126.

[1505] *Ibid*., p. 125.

[1506] Arrêté du 20 juin 2005, *op. cit.*

postulat relève de la caricature à plus d'un titre. Il suppose déjà que les acteurs publics et privés à but non lucratif manquent de moyens et ne prennent jamais de décisions contraires à la législation en vigueur. Il implique aussi que les acteurs privés à but lucratif soient beaucoup plus avancés techniquement, notamment dans des technologies permettant de traiter les données pour les rendre réidentifiantes, et ont pour objectif de créer de la richesse par tous les moyens, y compris en violant la loi. Nous pourrions discuter longuement de la légitimité de ces assertions : elles ne peuvent pas, à elles seules, justifier l'interdiction d'accès au SNIIRAM pour les acteurs privés à but lucratif.

521. Au vu de ces développements, nous pouvons penser que le ministre de la santé et des solidarités a décidé d'interdire l'accès au SNIIRAM pour le secteur privé à but lucratif afin d'assurer la sécurité des données en se fondant sur une sorte de principe de précaution. Il semblerait que, compte tenu des nombreux doutes existant quant aux capacités de certaines entreprises à traiter les données pour réidentifier des individus dans un but commercial, la décision ait été prise de ne pas prendre de risque en fermant totalement l'accès à une catégorie entière d'acteurs. Cette décision, qui n'a été levée que par la loi du 26 janvier 2016[1507], serait finalement le fruit d'incertitudes à la fois concernant la pérennité du traitement destiné à anonymiser les données extraites, mais aussi concernant la capacité des autorités, CNIL en tête, à contrôler les traitements de données de santé potentiellement mis en œuvre dans ce cadre. Cela révèle aussi le manque de confiance du pouvoir réglementaire dans la fiabilité de l'accès sélectif aux données de santé : malgré un traitement préalable des données et un examen approfondi du dossier par la CNIL, le mécanisme serait encore insuffisant pour être étendu aux acteurs privés à but lucratif.

522. L'argument de la sécurité des données pour justifier l'interdiction d'accès au SNIIRAM est hautement contestable en l'état. Cela ne signifie pas que l'accès sélectif aurait dû être ouvert à tous dès 2005. En revanche, nous pensons qu'une réflexion commune avec les acteurs concernés aurait dû être menée afin de créer un moyen pour le secteur privé à but lucratif de solliciter l'obtention de données de santé de manière sécurisée pour la vie privée des individus. La sécurité des données est encore aujourd'hui une question centrale avec notamment la démocratisation du stockage de données en lignes, ou *cloud*, le développement des objets connectés, et tous les procédés dérivés du mélange entre données ouvertes et données massives.

[1507] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

Ces deux phénomènes soulèvent des questions depuis le début du XXIe siècle car les opportunités qu'ils offrent n'ont d'égal que les risques qu'ils créent : il se pourrait que chacun de ces mouvements ait eu une influence sur la décision d'interdire l'accès aux données de santé du SNIIRAM pour les acteurs privés à but lucratif.

SECTION 2 : LES RISQUES POTENTIELS INSUFFISANTS DE L'AUTORISATION D'ACCÈS

523. Lorsque la décision d'interdire aux acteurs privés à but lucratif d'accéder au SNIIRAM a été prise, nous pouvons penser que les autorités n'avaient peut-être pas le recul suffisant pour prendre la responsabilité de leur permettre d'obtenir des données qui sont en théories non identifiantes mais dont les technologies de l'informatique, en pleine croissance, pourraient les rendre réidentifiantes. En sus de l'argument sécuritaire déjà développé dans la section précédente[1508], les doutes existants quant aux possibilités offertes par les données ouvertes et les données massives ont pu conforter la décision du ministre de la santé et des solidarités. Nous allons donc étudier en quoi l'argument de l'incertitude concernant l'impact de les données ouvertes n'est pas suffisant pour fermer l'accès au SNIIRAM (§1), puis nous aborderons la question des données massives et de leur influence certaine sur l'exclusion du secteur privé à but lucratif (§2).

Paragraphe 1 : La nouveauté des données ouvertes, argument irrecevable du refus d'autorisation d'accès

524. Le concept des données ouvertes[1509] est d'abord un mouvement qui a poussé à l'ouverture des bases de données scientifiques de manière globale dans les années 1990[1510]. Ce n'est qu'au début des années 2000 que le concept des données ouvertes a été transféré aux bases de données administratives[1511]. Dès lors que des réflexions existaient déjà au moment de la publication de

[1508] *Supra* n° 518 à 522.

[1509] Traduction proposée par la Commission générale de terminologie et de néologie de l'Académie française et inscrite au Journal officiel, texte n° 107, JORF n° 0103, 03/05/2014. Le texte les définit comme étant des « *données qu'un organisme met à la disposition de tous sous forme de fichiers numériques afin de permettre leur réutilisation* ».

[1510] *Supra* n° 69 à 76.

[1511] V. Initiative de Budapest pour l'accès ouvert lancée lors du congrès des 1er et 2 décembre 2001 par les institutions les plus avancées dans le domaine des archives ouvertes et diffusée le 14 février 2002 ; Déclaration de *Berlin sur le libre accès à la connaissance* définie lors du congrès de Berlin du 22 octobre 2003 tenu à la société

l'arrêté du 20 juin 2005[1512] fermant le SNIIRAM aux acteurs privés à but lucratif, nous pouvons considérer que des arguments en ont été tirés pour appuyer l'interdiction. Pourtant, si l'on examine la directive de 2003[1513], le texte s'attache plus à traiter, comme le signalent G. GORCE et F. PILLET dans leur rapport[1514], de la dimension liée à la réutilisation des données du secteur public, plutôt que des données ouvertes dans leur ensemble. La directive se garde même d'imposer aux Etats membres d'autoriser la réutilisation des informations du secteur public, comme le précise son considérant n° 9[1515]. Mais ce que nous constatons surtout, c'est que les organismes privés à but lucratif ne sont pas écartés ou visés par des mesures spécifiques dans le mécanisme des données ouvertes. Ce n'est donc pas dans cette directive que les autorités ont puisé leur inspiration pour justifier leur décision de fermer l'accès au SNIIRAM à une catégorie donnée d'acteurs. D'une manière globale, ce qui est frappant lorsque l'on aborde les documents disponibles sur ce sujet au début des années 2000, c'est le manque cruel de matière : tous les rapports, les publications, les ouvrages doctrinaux concernant la question de l'application des données ouvertes au domaine de la santé semblent être parus à partir de 2014. Il y a une explication à cela, ces documents ont été produits en vue de la transposition en droit français de la directive du 26 juin 2013[1516]. Les nombreuses questions sur les données ouvertes qui auraient dû se poser avant que l'interdiction d'accès ne soit imposée au secteur privé à but lucratif ont réellement été étudiées près de 10 années plus tard.

Dès lors, nous pouvons commencer par supposer que les autorités françaises n'avaient simplement pas suffisamment d'informations tangibles sur le fonctionnement des données ouvertes pour les inclure dans leur raisonnement : les doutes et incertitudes sur l'impact de l'application des données ouvertes aux données de santé, potentiellement nuisible pour le respect de la vie privée, aurait alors conduit à l'application d'un principe de précaution excluant directement une catégorie d'acteurs de l'accès au SNIIRAM. Mais si nous prenons la

Max-Planck ; Directive 2003/98/CE du 17 novembre 2003 concernant la réutilisation des informations du secteur public.

[1512] Arrêté du 20 juin 2005, *op. cit.*

[1513] Directive 2003/98/CE, *op. cit*.

[1514] GORCE G. et PILLET F., Rapport d'information au Sénat, *La protection des données personnelles dans l'open data : une exigence et une opportunité*, 16 avril 2014, 85 p.

[1515] Directive 2003/98/CE, *op. cit*., considérant 9 : « *La présente directive ne contient aucune obligation d'autoriser la réutilisation de documents. La décision d'autoriser ou non la réutilisation est laissée à l'appréciation des États membres ou de l'organisme du secteur public concernés* ».

[1516] Directive 2013/37/UE du 26 juin 2013 *modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public*.

problématique dans le sens inverse, nous pouvons examiner les réflexions développées à partir de 2014 et, partant des différentes préconisations requises, tenter de savoir si le ministre de la santé, avec tous ces éléments en mains, aurait maintenu cette décision d'interdire l'accès aux données de santé du SNIIRAM pour les acteurs privés à but lucratif.

525. Sur la première hypothèse, nous savons déjà que c'est le ministère de la santé et des solidarités qui a créé, de toutes pièces, une interdiction de bénéficier de l'accès sélectif qui n'était pas prévue par l'avenant du 16 mai 2005[1517] au protocole du 15 octobre 2001 relatif aux modalités de gestion et de renseignement du SNIIRAM[1518]. Le Conseil d'Etat a condamné cette liberté prise par le pouvoir réglementaire dans sa décision du 20 mai 2016 étudiée dans le titre précédent[1519]. Cette interdiction a nécessairement une source. Nous pensons que cette source pourrait découler de plusieurs ruissellements d'idées, l'un d'eux étant le facteur des données ouvertes. Le pouvoir exécutif n'avait pas encore les moyens de savoir si le secteur privé à but lucratif aurait les ressources pour exploiter toutes les données ouvertes mises à sa disposition pour, éventuellement, les traiter d'une façon qui serait contraire au droit au respect de la vie privée. *A fortiori*, le ministre de la santé et des solidarités s'est probablement interrogé sur l'avance dont disposaient potentiellement les organismes privés à but lucratif dans la maîtrise des données ouvertes recueillies par rapport aux acteurs publics et au secteur privé à but non lucratif. Après avoir pesé les intérêts des individus et des professionnels de santé d'un côté, des entreprises de l'autre, nous pouvons légitimement penser que la décision a été prise de ne faire courir aucun risque, aussi mince soit-il, sur les données de santé. L'application d'un tel principe de précaution est contestable[1520] en ce que cela prive des acteurs pourtant légitimes de recevoir des données qui sont, quoi qu'il arrive, traitées pour ne pas être réidentifiantes avant d'être transmises.

526. Intéressons-nous maintenant à notre seconde hypothèse. Le rapport délivré par la commission *open data* en santé[1521] en 2014 conclut à la nécessité d'ouvrir les bases de données

[1517] Avenant n° 1 du 16 mai 2005 *au protocole inter-régimes du 15 octobre 2001 relatif au système national d'information interrégime de l'assurance maladie*, BO Santé – Protection sociale – Solidarité n° 2005/10, 15/11/2005.

[1518] Protocole inter-régimes du 15 octobre 2001 *relatif au système national d'information interrégime de l'assurance maladie*, BO Santé – Protection sociale – Solidarité n° 2002/14, 07/04/2002.

[1519] *Supra* n° 501 à 504.

[1520] *Supra* n° 521.

[1521] BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé*, 09/07/2014, 122 p.

en santé en organisant la mise à disposition de toutes les données anonymes « *sans préjuger de l'utilisation qui en sera faite* »[1522]. La mise en œuvre d'un traitement spécifique dédie aux acteurs privés à but lucratif n'est nullement évoquée. Plus important encore, ledit rapport s'intéresse directement au SNIIRAM élargi, qualifié de « *base indirectement nominative* »[1523] : les auteurs considèrent que toutes les données anonymes qui en sont issues doivent aussi être mises à disposition de tous, quelle que soit la nature des destinataires des données. Ce sont donc nécessairement des données agrégées qui doivent devenir des données ouvertes d'après le rapport.

Un rapport d'information au Sénat[1524], également délivré en 2014 et salué par la doctrine[1525], traite des critères qui doivent être remplis pour que des données personnelles puissent devenir des données ouvertes et réutilisées. Les auteurs du rapport mettent en avant les mesures découlant de la loi dite CADA[1526], de la loi relative à l'informatique et aux libertés[1527], ainsi que du code pénal. Il en ressort que dès lors que les données ont fait l'objet d'un traitement conduisant à les rendre anonymes, leur mise à disposition et leur réutilisation est possible. Toutefois, contrairement au rapport vu précédemment, celui-ci se veut bien plus prudent et pointe les risques pesant sur les données anonymes rendues ouvertes en rappelant que, d'après C. KIRCHNER qui représente l'Institut national de la recherche en informatique et en automatique (INRIA) « *aucune technique d'anonymisation n'est en théorie infaillible* »[1528]. Dès lors, le rapport fait référence au SNIIRAM en indiquant que « *la richesse des informations contenues dans ces bases rend le risque de ré-identification très important, ce qui justifie les mesures de restriction d'accès aujourd'hui mises en œuvre* ». Là encore, les auteurs posent un diagnostic sur l'opportunité d'appliquer le principe des données ouvertes à la base SNIIRAM : ils semblent d'accord avec le principe de fermeture et la mise en place d'accès sur autorisation

[1522] *Ibid.*, p. 44.

[1523] *Ibid.*, p. 51.

[1524] GORCE G. et PILLET F., Rapport d'information au Sénat, *op. cit*.

[1525] CASTETS-RENARD C., « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data », *Revue Lamy de Droit de l'Immatériel*, 01/10/2014, supplément au n° 108, p. 38-45.

[1526] 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*, dite loi "CADA" (Commission d'accès aux documents administratifs), JORF, 18/07/1978.

[1527] Loi n° 78-17 du 6 janvier 1978, *op. cit.*

[1528] GORCE G. et PILLET F., Rapport d'information au Sénat, *op. cit*., p. 46.

préalable mais ne se prononcent à aucun moment sur le bien-fondé de l'interdiction d'accès qui pèse sur les acteurs privés à but lucratif.

Au-delà de ces rapports, les auteurs de doctrine comme C. DEBOST[1529], P. DESMARAIS[1530], ou A. LAUDE, [1531] ont écrit à propos du principe des données ouvertes appliqué aux données de santé contenues dans le SNIIRAM. Ces écrits, comme les rapports, ne s'intéressent pas à la question de l'exclusion des acteurs privés à but lucratif de l'accès aux données de santé.

Il ressort de ces différents rapports et articles de doctrine qu'à partir du moment où une donnée de santé à caractère personnel a fait l'objet d'un traitement la rendant anonyme, tel qu'une agrégation, elle peut, et même doit pour P. BURNEL et F. VON LENNEP, être rendue publique et réutilisable. Revenons alors à l'objectif de ce développement qui est de savoir si, avec ces éléments en main, le ministre de la santé et des solidarités aurait pu décider d'interdire l'accès au SNIIRAM pour le secteur privé à but lucratif. La question qu'il aurait dû se poser est la suivante : l'accès sur autorisation préalable permet-il d'obtenir des données identifiantes ou réidentifiantes ? D'après la procédure prévue par le chapitre X de la loi relative à l'informatique et aux libertés[1532] alors en vigueur, la réponse aurait probablement été négative : en effet, la CNIL qui procède à la délivrance de l'autorisation d'accès s'assure que seules les données nécessaires au traitement prévu soient transmises et réutilisées (à l'exclusion du NIR, du nom et du prénom). En outre, il était d'ores et déjà prohibé d'utiliser les données de santé obtenues à des fins de recherche ou d'identification des personnes. La procédure d'accès sélectif aurait alors pu être ouverte aux acteurs privés à but lucratif.

527. Nous sommes conscients que tout le développement qui précède requiert une certaine imagination car tout cela reste de l'ordre de la conjecture. Avec le recul que nous avons aujourd'hui, nous savons que justifier la fermeture du SNIIRAM pour le secteur privé à but lucratif par la méconnaissance des conséquences des données ouvertes, n'est pas un argument recevable. En effet, dès lors qu'il y a une procédure d'accès préalable, on ne peut pas parler de

[1529] DEBOST C., « Publication du rapport sur la gouvernance et l'utilisation des données de santé, la promesse d'un entrebâillement de l'Open data dans le secteur de la santé ? », *RDS*, janvier 2014, n° 57, p. 947 à 949.

[1530] DESMARAIS P., « Open data santé, un rapport décevant pour un retard de transposition certain ? », *JCP A*, 08/09/2014, n° 36, 716.

[1531] LAUDE A., « Démocratie sanitaire, open data et Médiator », *JDSAM*, Chronique 2, Droits des malades et bioéthique, n° 1 de 2014, p. 58 à 61.

[1532] Loi n° 78-17 du 6 janvier 1978, *op. cit.,* modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.,* chap. X.

données ouvertes. C'est la mise à disposition proactive de données de santé anonymes et non réidentifiantes qui pourrait être classé dans la catégorie des données ouvertes. Dans le cas de l'accès sélectif au SNIIRAM il est nécessaire d'obtenir une autorisation en amont, nous ne pouvons donc pas assimiler ce mécanisme aux données ouvertes : cet état de fait parachève notre réflexion sur l'argument éventuel du manque de connaissances concernant le phénomène des données ouvertes pour interdire l'accès aux données de santé du SNIIRAM. Nous comprenons bien qu'il n'existe pas d'élément particulier qui appuie l'interdiction prévue par l'arrêté de 2005, ni dans les mois qui précèdent sa publication, ni dans les années qui l'ont suivie. Les principes applicables aux données ouvertes sont donc à écarter, il est possible qu'il n'en aille pas de même s'agissant des données massives.

Paragraphe 2 : L'inconnue des données massives, argument fragile du refus d'autorisation d'accès

528. Lors de la décision d'introduire l'interdiction d'accéder au SNIIRAM pour les acteurs privés à but lucratif dans l'arrêté de 2005[1533], les données massives[1534] n'en étaient qu'à l'aube de leur développement. Ce qui est désigné comme l'or du XXI[e] siècle[1535] a fait l'objet de nombreuses analyses destinées à comprendre si un équilibre peut être trouvé entre les opportunités promises par ce concept d'une part, et les risques qui en découlent d'autre part. A l'heure où nous écrivons ces lignes, nous savons que les questionnements relatifs au fonctionnement et aux conséquences des données massives étaient bien plus importants que les connaissances théoriques sur le sujet. C'est justement la méconnaissance de cette méthode de traitement des données qui a pu participer à convaincre le ministre de la santé et des solidarités de fermer l'accès au SNIIRAM pour le secteur privé à but lucratif. En effet, de façon similaire à ce que nous avons constaté s'agissant des données ouvertes[1536], les réflexions sur le sujet des données massives en santé, qu'elles proviennent de rapports officiels, d'avis émanant d'autorités diverses, ou d'ouvrages de doctrine, n'ont commencé à fleurir qu'à partir de 2013[1537]. Cette année-là, L. MARINO a d'ailleurs bien résumé le double visage des données

[1533] Arrêté du 20 juin 2005, *op. cit.*

[1534] Traduction proposée par la Commission générale de terminologie et de néologie de l'Académie française et inscrite au Journal officiel, texte n° 89, JORF n° 0193, 22/08/2014. Le texte les définit comme étant des « *Données structurées ou non dont le très grand volume requiert des outils d'analyse adaptés* ».

[1535] KALTENBACH L. et LE GUAY O., « Ces données personnelles qui valent de l'or », *JCP E*, 11/09/2014.

[1536] *Supra* n° 524.

[1537] MARINO L., « Le big data bouscule le droit », *Revue Lamy droit de l'immatériel*, 01/12/2013, n° 99, p. 55-58.

massives en prononçant cette phrase en ouverture du colloque « le big data bouscule le droit » : « *le big data c'est Dr Jekyll et Mr Hyde* »[1538], en d'autres termes, le concept offre de formidables opportunités d'un côté et présente des risques insoupçonnés de dérives menaçant le respect de la vie privée de l'autre.

Cette somme d'inconnues sur le sujet, bien trop nombreuses, notamment concernant les risques sur la vie privée des individus, a très probablement joué un rôle actif dans le contenu de l'arrêté de 2005[1539]. Il convient alors de s'interroger sur l'opportunité d'exclure les acteurs privés à but lucratif de l'accès au SNIIRAM sous couvert de l'insuffisance des connaissances relatives aux tenants et aboutissants des données massives. Nous allons constater que les risques imaginables au début des années 2000 ont été pour la plupart théorisés et vérifiés dans les années 2010 : toutefois, une solution différente de l'interdiction pure et simple d'accéder aux données de santé aurait dû être trouvée par le pouvoir réglementaire.

529. Si l'accès aux données de santé a été fermé aux acteurs privés à but lucratif, nous supposons que c'est à cause de la crainte de voir ceux-ci utiliser les informations récupérées afin de les traiter de façon systématique sans se soucier des problématiques de vie privée. Au début des années 2000, les autorités subodoraient déjà une suprématie du secteur privé à but lucratif dans la maîtrise de cette nouvelle technologie face aux acteurs publics et aux gestionnaires des bases de données administratives en santé. Cet état de fait a été vérifié au fil des années comme l'ont souligné A. MAZEAUD et G. GOURGUES dans un article paru en 2017[1540] : les auteurs constatent effectivement que les données massives « *rest*[ent] *pour l'instant principalement pris*[es] *en charge* [par] *les opérateurs privés* »[1541]. Ils considèrent que c'est avant tout l'éthique qui doit guider la régulation des données massives en matière de santé publique. Cette meilleure maîtrise d'une technologie nouvelle, porteuse de nouveaux risques sur les données était donc de nature à faire naître les craintes les plus importantes sur l'intégrité des données de santé, si celles-ci étaient mises à disposition des acteurs privés à but lucratif. Ces propos sont évidemment à nuancer car l'éthique a nécessairement une place importante dans l'activité des acteurs privés à but lucratif qui s'efforcent d'exercer leur activité en

[1538] *Ibid.*, p.55.

[1539] Arrêté du 20 juin 2005, *op. cit.*

[1540] GOURGUES G., MAZEAUD A., « Peut-on délibérer du Big Data en santé sans controverser ? Retour sur l'expérience d'un atelier citoyen français », *Revue française des affaires sociales*, 2017/4, p. 95-115.

[1541] *Ibid.*, p. 97.

maintenant une relation de confiance avec les individus. Surtout, si le secteur privé à but lucratif est susceptible de manquer à ce critère d'éthique, il ne faut pas oublier que les acteurs publics et les acteurs privés à but non lucratif ne sont pas infaillibles non plus et peuvent parfaitement être amenés à prendre des décisions contraires à l'éthique[1542].

530. Les publications relatives aux données massives en santé semblent d'ailleurs unanimes s'agissant du risque accru que le concept fait peser sur le respect de la vie privée. Dans leur rapport d'information au Sénat[1543], F. PILLET et G. GORCE soulignent que « *à plusieurs reprises au cours des auditions les intervenants ont jugé que les risques liés au « big data », c'est-à-dire à la collecte, au traitement et à la diffusion massifs des données personnelles par des entreprises privées étaient bien supérieurs à ceux suscités par l'open data* »[1544]. Un risque a principalement été cerné par les auteurs au fil des années pour être consacré comme le facteur le plus dangereux pour la vie privée des individus : il s'agit du risque de réidentification. Ce risque est bel et bien amplifié par la quantité de données traitables grâce aux données massives, comme le signale L. CLUZEL-METAYER, « *il suffit de croiser les informations pour qu'elles deviennent identifiantes* »[1545]. C. CASTETS-RENARD, quant à elle, souligne que l'accumulation « *d'informations sur les individus, la manipulation et l'agrégation des données sont sources de désanonymisation* »[1546]. Nous savons que si les acteurs privés à but lucratif avaient eu accès au SNIIRAM dès 2005, les données qui auraient été mises à leur disposition auraient nécessairement été traitées pour être anonymes. De plus, la loi relative à l'informatique et aux libertés interdisait spécifiquement, à son article 66[1547], de traiter les données de santé obtenues dans le cadre de l'accès sélectif à des fins de recherche ou d'identification des personnes. Toutefois, la maîtrise des données massives associée à une volonté d'enfreindre la loi (ce qui, nous en conviendrons, relève de l'exception), aurait pu conduire certains organismes privés à but lucratif à réidentifier des individus[1548]. C'est donc de ce risque, réel mais limité à

[1542] *Supra* n° 520.

[1543] GORCE G. et PILLET F., Rapport d'information au Sénat, *op. cit*.

[1544] *Ibid.*, p. 27.

[1545] CLUZEL-METAYER L., « Les limites de l'open data », *AJDA*, 25/01/2016, n° 2, p. 102-107.

[1546] CASTETS-RENARD C., « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data », *Revue Lamy de Droit de l'Immatériel*, 01/10/2014, supplément au n° 108, p. 38-45.

[1547] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*, art. 66.

[1548] A titre d'exemple, une opération de réidentification des individus pourrait être menée par une entreprise d'assurance pour parvenir à cibler ses clients et détecter des éléments relevant de la vie privée de ces individus susceptibles de justifier des modifications contractuelles telles qu'une hausse de la prime d'assurance ou une

quelques acteurs mal intentionnés, que pourrait découler l'interdiction d'accès qui a duré de 2005 à 2016.

531. Le risque de réidentification mis en exergue par les auteurs est-il pour autant de nature à justifier une telle interdiction ? Cela n'est pas si sûr. En effet, H. TANGHE et P.-O. GIBERT s'accordent à dire, dans une publication commune[1549], que se limiter à rendre accessibles les données de santé qui sont garantes d'un risque zéro de réidentification comporte une limite importante qui ôterait tout intérêt à la mise à disposition de données. En effet, la garantie du risque zéro de réidentification pourrait, à terme, conduire à « *appauvrir de manière excessive les jeux de données et à en réduire l'intérêt d'utilisation* » étant donné que « *l'état de l'art ne permet pas d'assurer une anonymisation fiable à 100%* »[1550]. En outre, les auteurs du rapport sur la protection des données personnelles remis au Sénat en 2014[1551] ont constaté que « *les dispositifs d'anonymisation utilisés ont été suffisamment robustes pour éviter toute diffusion accidentelle de données personnelles* »[1552]. Dès lors, nous pouvons en déduire, avec le recul que nous avons aujourd'hui, que l'interdiction imposée aux acteurs privés à but lucratif de bénéficier de l'accès sélectif n'aurait pas été justifiée par la seule existence d'un risque potentiel de réidentification.

532. A l'issue de ces observations, rappelons que les autorités françaises n'avaient pas, en 2005, les mêmes connaissances que nous avons aujourd'hui. Les enjeux des données massives étaient encore à explorer mais le risque de réidentification était probablement déjà dans tous les esprits. C'est donc à partir de l'absence de connaissances sur un sujet potentiellement à risque pour la vie privée des individus que le ministre de la santé et des solidarités a acté la mise à l'écart des organismes privés à but lucratif. C'est finalement l'option du risque zéro qui a été choisie, les autorités préférant un déséquilibre en faveur de la protection de la vie privée, plutôt que la recherche d'un juste milieu qui aurait permis aux acteurs privés à but lucratif d'accéder à des données du SNIIRAM sous le contrôle de la CNIL.

---

résiliation anticipée du contrat. Il faut avoir à l'esprit que la mise en œuvre d'un tel dispositif de réidentification requiert du matériel, du personnel et des compétences extrêmement spécifiques.

[1549] TANGHE H., GIBERT P.-O., « L'enjeu de l'anonymisation à l'heure du Big Data », *Revue française des affaires sociales*, 2017/4, p. 79-93.

[1550] *Ibid*., p. 11.

[1551] GORCE G. et PILLET F., Rapport d'information au Sénat, *op. cit*.

[1552] *Ibid*., p. 49.

533. Compte tenu des incertitudes et du contexte de fort développement technologique, nous pouvons conclure que les phénomènes des données ouvertes et des données massives ont eu une influence directe sur la décision d'exclure les organismes privés à but lucratif. Avec nos connaissances actuelles, nous savons que ces craintes, par anticipation, n'étaient pas toutes justifiées. Finalement, il importe peu que les raisons invoquées soient qualifiées de bonnes ou mauvaises, de justifiées ou de superfétatoires car tous les arguments invoqués ont contribué à construire le système d'accès aux données de santé ouvert aux acteurs privés à but lucratif qui existe aujourd'hui. L'objet de la prochaine section est donc d'analyser le contexte actuel qui permet d'ouvrir l'accès sélectif aux données de santé du SNIIRAM, devenu SNDS par la loi de modernisation de notre système de santé[1553], tout en signalant que certaines problématiques n'ont pas encore été résolues.

[1553] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

CONCLUSION DU CHAPITRE I

534. L'exclusion des acteurs privés à but lucratif du bénéfice de l'accès aux données de santé n'a été levée qu'avec l'entrée en vigueur de la réforme du 26 janvier 2016[1554]. Avant cela, l'interdiction totale d'accès dès l'arrêté de 2005[1555] présente un caractère arbitraire pourtant basé sur l'objectif louable de protéger le droit au respect de la vie privée des individus. Mais le raisonnement ayant conduit à cette mise à l'écart des entreprises est discutable. Effectivement, il semble que le pouvoir réglementaire est parti du principe que les acteurs privés à but lucratif seraient incapables de résister à la tentation de violer la protection des données de santé à caractère personnel. La sécurité des données obtenues serait donc, par principe, mieux assurée par les acteurs publics ou privés à but non lucratif. Cet argument est pourtant très difficile à défendre en pratique. Ainsi, sans chercher de solution qui permettrait de concilier un accès aux données avec la garantie de sécurité adéquate, c'est un principe d'interdiction qui a été créé et qui aura duré plus de 10 ans. Mais au-delà de cette crainte pour la sécurité des données, crainte légitime qui concerne tous ceux qui accèdent aux données de santé pour les traiter et pas seulement les acteurs privés à but lucratif, il est difficile de connaître les fondements de l'interdiction car celle-ci semble aller de soi. Aucun document préalable à l'arrêté de 2005[1556] n'explique concrètement le raisonnement suivi.

535. Ce ne sont pas non plus le développement des données ouvertes, ou celui des données massives qui conduisent à justifier l'exclusion du secteur privé à but lucratif de l'accès aux données de santé. Ces techniques, certes nouvelles au début des années 2000, sont accessibles à n'importe quel acteur traitant des données. Dès lors, aussi bien les bénéficiaires de l'accès permanent que ceux de l'accès sélectif ont l'opportunité de traiter les données obtenues en expérimentant de nouveaux types de traitements. Exclure uniquement les entreprises privées au motif que le développement des données ouvertes et des données massives leur permettrait notamment de réidentifier plus facilement les individus n'est donc pas justifiable. Finalement, c'est aujourd'hui une plus grande connaissance de ces techniques et des enjeux qui les entoure qui permet d'ouvrir l'accès aux données de santé aux acteurs privés à but lucratif dans un cadre défini et soumis à un contrôle important.

[1554] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1555] Arrêté du 20 juin 2005, *op. cit.*

[1556] *Ibid.*

CHAPITRE II
L'ACCÈS AUX DONNÉES DE SANTÉ AUTORISÉ DANS UN CONTEXTE FAVORABLE

536. La décennie de mise en œuvre de l'accès sélectif au SNIIRAM, excluant sciemment le secteur privé à but lucratif, a permis de mettre en exergue les faiblesses et fragilités du mécanisme. Un diagnostic a finalement été posé sur les limites à la décision prise dans l'arrêté du 20 juin 2005[1557] et le pouvoir réglementaire a refondu l'ensemble du système d'accès aux données de santé pour y intégrer les organismes privés à but lucratif[1558]. Il est donc important d'examiner en premier lieu comment le pouvoir réglementaire a été convaincu de changer de point de vue (Section 1), puis nous verrons que certaines solutions sont venues du droit de l'Union européenne, bien que toutes les problématiques n'aient pas encore été résolues (Section 2).

SECTION 1 : LES ARGUMENTS PROPICES À L'AUTORISATION D'ACCÈS

537. Les années qui ont suivi l'interdiction d'accès aux données du SNIIRAM pour les acteurs privés à but lucratif ont fait émerger des situations qui, après analyse, ont permis de comprendre que ce principe de non accès ne pouvait être durable. Il nous apparaît nécessaire de mettre en lumière les incohérences de l'interdiction d'accès dans la pratique (§1), avant de nous intéresser à l'apport de contre-arguments convaincants, favorables à l'ouverture des données pour les acteurs privés à but lucratif (§2).

Paragraphe 1 : L'autorisation d'accès favorisée par les incohérences de l'interdiction

538. Le fait de mettre à l'écart de l'accès aux données de santé dans le cadre de la recherche, toute une catégorie d'acteurs, en raison de leur but lucratif, a fait naître plusieurs situations inconfortables pour le pouvoir réglementaire et bien difficiles à justifier. Nous proposons de consacrer cette sous-partie à l'étude des cas les plus emblématiques en commençant par la solution que les acteurs privés à but lucratif ont trouvée pour pouvoir réaliser, indirectement,

[1557] Arrêté du 20 juin 2005, *op. cit.*

[1558] *Supra* n° 494 à 500.

des recherches utilisant les données de santé contenues dans le SNIIRAM. Nous l'avons évoqué dans le premier titre de la présente partie[1559], si les organismes privés à but lucratif n'ont pas eu la possibilité de déposer eux-mêmes des dossiers auprès de l'IDS, ils ont eu recours à « *l'intermédiation d'équipes de recherche publique* »[1560] notamment dans le secteur du médicament. Cette faculté de recourir à un acteur admis à obtenir des données de santé dans le cadre du chapitre X de la loi relative à l'informatique et libertés[1561], si elle existe et a été utilisée, relève plus de la cote mal taillée que de la solution viable dans la durée. En effet, les acteurs privés à but lucratif n'ont eu d'autre choix que de déléguer la réalisation de leurs recherches aux acteurs disposant du droit d'obtenir les données nécessaires.

Dans la pratique, il est certain que ce procédé ne devait pas être des plus simples à mettre en place. Une phase préparatoire devait nécessairement être réalisée pour contractualiser la prestation auprès du laboratoire public de recherche retenu et pour s'assurer que celui-ci ait bien toutes les informations à sa disposition pour demander les bonnes données, répondre à toutes les demandes potentielles de la CNIL et mener à terme le projet de recherche initié par l'acteur privé à but lucratif initial. Cette faculté ne permettait pas réellement de passer outre l'interdiction fixée dans le décret de 2005[1562] et reprise jusqu'à la réforme du 26 janvier 2016[1563]. L'objectif d'empêcher le secteur privé à but lucratif de récupérer des données de santé issues du SNIIRAM demeurait rempli : seuls les résultats de la recherche, une fois connus et publiés, leur étaient transmis. Pourtant, reconnaissons que ce système ne pouvait pas être satisfaisant bien que conforme aux dispositions légales et réglementaires en vigueur. Il comportait deux fortes contraintes que les bénéficiaires réels de l'accès sélectif d'alors n'avaient pas à subir : il s'agit de la contrainte du temps supplémentaire requis pour mettre en œuvre et contractualiser le projet de recherche d'une part, et de la contrainte du coût pécuniaire inévitable d'une telle mission déléguée à un prestataire tiers d'autre part. Etant interdits d'accès aux données du SNIIRAM, les acteurs privés à but lucratif ont longtemps été contraints de se résigner à recourir à cet accès sélectif par procuration. Le gouvernement français ne pouvait pas laisser prospérer cette situation qui plaçait les entreprises dans une situation très inconfortable,

[1559] *Supra* n° 468 à 473.

[1560] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 54.

[1561] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*

[1562] Arrêté du 20 juin 2005, *op. cit.*

[1563] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

nonobstant leur capacité potentielle à présenter toutes les garanties nécessaires à la sécurité des données de santé.

539. En parallèle de cette première incohérence inhérente à l'interdiction d'accès aux données de santé du SNIIRAM, un autre point attire notre attention par son caractère contradictoire : celui de la faculté offerte aux acteurs privés à but lucratif d'accéder aux données du PMSI[1564]. Effectivement, de 2005 à l'entrée en fonction du nouveau SNDS[1565], les entreprises ont été entièrement libres de demander à obtenir des données de santé liées à l'activité hospitalière. Ces données, tout aussi sensibles que les données de soins de ville contenues dans le SNIIRAM, étaient accessibles en suivant une procédure presque identique à celle qui concerne l'accès sélectif[1566], à ceci près que l'IDS n'était pas sollicité. Cet écart important qui existe dans la considération du secteur privé à but lucratif en fonction de la provenance des données de santé sollicitées est à peine soulevé par la Cour des comptes qui écrit, dans son rapport de 2016 que « *les organismes à but lucratif n'ont pas accès aux données du SNIIRAM, en vertu d'une interdiction générale posée par l'arrêté, alors qu'ils accèdent aux données du PMSI* »[1567]. De son côté, P.-L. BRAS admet que cette « *communication large des données du PMSI s'avèr*[e], *à l'expérience, porteus*[e] *d'une contradiction* »[1568]. C'est bel et bien le constat que nous faisons : nous avons admis[1569] que l'accès sélectif au SNIIRAM avait été interdit aux acteurs privés à but lucratif pour des raisons de sécurité au motif qu'un risque rémanent de réidentification existait. Si l'anonymisation des données contenues dans le SNIIRAM n'était pas assez sûre pour intégrer le secteur privé à but lucratif dans l'accès sélectif, comment se fait-il que, dans le même temps, la procédure d'accès aux données du PMSI ait été possible ? Si un risque a été détecté sur les données provenant d'une première base, pourquoi ce risque n'existe-t-il pas pour une seconde base qui contient des données tout aussi sensibles ? P.-L. BRAS pose le problème en ces termes : « *soit ces données sont indirectement nominatives et, dans ce cas,*

[1564] *Supra* n° 471.

[1565] Les premières demandes d'accès au SNDS ont pu être déposées à partir du 28 août 2017.

[1566] V. *supra* n° 323 à 328 pour la description du fonctionnement de l'accès sélectif avant la réforme du 26 janvier 2016.

[1567] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 54.

[1568] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.*, p. 57.

[1569] *Supra* n° 521.

l'accès peut paraître trop large ; soit l'accès aux données ne présente pas de risque de réidentification et dans ce cas l'accès aux données est trop restreint »[1570].

Ces questionnements pointent du doigt l'incertitude des autorités sur leur faculté à protéger les données de santé contenues dans les bases administratives[1571] : dans un cas, ces données semblent suffisamment protégées pour pouvoir être obtenues dans le respect des chapitres IX et/ou X de la loi relative à l'informatique et aux libertés[1572], dans l'autre, la protection qui leur est conférée est trop fragile pour laisser le secteur privé à but lucratif les solliciter dans une finalité de recherche. Il s'agit sans doute de l'incohérence la plus importante du système d'accès aux données de santé antérieur à la réforme du 26 janvier 2016[1573].

540. Le troisième élément de nature à apporter un sentiment d'instabilité dans le principe d'interdiction d'accès aux données de santé pour les acteurs privés à but lucratif est cette distinction qui existe entre les organismes à but non lucratif et les organismes à but lucratif. Le pouvoir réglementaire semble s'être appuyé sur cette dichotomie pour exclure la deuxième catégorie du dispositif d'accès, diffusant indirectement l'idée selon laquelle les acteurs à but lucratif sont irrémédiablement amenés à violer le droit au respect de la vie privée des individus. Cette hypothèse, dont nous avons déjà questionné[1574] la légitimité, n'est pourtant pas le seul critère de choix pour permettre aux acteurs d'accéder aux données de santé. Sinon, comment justifier que des entreprises d'assurance, organismes privés à but lucratif, aient pu bénéficier d'un accès permanent dès 2011 au même titre que les institutions de prévoyance et les mutuelles qui sont des organismes privés mais à but non lucratif ? Si les autorités s'étaient uniquement basées sur le critère de sélection « but lucratif / but non lucratif », ils n'auraient pas pu intégrer les entreprises d'assurance dans le mécanisme d'accès aux données de santé. Nous comprenons bien que d'autres critères entrent nécessairement en ligne de compte comme l'activité ou la mission de l'organisme privé à but lucratif : en l'occurrence c'est la mission de gérer les remboursements de soins complémentaires des individus assurés. Cette zone d'ombre a notamment été signalée par le rapport BRAS qui indique que « *aucun critère ferme* [ne] *définit*

[1570] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 57.

[1571] *Supra* n° 521 à 535.

[1572] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par la loi n° 2004-801 du 6 août 2004, *op. cit.*, chap. IX et X.

[1573] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1574] *Supra* n° 518 à 522.

les contours [des acteurs autorisés à accéder au SNIIRAM, ce qui] *ne peut que nourrir chez ceux qui en sont exclus le sentiment que des données publiques sont confinées sans raisons impérieuses de sécurité* »[1575]. Le fait que l'exclusion des acteurs privés à but lucratif fermement prévue par arrêté s'accompagne d'exceptions pour certains d'entre eux qui se sont vu attribuer un droit d'accès permanent affaiblit grandement l'argument du ministre de la santé et des solidarités et le rend d'autant plus difficile à défendre.

541. Compte-tenu de ces points de contexte, il est évident que la possibilité de déposer une demande d'accès à des données de santé provenant des bases de données de l'assurance maladie ne pouvait plus être interdit au secteur privé à but lucratif sans la preuve d'une argumentation solide. Cette dernière étant absente, la réforme en profondeur du mécanisme était inévitable, d'autant plus que les arguments favorables à une ouverture de l'accès au bénéfice des acteurs privés à but lucratif se sont vite multipliés.

Paragraphe 2 : L'autorisation d'accès favorisée par des contre-arguments convaincants

542. Le début des années 2010 marque un tournant dans les réflexions relatives au système d'accès aux données de santé. La mise au jour de l'affaire sanitaire du Mediator[1576] par I. FRACHON en 2010 semble être l'un des éléments déclencheurs des questionnements qui ont conduit le pouvoir législatif et réglementaire à changer de point de vue et à faire évoluer les données de santé vers une plus grande ouverture. En effet, les questions posées par les révélations de cette affaire, notamment sur l'utilisation insuffisante, ou inadéquate, des données de santé disponibles par les acteurs disposant d'un accès permanent ou sélectif, ont conduit à s'interroger sur la légitimité des arguments avancés par le pouvoir réglementaire pour fermer les bases de données de santé, notamment celle du SNIIRAM. Ainsi, dans une entrevue publiée dans le journal Le Monde en 2013[1577], D. SICARD, président du comité consultatif national d'éthique de 1999 à 2008, devenu ensuite son président d'honneur, affirmait que « *les résistances à l'Open data en santé trouvent, de façon évidente, leur origine dans la volonté de maintenir l'illusion que la santé des français est gérée avec rigueur et discernement* ». Ce

[1575] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.*, p. 57.

[1576] *Supra* n° 2, 149 et 186.

[1577] SICARD D. in *Le Monde*, 07/10/2013.

sentiment d'illusion était d'autant plus prégnant que l'affaire du Mediator a révélé une maîtrise inaboutie des bases de données de santé. Les différents travaux menés ont également été influencés par la nécessité de transposer, dans les meilleurs délais, la nouvelle directive européenne mettant à jour les dispositions communes en matière de réutilisation des informations du secteur public[1578]. Ces raisonnements dépassent bien entendu le seul cadre de l'accès aux données pour les acteurs privés à but lucratif : ils ont même, plus généralement, une approche centrée sur la revendication de données ouvertes en santé. Cependant, les contre-arguments développés nous intéressent fortement car ils ont indéniablement eu une résonance et un impact particuliers concernant l'accès des acteurs privés à but lucratif aux données de santé.

543. Souvenons-nous que la principale justification à l'interdiction d'accès aux données de santé pour le secteur privé à but lucratif réside dans l'existence d'un risque sur la sécurité des données[1579] qui pourraient être traitées pour devenir réidentifiantes et permettre d'attenter au respect du droit au respect de la vie privée des individus. Au motif qu'un tel risque existe (car il existe encore aujourd'hui), les données de santé du SNIIRAM étaient entièrement inaccessibles, aussi bien aux acteurs privés à but lucratif, qu'au grand public. Il était donc nécessaire que les données présentent un risque zéro de réidentification pour être sollicitées par des acteurs privés à but lucratif ou par des citoyens. Or, des études et rapports ont parfaitement montré que, d'une part, la sécurité des bases de données ne pouvait pas être entièrement à l'abri d'une attaque informatique menée par des *hackers*[1580] ; et que, d'autre part, le risque zéro de réidentification n'existe pas car les techniques d'anonymisation des données ne sont pas infaillibles[1581]. Le fondement même de l'interdiction d'accès a donc volé en éclats en l'espace de quelques années. Il ne faut cependant pas imaginer que les auteurs ayant signalé les limites de l'exclusion des acteurs privés à but lucratif aient pour autant pris position pour une ouverture

[1578] Directive 2013/37/UE du 26 juin 2013 *modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public*.

[1579] *Supra* n° 518 à 522.

[1580] MESSI P., « Big Brother : la surveillance de la population », *Les Tribunes de la santé*, 2010/4, n° 29, p. 71 à 73. A titre d'exemple, un hôpital situé en Californie, le Hollywood Presbyterian Medical Center, a fait l'objet d'un piratage qui a paralysé l'ensemble de son système informatique, mettant notamment toutes les données de santé contenues dans ledit système en péril. Les hackers auraient demandé plus de 3 millions de dollars de rançon pour libérer le système, sans aucune garantie que les données ne seraient pas dupliquées ; v. LOUIS J.-P., « Des hackers prennent en otage le système informatique d'un hôpital », *Les Echos*, 17/02/2016.

[1581] GORCE G. et PILLET F., Rapport d'information au Sénat, *op. cit.*, p. 46 à 49.

incontrôlée des bases de données. Au contraire, un document comme le rapport BRAS[1582] dénonçait, en 2013, la prudence excessive dans la mise à disposition des données de santé et proposait de résoudre ce blocage en mettant en œuvre une « *expertise systématique et publique sur les risques de réidentification* » afin de savoir quelles données peuvent être diffusées à un public large, en données ouvertes par exemple, et quelles données ne doivent être rendues accessibles qu'à la suite d'une procédure d'accès sélectif. Nous pouvons signaler que d'autres voix, plus politiques, se sont élevées en faveur de l'accès des acteurs privés à but lucratif aux données de santé. Tel est le cas de la ministre déléguée chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique, F. PELLERIN, qui déclarait en 2013, d'après des propos rapportés par C. DEBOST, que « *plus nos startups (…) peuvent accéder à des données différentes et riches, plus elles pourront imaginer des applications nouvelles et utiles pour les gens* »[1583]. Malgré le risque de paraître légèrement excessif, nous pouvons considérer qu'au cours des années qui ont précédé la réforme 26 janvier 2016[1584], les acteurs privés à but lucratif semblent être passés du statut de *persona non grata* de l'accès aux données de santé à celui de chaînon indispensable à l'optimisation de l'utilisation des données récoltées. Il est avéré que l'intégration des acteurs privés à but lucratif dans l'accès sélectif est le fruit d'une volonté politique certaine de mettre fin à plusieurs années d'exclusion sans véritable argument juridique tenable.

544. En complément de ces contre-arguments qui ont su convaincre les pouvoirs réglementaire et législatif, le droit européen est intervenu pour contraindre des Etats européens à agir en faveur de l'ouverture des données incluant les acteurs privés à but lucratif. En effet, la directive européenne[1585] évoquée au début des présents développements a radicalement inversé le principe de mise à disposition des données publiques. Son considérant n° 8 modifie la directive 2003/98/CE[1586] pour « *imposer aux Etats membres une obligation claire de rendre tous les documents réutilisables* ». Les observateurs argueront de l'existence d'exceptions à cette obligation qui concernent directement les données de santé à caractère personnel. L'article 1er,

[1582] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit*., p. 58.

[1583] PELLERIN F., discours de clôture du 4e concours dataprotections, *in* DEBOST C., « Publication du rapport sur la gouvernance et l'utilisation des données de santé, la promesse d'un entrebâillement de l'Open data dans le secteur de la santé ? », *op. cit.*, p. 2.

[1584] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1585] Directive 2013/37/UE du 26 juin *op. cit*.

[1586] Directive 2003/98/CE, *op. cit*.

c quater de la directive précise ainsi que ladite directive ne s'applique pas « *aux documents dont l'accès est exclu ou limité en application des règles d'accès pour des motifs de protection des données à caractère personnel* »[1587]. Cependant, comme nous l'avons analysé précédemment[1588], les données de santé proposées dans le cadre de l'accès sélectif sont censées avoir perdu leur caractère personnel en raison du traitement préalable dont elles font l'objet pour, par exemple, être présentées sous forme de données agrégées, ou bien d'échantillons anonymisés : elles devraient alors être accessibles aux acteurs dont le projet entre dans le cadre défini par la législation nationale. Les autorités françaises étaient donc fortement incitées à trouver une solution pour repenser le système d'accès aux données de santé : l'obligation de transposer la directive a abouti à l'adoption de la loi du 28 décembre 2015[1589]. Bien que le contenu de cette directive soit intrinsèquement lié aux données ouvertes (données traitées à l'initiative du gestionnaire de base de données pour les anonymiser et les mettre à disposition de tous) sans procédure d'accès préalable, et ne concerne pas directement les données de santé proposées dans le cadre d'un accès sélectif (données potentiellement identifiantes, traitées selon les demandes d'accès, au cas par cas, pour devenir non réidentifiantes), son esprit est favorable à l'intégration des acteurs privés à but lucratif dans la procédure d'accès sélectif. Dès lors, nous comprenons que le contexte législatif, réglementaire et politique a évolué dans les années 2010 pour devenir plus favorable au secteur privé à but lucratif sans pour autant perdre en sévérité s'agissant des garanties à apporter en matière de sécurité des données traitées[1590].

545. Tous ces éléments combinés ont contribué à sonner le glas de l'exclusion des acteurs privés à but lucratif de l'accès sélectif aux données de santé. Les incohérences identifiées de cette exclusion et la naissance de contre-arguments convaincants ont permis d'apaiser les craintes liées aux risques pesant sur la protection de la vie privée des individus par la délivrance de garanties suffisantes sur le contrôle des acteurs privés à but lucratif.

[1587] Directive 2013/37/UE du 26 juin *op. cit*., art. 1er, c quater.

[1588] *Supra* n° 397.

[1589] Loi n° 2015-1779 du 28 décembre 2015 *relative à la gratuité et aux modalités de la réutilisation des informations du secteur public*, JORF n° 0301, 29/12/2015.

[1590] *Supra* n° 496 à 498.

SECTION 2 : LES GARANTIES BIENVENUES MAIS INCOMPLÈTES DE L'AUTORISATION D'ACCÈS

546. L'adoption de la réforme créant le SNDS[1591] et incluant les acteurs privés à but lucratif dans l'accès sélectif aux données de santé a été suivie de près par une nouvelle norme européenne hautement importante : le Règlement général relatif à la protection des données, ou RGPD[1592]. Le contenu de ce Règlement, entré en vigueur le 25 mai 2018, et menant à une adaptation du droit français[1593], donne des garanties supplémentaires au traitement des données de santé issues du SNDS par le secteur privé à but lucratif (§2). Toutefois, l'effectivité de l'accès des acteurs privés à but lucratif reste à confirmer en premier lieu, après quelques mois de fonctionnement, et toutes les subtilités de l'accès sélectif n'ont pas encore été explicitées (§1).

[1591] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1592] Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*. ALIX P., « Le DPO et le secteur de la communication », *LEGICOM*, n° 59, 2017/2, p. 115-122 ; BENOÎT-ROHMER F., « Chronique Union européenne et droits fondamentaux – L'adoption de mesures visant à renforcer la protection des données personnelles », *RTD Eur*., 2017, p. 355 ; BOTCHORICHVILI N., « Transferts de données personnelles hors de l'Union européenne – quelles nouveautés avec le RGPD ? », *LEGICOM*, n° 59, 2017/2, p. 39-46 ; BOUNEDJOUM A., SIMON F.-L., « RGPD : quelles nouvelles règles en matière de responsabilité et quels impacts sur les contrats ? », *AJ Contrat*, 2018, p. 172 ; BRINGAUD R., « Les mutations de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés au nouvelles exigences communautaires de traitement des données personnelles en matière de santé », *RDS*, n° 82, 2018, p. 267-268 ; CANTERO I., « Quel cadre pour le transfert des données personnelles hors de l'Union européenne ? », *Juris tourisme*, n° 207, 2018, p. 33 ; CHALTIEL F., « Le règlement général européen sur la protection des données », *Revue de l'Union européenne*, 2018, p. 249 ; CHASSANG Gauthier, « E-santé, droit de l'union européenne et protection de la vie privée des personnes : vers l'émergence d'un « technodroit » spécifique au travers de la proposition de règlement général sur la protection des données personnelles ? », *Revue Lamy de Droit de l'Immatériel*, 01/10/2014, supplément au n° 108, p. 46-56 ; EL BOUJEMAOUI W., MAZARS M.-F., « Maîtriser le socle du droit de la protection des données pour aborder l'application du Règlement européen (RGPD) », *Revue droit du travail*, 2018, p. 298 ; EYNARD J., « Une application systématique du RGPD ? », *Juris tourisme*, n° 207, 2018, p. 19 ; FAVRO K., « La démarche de *compliance* ou la mise en œuvre d'une approche inversée », *LEGICOM*, n° 59, 2017/2, p. 21-28 ; GOLA R., « Le Règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *LEGICOM*, n° 59, 2017/2, p. 29-38 ; GRIT M., « Focus sur le règlement européen relatif à la protection des données à caractère personnel », *RDS*, n° 83, 2018, p. 340-341 ; LANGLET V., « Nom de code : délégué à la protection des données », *Juris tourisme*, n° 207, 2018, p. 29 ; LE ROY M., ZOLYNSKI C., « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *LEGICOM*, n° 59, 2017/2, p. 105-113 ; MACIEL-HIBBARD M., « Protection des données personnelles et cyber(in)sécurité », *Politique étrangère*, 2018/2 (Eté), p. 55-66 ; MALLET-POUJOL N., « Protection des données personnelles et droit à l'information », *LEGICOM*, n° 59, 2017/2, p. 49-59 ; MARINO L., « Le règlement européen sur la protection des données personnelles : une révolution ! » (PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 2016), *JCP-G*, 30/05/2016, n° 22, p. 628 ; PASTOR J.-M., « Les nouvelles règles de protection des données personnelles », *AJDA*, 2018, p. 945.

[1593] Loi n° 2018-493 du 20 juin 2018 *relative à la protection des données personnelles*, JORF, n° 0141, 21/06/2018.

Paragraphe 1 : L'autorisation d'accès fonctionnelle mais imparfaite

547. Depuis l'année 2016, les acteurs privés à but lucratif sont admis à accéder aux données de santé du SNIIRAM élargi via le nouveau SNDS. Cette nouvelle faculté a été reconnue par la loi[1594] pour que, peu de temps après, le juge administratif déclare infondée[1595] juridiquement l'insertion du principe d'interdiction d'accès aux données de santé dans les arrêtés relatifs au fonctionnement du SNIIRAM parus entre 2005[1596] et 2013[1597]. L'entrée en vigueur du nouveau système, accompagnée du nouveau cadre européen fixé par le Règlement général relatif à la protection des données[1598] encadre entièrement le processus d'accès sélectif des acteurs privés à but lucratif afin de prévenir et d'éviter toute violation du droit au respect de la vie privée. Ainsi, il est intéressant de connaître les caractéristiques des demandes effectuées par les acteurs privés à but lucratif dans le cadre du nouvel accès sélectif pendant les 8 premiers mois d'activité du dispositif (A). Dans le même temps, des accès simplifiés censés répondre aux demandes les plus courantes sont encore en construction, ce qui montre que l'accès sélectif au bénéfice des acteurs privés but lucratif n'a pas encore atteint son plein potentiel (B).

A) L'accès sélectif classique opérationnel

548. Les premiers dépôts de dossiers auprès de l'INDS ont eu lieu en septembre 2017 et l'Institut a publié un bilan de son activité au début du mois de juin 2018[1599]. Nous allons le constater rapidement, si les acteurs privés à but lucratif ont eu plusieurs dossiers acceptés, certaines particularités ne manquent pas de surprendre. Avant toute chose il convient de savoir combien de dossiers de demandes d'accès au SNDS ou à l'une de ses composantes, comme

[1594] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*, et *supra* n° 494 à 500.

[1595] Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, recueil Lebon, Celtipharm, et *supra* n° 501 à 504.

[1596] Arrêté du 20 juin 2005, op. cit.

[1597] Arrêté du 19 juillet 2013 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, JORF n° 0187, 13/08/2013.

[1598] Règlement 2016/679, *op. cit.*

[1599] Depuis lors, le tableau de suivi des dossiers déposés peut être téléchargé à tout moment sur le site de l'INDS.

l'EGB[1600], le PMSI[1601] ou le CépiDC[1602], ont été traités par l'INDS. Tous types d'acteurs confondus (publics, privés à but non lucratif, privés à but lucratif), nous recensons 122 dossiers déposés au total : sur ces 122 dossiers, seulement 33 d'entre eux avaient reçu, début juin 2018, une autorisation de mener à terme le projet de recherche dans le domaine de la santé en obtenant les données de santé sollicitées. Ce nombre peut paraître faible : il est probable que plusieurs dossiers déposés en mai n'aient pas encore été examinés, soit par le CEREES, soit par la CNIL. Sur ces 122 dossiers, le nombre d'autorisations pourrait donc, *in fine,* être plus élevé. Parmi tous ces dossiers, nous en comptons 62 qui proviennent de responsables de traitement qui sont des acteurs privés. Seulement 10 d'entre eux sont à l'initiative d'acteurs privés à but non lucratif dans lesquels nous intégrons deux acteurs non identifiés que l'INDS classe dans une catégorie « *Autres* »[1603]. Puis 52 demandes ont été déposées par des acteurs privés à but lucratif. Les industriels de la santé sont en première place avec 35 dossiers déposés par leurs soins. Viennent ensuite les bureaux d'étude qui ont sollicité l'accès aux données de santé du SNDS à 14 reprises. Puis une clinique, une université ou école, et un média, ont chacun déposé un dossier auprès de l'INDS.

549. La première remarque que nous pouvons formuler concerne la proportion du nombre de demandes provenant du secteur privé à but lucratif qui est proche de 43% sur l'ensemble des dossiers traités. Cette donnée importante vient confirmer le fait que l'ouverture de l'accès sélectif était très attendue et particulièrement nécessaire aux besoins des industriels de santé et des bureaux d'études. Ce qui nous permet aussi d'attester que le nouveau système est fonctionnel et donne l'opportunité à tous les acteurs privés à but lucratif d'obtenir une autorisation après examen de leur dossier, c'est la proportion de dossiers acceptés par la CNIL : entre septembre 2017 et juin 2018, sur les 62 dossiers déposés par le secteur privé (à but lucratif ou non), seulement 19 autorisations avaient été délivrées (elles étaient 33 si l'on inclut aussi celles qui concernaient le secteur public) et 12 d'entre elles concernaient une demande faite par

[1600] L'EGB est l'échantillon généraliste des bénéficiaires, constitué depuis 2005, au 1/97e de la population couverte par l'assurance maladie. Il est constitué directement à partir des données contenues dans le SNIIRAM.

[1601] Le PMSI est le programme de médicalisation des systèmes d'information qui regroupe les données de santé relatives à l'hospitalisation. Il est mis en œuvre par l'ATIH : l'agence technique de l'information sur l'hospitalisation.

[1602] Le CépiDC est le centre d'épidémiologie sur les causes médicales de décès qui est mis en œuvre par l'Inserm : l'institut national de la santé et de la recherche médicale.

[1603] Les acteurs privés à but non lucratif qui ont déposé un dossier à l'INDS entre septembre 2017 et début juin 2018, sont : 5 associations dites « loi 1901 », 2 centres de lutte contre le cancer, 1 établissement public à caractère scientifique et technologique (EPST).

un industriel de la santé. Ainsi les entreprises de la santé ont obtenu 63% des autorisations visant le secteur privé, et 36% du total des autorisations accordées par la CNIL, tous organismes confondus. Cette réalité est très encourageante et démontre, par les faits, que l'accès sélectif au SNDS fonctionne.

550. La seconde remarque a trait aux modalités de réalisation des traitements déposés par les industriels de santé ainsi que des autres acteurs privés à but lucratif. Nous avons vu précédemment[1604] que d'après l'article L. 1461-3, II du code de la santé publique, pour qu'une entreprise privée produisant ou commercialisant des produits à finalité sanitaire destinés à l'homme et à finalité cosmétique[1605], une entreprise de crédit, un organisme assureur ou un intermédiaire d'assurance obtienne une autorisation d'accès aux données de santé, il est tenu, soit de démontrer que le traitement mis en œuvre empêche toute utilisation des données pour l'une des deux finalités interdites[1606] ; soit de faire appel à un laboratoire de recherche ou un bureau d'études, qu'il soit public ou privé, pour réaliser le traitement. Les 35 industriels de la santé ont tous, sans exception, choisi la deuxième solution, estimant probablement que la première présente un risque trop élevé de faire émerger un motif de refus lors de l'examen du dossier par la CNIL. Ainsi 26 entreprises ont décidé de solliciter un bureau d'études privé, 4 ont chargé un Centre Hospitalier Universitaire (CHU) de mener la recherche, 3 ont délégué cette mission à l'INSERM-CNRS, 1 à un Centre de Lutte Contre le Cancer (CLCC) et 1 à un laboratoire d'école ou d'université. Cette procédure a tout l'air d'être le miroir du chemin de traverse que devaient emprunter les acteurs privés à but lucratif avant la réforme[1607] pour pouvoir réaliser des recherches à partir de données de santé provenant du SNIIRAM. Si tous les acteurs privés à but lucratif ne sont pas concernés par cet état de fait (les bureaux d'études sont, par exemple, libres de réaliser le traitement de données de santé eux-mêmes), nous voyons bien que l'impact du dispositif est important dans la pratique au regard du volume de dossiers déposés par les industriels de la santé qui représentent 74% de l'ensemble des demandes d'accès effectuées par le secteur privé à but lucratif. Souvenons-nous que la solution de passer par un

[1604] *Supra* n° 497.

[1605] L'article L. 5311-1 du code de la santé publique dresse une liste non exhaustive des types de produits concernés parmi lesquels nous trouvons aussi des médicaments, des produits sanguins labiles, des lentilles oculaires correctrices, des produits de tatouage, ou encore des logiciels d'aide à la prescription et à la dispensation.

[1606] Les finalités interdites sont précisées au V de l'article L. 1461-1 du code de la santé publique : il s'agit, d'une part, de la promotion des produits à finalité sanitaire destinée à l'homme et à finalité cosmétique et, d'autre part, de l'exclusion de garanties de contrats d'assurance et de modifications de cotisations ou de primes d'assurances d'une personne ou d'un groupe de personnes présentant le même risque.

[1607] Il s'agit de ce que nous avons désigné par les termes « accès sélectif par procuration » *supra* n° 468 à 473.

organisme tiers pour lui faire mettre en œuvre un traitement de données de santé à caractère personnel issues du SNIIRAM était considérée comme un contournement aussi bien par l'IDS[1608] que par la Cour des comptes[1609].

Plutôt que de s'affranchir de ce mode de fonctionnement, le législateur a considéré qu'il s'agissait là d'un moyen de garantir que des entreprises telles que des organismes assureurs ou des laboratoires pharmaceutiques ne procèdent pas au traitement des données obtenues pour l'une des finalités spécifiquement prévues par la loi. Cette situation est paradoxale car nous avons identifié[1610] l'existence d'inconvénients inhérents à ce mécanisme d'accès sélectif par procuration. Cependant, ces inconvénients, qui peuvent avoir pour conséquence d'alourdir la procédure d'accès au SNDS, semblent moins effrayer les acteurs privés à but lucratif concernés que les répercussions possibles de l'alternative proposée par l'article L. 1461-3, II, du code de la santé publique. En effet, si les organismes privés à but lucratif que sont les industriels de la santé décident de ne pas faire appel à un bureau d'étude et de réaliser le traitement des données de santé obtenues eux-mêmes, ils doivent arriver à convaincre l'INDS, le CEREES et la CNIL que le traitement envisagé ne pourra en aucune manière permettre de poursuivre l'une des finalités interdites par l'article L. 1461-1, V, du code de la santé publique. Or, plus de 8 mois après l'entrée en vigueur du nouvel accès au SNDS, personne ne sait réellement quels sont les critères qui permettent de donner une telle garantie. Mais il est évident que bâtir un dossier de demande d'accès aux données de santé est coûteux en temps et en argent. Il semble logique que, compte tenu du manque total d'informations sur les critères à remplir pour prouver que le traitement de données envisagé empêche toute utilisation pour l'une des finalités interdites par la loi, les acteurs privés à but lucratif ne déposent pas de dossier sur ce fondement : ils refusent de prendre le risque de se voir opposer un refus de la part de la CNIL et préfèrent opter pour la sécurité en sollicitant un bureau d'études tiers. Il nous semble donc primordial qu'un document, tel qu'un référentiel, comme il en existe pour les bureaux d'études et les laboratoires de recherche[1611], soit officiellement publié afin de donner aux organismes qui voudraient avoir

[1608] Institut des données de santé, « Enjeux et étapes », *Rapport au Parlement, op. cit.*, p. 18.

[1609] Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *op. cit.*, p. 54.

[1610] *Supra* n° 538.

[1611] L'article L. 1461-3, II, du code de la santé publique indique que les « *responsables des laboratoires de recherche et des bureaux d'études présentent à la Commission nationale de l'informatique et des libertés un engagement de conformité à un référentiel incluant les critères de confidentialité, d'expertise et d'indépendance, arrêté par le ministre chargé de la santé, pris après avis de la même commission* ». Ce référentiel a été publié par 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*, JORF n° 0172, 25/07/2017.

recours à cette alternative. Le choix laissé aux organismes privés à but lucratif les plus demandeurs de données de santé que sont les industriels de la santé ressemble donc à un sens unique. Le système prévu par la loi incite donc fortement ces acteurs privés à but lucratif à déléguer la mise en œuvre du traitement ce qui dénature, de fait, le principe de choix prévu par le texte de loi.

B) Les accès simplifiés encore en phase de développement

551. L'accès aux données de santé médico-administratives du SNDS peut se faire par les canaux classiques, c'est-à-dire en passant par la procédure d'accès sélectif. Mais nous savons que des accès simplifiés ont aussi été pensés notamment pour éviter d'engorger le guichet unique. Qu'en est-il du développement de ces accès simplifiés au bénéfice des acteurs privés à but lucratif ? Rappelons que les accès simplifiés ont pour objectif principal de permettre aux bénéficiaires de l'accès sélectif d'obtenir facilement et rapidement des données au moyen d'une procédure spécifique et prédéterminée par les autorités. Comme nous l'avons étudié dans la deuxième partie de cette étude[1612] dédiée aux acteurs publics ordinaires et aux acteurs privés à but non lucratif, seuls deux accès simplifiés étaient véritablement opérationnels à la fin de l'année 2018 : le mécanisme des méthodologies de référence d'une part, la demande d'accès à l'EGB[1613] d'autre part. Ces deux catégories d'accès simplifié sont également ouvertes aux acteurs privés à but lucratif. Signalons de prime abord que leur mise en place tardive au quatrième trimestre 2018 est le signe que l'accès sélectif pour le secteur privé à but lucratif est en pleine construction : les premiers mois de pratique des accès simplifiés opérationnels pourraient encore donner lieu à des modifications pour corriger des dysfonctionnements ou pour élargir la palette d'opportunités.

552. Examinons en premier lieu la procédure d'accès à l'EGB. Elle a été homologuée par une délibération de la CNIL datée du 12 avril 2018[1614], mais elle n'a véritablement été mise en avant qu'au cours du mois de juillet de la même année. L'homologation permet à un demandeur

[1612] *Supra* n° 420 à 427.

[1613] Pour rappel, l'EGB est l'échantillon généraliste des bénéficiaires du système national inter-régimes de l'Assurance maladie (SNIIRAM), composante du système national des données de santé (SNDS).

[1614] Délibération n° 2018-134 du 12 avril 2018 portant homologation de conditions de mise à disposition de l'échantillon généraliste des bénéficiaires (EGB) et des bases de données thématiques appelées « datamarts » du Système National d'Information Inter Régimes de l'Assurance Maladie (SNIIRAM).

d'obtenir un accès à l'EGB et/ou aux datamarts[1615] et tableaux de bord du SNIIRAM dans le cadre d'une recherche en santé, présentant un caractère d'intérêt public, et ne nécessitant pas d'autres données pour être menée. C'est l'INDS qui est chargé d'examiner les demandes d'accès simplifié à l'EGB. Les traitements envisagés à partir des données obtenues doivent respecter trois caractéristiques impératives : ils doivent être réalisés au sein du portail sécurisé de la CNAM ; ils ne doivent croiser aucun identifiant potentiel ; ils ne doivent pas accéder au portail plus de 24 mois. Partant de là, l'INDS se prononce à partir des critères précisés par la délibération de la CNIL tels que la finalité d'intérêt public de la recherche, la justification de la pertinence scientifique du projet, la durée du traitement, le respect des règles applicables au SNDS et notamment du référentiel de sécurité[1616] défini en 2017. La décision de l'INDS intervient dans les 15 jours ouvrés à partir de la réception du dossier complet : en cas de silence, la demande est réputée acceptée. En revanche, si le dossier est refusé, l'INDS peut, après acceptation du responsable du traitement, le transmettre au CEREES afin de poursuivre la procédure classique d'accès sélectif. Si nous développons, ici, ce type d'accès simplifié, c'est en raison de la nature des acteurs qui s'en sont servi en 2018. Effectivement d'après le relevé d'activité mis à disposition, fin novembre 2018 par l'INDS, seulement deux demandes d'accès à l'EGB ont été déposées en septembre et autorisées en octobre, et elles proviennent d'industriels de santé qui sont des acteurs privés à but lucratif. Cela démontre l'intérêt de ce dispositif pour les industriels : il est probable que cet accès simplifié monte rapidement en charge et permette à de nombreuses recherches en santé d'être menées sans passer par l'autorisation de la CNIL. Un recours fréquent à ce type d'accès est une bonne nouvelle car ce n'est qu'avec un grand nombre d'utilisations que les demandeurs de données de santé et les acteurs du SNDS pourront perfectionner le dispositif.

553. En second lieu, l'autre accès simplifié que peuvent déjà utiliser les acteurs privés à but lucratif est la déclaration de conformité à une méthodologie de référence. Cependant, une seule méthodologie de référence est disponible pour de tels acteurs : c'est la numéro MR-006[1617]. De

[1615] Les datamarts sont les bases thématiques de données agrégées orientées soit vers les dépenses (base DAMIR, ou Dépenses d'assurance maladie inter-régimes) ou vers l'analyse de l'offre de soins (base AMOS, ou Assurance maladie offre de soins).

[1616] Arrêté du 22 mars 2017 *relatif au référentiel de sécurité applicable au Système national des données de santé*, JORF, n° 0071 du 24/03/2017.

[1617] Délibération n° 2018-257 du 7 juin 2018 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 dispositions par l'ATIH par l'intermédiaire d'une solution sécurisée (MR-006).

plus, deux limites conséquentes sont prévues. La première de ces limites a trait à la nature des acteurs qui peuvent se prévaloir de cette méthodologie de référence. Seuls les acteurs qui produisent ou commercialisent des produits à finalité sanitaire destinés à l'homme et des produits à finalité cosmétique[1618] sont admis à en bénéficier. Cela exclut d'emblée toutes les entreprises qui font de la recherche mais qui n'ont pas ce type d'activité. La seconde limite vise la nature des données qui peuvent être sollicitées dans le cadre de cette procédure simplifiée. Seules les données issues du PMSI sont accessibles par ce biais. Connaissant cela, entre le mois d'août et le mois de novembre 2018, 17 déclarations de conformité à la méthodologie de référence ont tout de même été enregistrées par l'INDS : 16 proviennent d'un industriel de santé tandis qu'une seul est issue d'une organisation de recherche clinique par contrat (CRO). Bien entendu, le bénéfice de cette méthodologie est conditionné au respect de normes de sécurité très strictes afin de prévenir toute violation du droit au respect de la vie privée des individus. Les règles fixées par les référentiels homologués[1619] par la CNIL doivent nécessairement être appliquées. Par ailleurs, le responsable du traitement qui a recours à la méthodologie de référence MR-006 a interdiction de traiter lui-même les données obtenues : il est obligé de contracter avec un sous-traitant habilité tel qu'un laboratoire de recherche ou un bureau d'études indépendant. Enfin, le responsable du traitement doit faire réaliser des audits externes indépendants en son sein au moins une fois tous les 3 ans à compter de l'engagement de conformité. Nous comprenons que l'usage de la méthodologie de référence en tant qu'accès simplifié reste circonscrit à des cas bien précis : la généralisation de ce type d'accès ne pourra avoir lieu qu'avec la multiplication des méthodologies homologuées par la CNIL. Il n'est pas exclu que des méthodologies soient pensées pour correspondre à chaque type d'acteur pouvant mener une recherche présentant un caractère d'intérêt public. Il serait également possible d'ouvrir certaines méthodologies à d'autres données que celles du PMSI, telles que les données du SNIIRAM ou celles de la BCMD[1620].

Nous le comprenons, les accès simplifiés au bénéficie des acteurs privés à but lucratif sont, comme les accès simplifiés des acteurs publics ordinaires ou privés à but non lucratif,

[1618] Article L. 5311-1 II du code de la santé publique.

[1619] Arrêté du 22 mars 2017 *relatif au référentiel de sécurité applicable au Système national des données de santé*, *op. cit*., et 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*, JORF n° 0172 du 25/07/2017.

[1620] La BCMD est la base de données sur les causes médicales de décès élaborée par le laboratoire CépiDC, dépendant de l'Inserm.

progressivement mis en place. Si le lancement de l'accès sélectif aux données de santé du SNDS était découpé en phases, la procédure d'accès classique (dépôt à l'INDS, transmission au CEREES, puis décision finale de la CNIL), lancée à la fin du mois d'août 2017 constituerait la phase 1, tandis que la création des accès simplifiés en serait la phase 2. Ainsi, à la fin de l'année 2018, si le fonctionnement des premiers accès sélectifs est attesté par les registres d'activité tenus à jour par l'INDS, il sera nécessaire d'observer l'évolution du taux de recours à ces procédures dans la durée.

554. Un point supplémentaire mérite d'être abordé à propos de ces accès simplifiés au bénéfice des acteurs privés à but lucratif. L'encadrement des démarches tel qu'il est prévu par les délibérations[1621] de la CNIL tient compte des nécessités de respect des règles de sécurité, de maîtrise du parcours des données et de transparence[1622] en conformité notamment avec le RGPD. Il en découle la tenue à jour du répertoire public des études réalisées sous méthodologie de référence tenu par l'INDS qui permet à toute personne d'obtenir la liste des méthodologies de référence mises en œuvre. S'agissant des accès simplifiés à l'EGB, la liste des autorisations peut être trouvée dans un fichier distinct appelé tableau de suivi des dossiers déposés. Cette volonté de transparence est louable en ce qu'elle rend disponible la liste des accès simplifiés aux données de santé. Pourtant, deux incohérences pratiques pourraient être rectifiées.

La première incohérence concerne la dispersion de l'enregistrement des accès simplifiés dans plusieurs fichiers : les accès simplifiés à l'EGB, soumis à autorisation préalable de l'INDS, sont répertoriés dans un fichier global qui contient tous les dossiers déposés à l'INDS en vue d'un examen ; tandis que les déclarations de conformité à une méthodologie de référence sont inventoriées dans un fichier distinct destiné à ne contenir que ce type d'accès simplifié. Si ce modèle continue à se développer, il est probable que les décision uniques[1623] prononcées par la CNIL soient, elles aussi consignées dans un fichier qui leur sera propre. Les accès simplifiés aux données de santé du SNDS seront alors comme atomisés, chacun dans leur propre répertoire

[1621] Délibération n° 2018-134 du 12 avril 2018, *op. cit*., et délibération n° 2018-257 du 7 juin 2018, *op. cit*.

[1622] La délibération n° 2018-257 du 7 juin 2018, *op. cit* dispose d'un paragraphe 6.2 intitulé « *Principe de transparence* » et prévoyant la mise en place du répertoire public des études réalisées sous méthodologie de référence.

[1623] La décision unique de la CNIL est prévue par l'article 66, IV de la loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit*. Elle permet de « *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* ». V. *supra* n° 413.

au lieu de créer un répertoire unique des accès simplifiés, facilement accessible. Un travail de facilitation d'accès et de compréhension de l'information devra nécessairement être mené : la transparence, dont le principe est porté par l'INDS, n'aura de sens qu'à la condition qu'elle s'accompagne d'un accès aisé aux informations réputées transparentes.

La seconde incohérence porte précisément sur l'accessibilité des informations censées être transparentes. Dans le cadre de la méthodologie de référence MR-006, l'un des critères de transparence déterminés par la CNIL[1624] est la transmission, par le responsable du traitement, de sa déclaration d'intérêts ainsi que celle du laboratoire de recherche ou du bureau d'études désigné responsable de mise en œuvre dudit traitement. Dès lors nous nous attendons à ce que ces déclarations d'intérêts soient consultables librement. Elles sont bien mentionnées dans le répertoire public des études réalisées sous méthodologie de référence. En revanche, elles ne sont pas consultables, le fichier téléchargeable sur le site internet de l'INDS comporte, dans sa colonne « Déclaration d'intérêts », une liste de noms de fichiers, généralement au format « .docx » ou « .pdf » ce qui nous indique qu'une base de données des déclarations d'intérêt existe bien. Pourtant, il n'est pas possible d'en consulter le contenu à la fin de l'année 2018. De façon plus surprenante, l'outil de recherche des méthodologies de référence proposé par le site internet de l'INDS ne donne que 6 informations par étude : le titre de l'étude, le numéro de la méthodologie de référence utilisée, la nature du responsable du traitement, la nature du responsable de mise en œuvre, la date prévisionnelle de fin de l'étude, la ou les source(s) de données mobilisée(s). Il n'aurait pas été absurde que, dans le cas de la MR-006 utilisée par les acteurs privés à but lucratif, la déclaration d'intérêts soit, elle aussi rendue publique.

555. Au-delà de ces points d'amélioration de l'accès sélectif au bénéfice des acteurs privés à but lucratif, rappelons qu'une autre question demeure en suspens, celle du coût de l'accès aux données du SNDS. Sans revenir en détails sur la question dont nous en avons déjà exploré les enjeux dans la partie précédente[1625], il convient de rappeler que les acteurs chargés de la mise en œuvre de la réforme réfléchissent aux moyens de financer la mise à disposition des données de santé dans le cadre de l'accès sélectif. Au mois de décembre 2018, aucune information supplémentaire n'a filtré au sujet de la politique tarifaire éventuel de l'accès sélectif au SNDS. Cette question cruciale évoquée en détails dans le rapport déposé par la Commission des affaires

[1624] Délibération n° 2018-257 du 7 juin 2018, *op. cit.*

[1625] *Supra* n° 416 à 419.

sociales à l'Assemblée nationale en février 2017[1626] doit nécessairement trouver un écho dans la pratique car le SNDS doit trouver modèle économique fiable pour être pérenne. Sans informations supplémentaires à l'heure actuelle, nous partons du principe que, jusqu'à maintenant, les acteurs privés à but lucratif qui ont vu leur dossier d'accès au SNDS accepté par la CNIL ou qui ont eu recours à l'un des accès simplifiés n'ont pas eu à payer de redevance.

Paragraphe 2 : L'autorisation d'accès confortée par le Règlement européen relatif à la protection des données

556. Le Règlement général relatif à la protection des données[1627] a été adopté le 27 avril 2016, quelques mois seulement après la loi de modernisation de notre système de santé[1628]. Ce texte général ne porte pas spécifiquement sur l'accès des acteurs privés à but lucratif aux données de santé en France. Pourtant, son contenu est étroitement lié à ce sujet en ce qu'il encadre strictement le traitement de données à caractère personnel, y compris lorsque ces données sont dites sensibles, telles les données de santé. Les mesures prévues par le Règlement et appliquées en France imposent des obligations supplémentaires aux acteurs privés à but lucratif d'une part, et tendent à rassurer *a minima* toutes les personnes craignant que le bénéfice de l'accès sélectif permette l'installation de mécanismes de réidentification massive à des fins commerciales.

557. L'apport le plus symbolique du Règlement européen est la hausse conséquente des amendes encourues par tous les acteurs qui ne respectent pas les dispositions relatives à la protection des données. Comme nous l'avons évoqué dans la précédente partie[1629], les amendes encourues par les acteurs privé à but lucratif, au titre de l'article 83 du Règlement, peuvent désormais atteindre 2% du chiffre d'affaires annuel mondial d'une entreprise, si ce montant est supérieur à 10 millions d'euros. Dans le cas des violations les plus graves, ce montant peut aller jusqu'à 4% du chiffre d'affaires annuel mondial de l'entreprise, si ce montant est supérieur à 20 millions d'euros. Il est important de signaler que cette prise en compte du chiffre d'affaires pour déterminer le montant de l'amende est propre aux acteurs privés à but lucratif : les acteurs

[1626] Rapport d'information déposé par la Commission des affaires sociales à l'Assemblée nationale 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, 21 février 2017, p. 108 à 130.

[1627] Règlement 2016/679, *op. cit.*

[1628] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1629] *Supra* n° 292.

publics et les acteurs privés à but lucratif, n'ayant pas de chiffre d'affaires, voient leur amende potentielle plafonnée à 10 millions ou 20 millions d'euros selon la gravité de la violation commise. Ces nouveaux montants, bien supérieurs au maximum de 3 millions d'euros prévu par la loi du 7 octobre 2016[1630], ont deux vertus. La première vertu tient à leur caractère dissuasif envers les acteurs privés à but lucratif. Ceux d'entre eux qui obtiennent un accès aux données de santé grâce à leur inclusion dans l'accès sélectif au SNDS savent désormais qu'ils risquent de se voir infliger une amende pouvant avoir un impact sur leur équilibre financier s'ils traitent les données reçues sans se préoccuper des règles qui régissent la vie privée des individus. La seconde vertu de ces nouveaux montants d'amende réside dans le signal fort qui est envoyé aux personnes dont les données de santé à caractère personnel sont transmises dans le cadre de l'accès au SNDS. L'information leur est délivrée que tout écart de conduite de la part des acteurs privés à but lucratif sera durement réprimandé. Nous savons qu'il faudra vraisemblablement attendre que les premières amendes importantes fondées sur ce Règlement soient prononcées pour que les individus les plus sceptiques soient convaincus de l'efficacité dissuasive du dispositif.

558. Au-delà de cette question, le Règlement général relatif à la protection des données prévoit aussi une mesure de sécurité supplémentaire pour les responsables de traitement qui souhaitent traiter des données de santé : sans être directement nommés, les acteurs privés à but lucratif sont particulièrement concernés. L'article 35[1631] précise que le traitement « *à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1* », parmi lesquelles figurent « *les données concernant la santé* »[1632], nécessite au préalable une analyse d'impact relative à la protection des données. Cette analyse doit contenir un minimum de quatre étapes destinées à dresser un état des lieux du niveau de protection des données par le traitement envisagé. Ainsi, les acteurs privés à but lucratif qui obtiennent des données de santé du SNDS sont tenus, au titre de la première étape, de délivrer une description complète des opérations de traitement envisagées et des finalités du traitement. Dans le cadre de la sous-section 2 de la section 3 du chapitre III du titre II de la loi relative à l'informatique et aux libertés[1633], seul un intérêt public peut justifier que le traitement de données de santé soit mis en œuvre, étant

[1630] Loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique*, JORF, n° 0235, 08/10/2016.

[1631] Règlement 2016/679, *op. cit.*, art. 35.

[1632] *Ibid.*, art. 9, paragraphe 1.

[1633] Loi n° 78-17 du 6 janvier 1978, *op. cit.*, modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*, art. 66.

entendu que « *la garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux constitue une finalité d'intérêt public* »[1634]. Cette ultime précision vise particulièrement les acteurs privés à but lucratif comme les laboratoires pharmaceutiques ou les entreprises fabricant des dispositifs médicaux qui souhaitent évaluer leurs produits. La deuxième étape de l'analyse d'impact consiste pour l'acteur privé à but lucratif à évaluer la nécessité et la proportionnalité des opérations de traitement au regard des finalités : en d'autres termes, le responsable du traitement doit démontrer que toutes les données traitées, ou à traiter, sont bien utiles et nécessaires à la finalité envisagée. La troisième étape a pour objet l'évaluation des risques pour les droits et libertés des personnes dont les données sont traitées. Enfin la quatrième étape demande au responsable du traitement d'analyser les mesures envisagées pour faire face aux risques identifiés sur les données et assurer leur sécurité.

Trois de ces étapes sont, en réalité, déjà prévues dans le cadre de l'accès sélectif dont bénéficient désormais les acteurs privés à but lucratif. En effet, l'analyse du traitement envisagé et de la proportionnalité des données traitées par rapport à la finalité prévue est déjà rendue obligatoire par le décret du 26 décembre 2016[1635]. Ce texte détaille le contenu des dossiers qui doivent être déposés auprès de l'INDS. Parmi les informations qui doivent impérativement être délivrées, rappelant les étapes 1 et 2 de l'analyse d'impact prévue par le Règlement général relatif à la protection des données[1636], figurent « *la méthodologie de l'étude ou de l'évaluation ou le protocole de recherche, indiquant notamment l'objectif du traitement de données à caractère personnel, les catégories de personnes concernées par le traitement, l'origine, la nature et la liste des données à caractère personnel utilisées et la justification du recours à celles-ci, la durée et les modalités d'organisation de la recherche de l'étude ou de l'évaluation, la méthode d'analyse des données ainsi que* […] *la justification du nombre de personnes et la méthode d'observation ou d'investigation retenue* »[1637]. En correspondance avec l'étape 4 prévue par le Règlement général relatif à la protection des données[1638], le responsable du traitement est tenu de présenter « *les dispositions prises pour assurer la sécurité des traitements et des*

[1634] *Ibid*., article 66, I.

[1635] Décret n° 2016-1872 du 26 décembre 2016 *modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, JORF n° 0301, 28/12/2016.

[1636] Règlement 2016/679, *op. cit.*

[1637] Décret n° 2016-1872 du 26 décembre 2016, *op. cit*., chap. IV, section 1, art. 21, 3°.

[1638] Règlement 2016/679, *op. cit.*

informations et la garantie des secrets protégés par la loi »[1639]. Nous constatons que les autorités françaises ont su se mettre au diapason du droit européen avant son entrée en vigueur. Toutefois, deux points particuliers nous intriguent.

559. D'abord, l'une des étapes prévues dans l'analyse d'impact demandée par le Règlement général relatif à la protection des données[1640] ne trouve pas de correspondance dans les informations qui doivent figurer dans le dossier de demande d'accès aux données de santé que l'acteur privé à but lucratif doit remettre à l'INDS. Il s'agit de l'évaluation des risques qui menacent les droits et libertés des personnes dont les données sont traitées. Une telle mesure est de nature à responsabiliser l'acteur privé à but lucratif car c'est à lui qu'il revient de mettre en lumière les failles potentielles du traitement qu'il prévoit : nous pouvons y voir une portée vertueuse qui encourage les responsables de traitement à l'auto-critique. Toutefois, il est étonnant que ce mécanisme n'ait pas trouvé écho en droit français dans le cadre de l'accès sélectif aux données de santé.

560. Ensuite, nous pouvons nous interroger sur l'obligation de réaliser une étude d'impact en préalable au dépôt d'une demande d'accès aux données de santé du SNDS. Bien qu'une telle étape nous semble importante pour assurer la sécurité des données traitées par les organismes privés à but lucratif, elle n'est obligatoire, s'agissant des données de santé à caractère personnel, que dans le cadre d'un « *traitement à grande échelle* »[1641]. Dès lors, il est nécessaire de se demander à partir de quelle quantité de données un traitement devient « *à grande échelle* ». Nous pourrions penser que cette expression est une référence aux données massives, auquel cas les acteurs privés à but lucratif demandant l'accès aux données de santé issues du SNDS n'auraient pas à réaliser d'étude d'impact. Cependant, le fait que l'accès sélectif limite, par définition, la quantité de données de santé qui peuvent être obtenu, ne signifie pas nécessairement que ces données ne peuvent pas être nombreuses et donner lieu à un traitement « *à grande échelle* ». Ceci est d'autant plus vrai que la recherche en santé nécessite d'utiliser une étendue suffisante de données pour obtenir des résultats probants. Dans la pratique, il est encore trop tôt, au moment de l'écriture de ces lignes, pour avoir un recul nécessaire quant à la

[1639] Décret n° 2016-1872 du 26 décembre 2016, *op. cit.*, chap. IV, section 1, art. 21, 10°.

[1640] Règlement 2016/679, *op. cit.*

[1641] *Ibid.*, art. 35, §3, b).

cohabitation de l'article 35 du Règlement général relatif à la protection des données[1642] avec la procédure d'accès sélectif prévue en droit français. Nous pouvons formuler l'hypothèse selon laquelle le contenu du dossier que les acteurs privés à but lucratif doivent déposer au secrétariat de l'INDS répond en grande majorité aux critères de l'analyse d'impact préalable prévue en droit européen. A ce titre, afin de ne pas imposer une double procédure qui complexifierait l'accès sélectif et irait à l'encontre de l'objectif de simplification de la réforme, il est probable que les autorités françaises dispensent les acteurs privés à but lucratif de procéder à l'étude d'impact, sachant que, quoi qu'il advienne, la CNIL vérifie le dossier de demande d'accès au SNDS et demeure seule apte à délivrer l'autorisation.

561. Il n'en demeure pas moins que, comme nous l'avons étudié dans la deuxième partie de cette étude[1643], la réforme européenne du droit de la protection des données personnelles impacte fortement la pratique de l'accès aux données de santé en droit national. Les acteurs privés à but lucratif sont d'autant plus affectés qu'ils sont passés d'une interdiction totale d'accès, avant la réforme du 26 janvier 2016[1644], à une procédure d'autorisation préalable qui, par l'application du droit européen, se veut aussi permissive que possible au regard du caractère sensible des données concernées.

Le Règlement européen[1645] opère un véritable « *renversement de perspective* »[1646] en impliquant les responsables de traitement de données à caractère personnel dans une démarche d'auto-discipline conduisant à une conformité totale aux textes. Cette obligation de conformité n'est pas discutable en soit : il est parfaitement admis que la protection des données à caractère personnel est primordiale, d'autant plus lorsque des données dites sensibles font l'objet d'un traitement. C'est à cet instant que des limites sont constatées car le droit européen, en ouvrant de nouvelles perspectives, crée par la même occasion de multiples possibilités d'interprétation : cela se caractérise par la publication progressive d'aides et de notes d'information par la CNIL. Le site internet de la Commission propose régulièrement, depuis le début de l'année 2018, des fiches pratiques à destination des responsables de traitement, des guides (tel le guide sur la

[1642] *Ibid*., art. 35.

[1643] *Supra* n° 337 à 343.

[1644] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1645] Règlement 2016/679, *op. cit*.

[1646] FAUVARQUE-COSSON B., « Protection des données personnelles », *D.*, 2018, p. 1033.

sécurité des données personnelles paru le 23 janvier 2018), des formulaires types de déclaration (nomination d'un DPO, violation de données personnelles). Mais la CNIL renvoie également aux lignes directrices endossées par le Comité européen de la protection des données (CEPD) qui ont pour objectif de clarifier les dispositions du Règlement européen et de les illustrer d'exemples concrets : un document reproduit ainsi les lignes directrices relatives à l'analyse d'impact relative à la protection des données[1647], ou AIPD, et à la manière de déterminer si le traitement est « *susceptible d'engendrer un risque élevé* ». A ce titre, la CNIL a d'ailleurs mis à disposition un outil informatique en *open source*, c'est-à-dire que son code est ouvert et peut notamment être modifié et adapté à l'environnement informatique interne de l'acteur qui souhaite mener une analyse d'impact : il s'agit du logiciel PIA ou *privacy impact assessment* (analyse d'impact sur la protection des données). Sans revenir sur la question de la nécessité, pour les acteurs privés à but lucratif, de réaliser une analyse d'impact[1648] avant de déposer une demande d'accès aux données de santé du SNDS, la multiplication des documents d'aide à l'application du droit européen est le signe qu'il ne s'accorde pas si simplement au droit national. Cela représente une couche supplémentaire de dispositions dont la mise en œuvre doit être largement anticipée avant de déposer un dossier auprès de l'INDS. Les acteurs privés à but lucratif en sont les premiers touchés étant donné qu'ils doivent montrer patte blanche pour être autorisés à réaliser un traitement utilisant des données de santé issues du SNDS : il est attendu de leur part la preuve d'une probité exemplaire et d'une maîtrise parfaite du parcours des données traitées afin de ne pas les exposer à un risque de violation du droit au respect de la vie privée.

562. Le droit européen amène donc des garanties supplémentaires destinées à assurer la bonne conduite des acteurs privés à but lucratif. Pourtant, les nouvelles libertés accordées dans l'obtention et le traitement des données de santé à caractère personnel restent encadrées par des ajouts à l'échelle européenne, au risque d'alourdir les mesures déjà prévues en droit français.

[1647] Groupe de travail « Article 29 » sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 », adoptées le 4 avril 2017 et modifiées en dernier lieu le 4 octobre 2017.

[1648] *Supra* n° 558.

CONCLUSION DU CHAPITRE II

563. L'inclusion des acteurs privés à but lucratif dans l'accès aux données de santé des bases médico-administratives est le résultat de plusieurs années de réflexions. Dans la pratique, l'interdiction totale d'accès a rapidement fait naître des incohérences flagrantes comme le recours à un tiers pour récupérer et traiter des données de santé issues du SNIIRAM, ou bien l'accès ouvert aux données du PMSI pourtant revêtues d'un caractère sensible. C'est avant tout ce sentiment de contradiction qui, petit-à-petit, a conduit à repenser le mécanisme d'accès aux données de santé. Dans le même temps, des éléments de contexte ont porté un coup sévère à l'argument selon lequel les données de santé ne peuvent être correctement traitées et gérées que par des acteurs publics. L'affaire du Mediator en est l'un des exemples les plus parlants. Le développement d'une doctrine sur l'inexistence du risque zéro de réidentification des individus a également joué un rôle majeur. En effet, les acteurs privés à but lucratif ont été interdits d'accéder aux données de santé au motif que cela représenterait un risque sur la sécurité des données. Autrement dit, les acteurs publics et privés à but non lucratif seraient, eux, aptes à garantir une sécurité sans failles. Or, en réalité, le risque zéro n'existe pas[1649] et l'incapacité des acteurs privés à but lucratif à l'atteindre ne peut justifier leur exclusion du mécanisme d'accès sélectif.

564. Ces raisonnements ont conduit à la création du SNDS et à l'accueil de tous les acteurs privés à but lucratif dans l'accès sélectif aux données de santé. Cependant, ces acteurs sont bien plus surveillés que les autres. S'ils souhaitent réaliser eux-mêmes le traitement des données de santé obtenues, ils doivent réussir à prouver que ce traitement ne pourra pas, d'une manière ou d'une autre, mener à atteindre l'une des deux finalités interdites par le code de la santé publique[1650]. Pour ne pas avoir à surmonter cet obstacle inédit, ils peuvent déléguer la récupération des données et leur traitement à un organisme tiers. Cette façon de procéder qui était perçue comme un détournement de l'accès aux données de santé avant la réforme de 2016[1651] est finalement devenue la norme. Saluons toutefois l'intégration des acteurs privés à but lucratif dans les bénéficiaires des accès simplifiés parmi lesquels se trouvent l'accès à

[1649] GORCE G. et PILLET F., Rapport d'information au Sénat, *op. cit.*

[1650] Art. 1461-1 V du code de la santé publique.

[1651] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

l'EGB et la déclaration de conformité à des méthodologies de références homologuées par la CNIL.

565. La création du SNDS et l'élargissement de l'accès aux données de santé ont été votés la même année que l'adoption du Règlement général relatif à la protection des données[1652] par l'Union européenne. Ce texte européen a entièrement mis à jour les modalités d'encadrement de l'accès aux données à caractère personnel. L'impact le plus visible est la définition de sanctions adaptées aux potentiels auteurs d'infractions : une entreprise qui se rend coupable d'une violation du droit relatif à la protection des données personnelles peut maintenant être condamnée à une amende dont le plafond peut atteindre entre 2% et 4% de son chiffre d'affaires annuel mondial. Cette perspective est autrement plus dissuasive que l'ancien montant qui était plafonné à 3 millions d'euros en France. Les acteurs privés à but lucratif qui accèdent aux données de santé et qui réalisent un traitement savent donc que le moindre écart de conduite peut coûter cher. Une obligation supplémentaire est également issue du Règlement européen avec l'obligation de procéder à une analyse d'impact préalablement à la mise en place d'un traitement de données de santé « *à grande échelle* ».

566. L'année 2016 représente finalement l'aboutissement d'un long chemin pour les acteurs privés à but lucratif. Ils sont passés d'une interdiction totale d'accès aux données de santé qui a duré plus de 10 ans, due à la méfiance des pouvoirs publics à leur égard, à une pleine intégration dans le mécanisme d'accès au SNDS moyennant quelques ajustements à leur intention.

[1652] Règlement 2016/679, *op. cit.*

CONCLUSION DU TITRE II

567. La réforme de l'accès sélectif pour y inclure les acteurs privés à but lucratif est le fruit de plusieurs années de réflexions. Avec le recul que nous avons aujourd'hui, sans pouvoir dire que cette réforme aurait pu avoir lieu plus tôt, nous pouvons affirmer que le principe d'interdiction d'accès fixé dès 2005 aurait pu, lui, être dénoncé plus précocement en raison de son absence de base légale. Il est probable que le contexte de fort développement technologique de la première décennie du XXI^{e} siècle, avec la démocratisation des données ouvertes et des mégadonnées, ait poussé les autorités françaises à ne laisser aucune marge de manœuvre au secteur privé à but lucratif dans le cadre de l'accès aux données de santé à caractère personnel. Mais les nombreuses craintes exprimées n'étaient pas suffisamment étoffées pour justifier une interdiction d'accès total. La question de la mise à l'écart des acteurs privés à but lucratif de l'accès aux données de santé semble pourtant avoir fait consensus pendant quelques années, au nom de la protection de la vie privée, jusqu'à ce que des sociétés, comme Celtipharm, devenu Openhealth, contestent la situation[1653].

568. L'émergence de nouvelles réflexions et rapports sur les opportunités d'accès aux données de santé à caractère personnel, dans le respect de la vie privée des individus, a finalement permis de préparer la réforme de l'accès sélectif et d'y inclure, au moyen de nouvelles garanties et obligations, les acteurs privés à but lucratif. Le droit européen est venu, dans le même temps, encadrer strictement l'ensemble des traitements de données à caractère personnel, en réservant un sort particulier aux traitements qui portent sur les données sensibles que sont les données personnelles de santé. Dans la pratique, le nouveau système d'accès au SNDS semble porter ses fruits si nous nous reportons aux tableaux de bord publiés par l'INDS : les acteurs privés à but lucratif font partie des grands demandeurs d'accès et ils ont obtenu, au mois de juin 2018, plus du tiers des autorisations délivrées par la CNIL depuis l'ouverture des dépôts de dossiers en septembre 2017.

[1653] Conseil d'Etat, 1ère - 6^{e} chambres réunies, 20 mai 2016, n° 385305, recueil Lebon, Celtipharm.

CONCLUSION DE LA PARTIE III

569. L'accès des acteurs privés à but lucratif aux données du SNDS est une nouveauté dans le droit français. L'inclusion des entreprises privées dans le cercle fermé des acteurs admis à déposer une demande d'accès sélectif[1654] auprès de l'INDS grâce à la réforme[1655] est l'aboutissement d'un processus long et tortueux. Entre l'exclusion quasi-totale du secteur privé à but lucratif du dispositif d'accès sélectif[1656] par l'arrêté de 2005[1657], et sa réintégration consacrée à la fois par la loi et la jurisprudence[1658] en 2016[1659], bien peu de voix se sont élevées face à la fragilité des arguments[1660] présentés par le pouvoir réglementaire.

570. Ce titre présente donc une importance particulière par sa portée générale qui consiste à aborder l'existant et à se projeter dans le passé pour comprendre, avec nos connaissances d'aujourd'hui, comment l'interdiction d'accès des acteurs privés à but lucratif a pu être créée et justifiée. Nous constatons que la protection de la vie privée est soit mise en avant, soit décelable en sous-texte, à chaque développement. L'évolution du système d'accès aux données de santé vers une ouverture pour les acteurs privés à but lucratif n'est pas seulement l'aboutissement d'un raisonnement juridique souvent représenté par des rapports officiels marquants[1661]. Elle est aussi le résultat d'une meilleure maîtrise et d'une meilleure connaissance des nouvelles technologies qui permettent de traiter les données. Ces deux facteurs sont essentiels car des risques qui étaient craints, si ce n'est fantasmés, au début des années 2000, sont aujourd'hui parfaitement identifiés, délimités et leur probabilité de survenir est mieux appréhendée. Ainsi, la volonté de ne permettre aux acteurs privés à but lucratif d'accéder aux

---

[1654] Sur le fonctionnement du nouvel accès sélectif, v. *supra* n° 300 à 347 et 393 à 442.

[1655] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1656] *Supra* n° 462 à 466.

[1657] Arrêté du 20 juin 2005.

[1658] *Supra* n° 493 à 504.

[1659] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*, et Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, *op. cit.*

[1660] *Supra* n° 515 à 517.

[1661] BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.* ; BURNEL P. et VON LENNEP F., *Rapport de la Commission open data en santé*, *op. cit.* ; GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *Pour une meilleure utilisation des bases de données administratives et médico-administratives nationales pour la santé publique et la recherche*, *op. cit.* ; GORCE G. et PILLET F., Rapport d'information au Sénat, *La protection des données personnelles dans l'open data : une exigence et une opportunité*, *op. cit*.

données de santé à caractère personnel que si le risque zéro de réidentification est garanti n'est plus qu'un vague souvenir. En effet, nous savons aujourd'hui qu'il est impossible d'assurer à cent pour cent que les données de santé à caractère personnel qui ont fait l'objet d'un traitement pour être non réidentifiantes, ne permettent, par le truchement de traitements automatisés sophistiqués et de croisements de données, de réidentifier, malgré toutes les précautions possibles, les individus. En revanche, le risque de faire perdre aux données tout leur intérêt a été mis en lumière[1662] car pour rendre une donnée à caractère personnel, il faut nécessairement lui ôter des caractéristiques précises : or, moins une donnée recèle d'informations, moins son traitement aura de portée scientifique. Plutôt que de fermer l'accès sélectif aux acteurs privés à but lucratif, les forçant à utiliser des moyens détournés[1663] pour faire réaliser des traitements par des acteurs habilités, eux, à déposer des dossiers, la réforme prend le parti de la responsabilisation en assumant qu'il existera, quelles que soient les précautions prises, sur la vie privée des individus, l'objectif étant que ce risque demeure infinitésimal.

571. La réforme du 26 janvier 2016[1664] créant le SNDS impose des obligations plus sévères à certaines entreprises comme les industries de santé, les organismes assureurs ou les organismes de crédit. Ils doivent répondre à tous les critères posés par la loi pour prétendre obtenir une autorisation d'accès aux données du SNDS à des fins de traitement. Certains critères sont, par ailleurs, suffisamment contraignants et l'appréciation des conditions à remplir pour y correspondre est encore trop floue pour que les entreprises visées soient nombreuses à prendre le risque de déposer un dossier sur leur fondement[1665].

Peu après la réforme, comme pour accompagner le droit français dans cette ouverture des accès, le Règlement européen relatif à la protection des données[1666] est venu apporter des mesures de protection des données supplémentaires afin de créer un encadrement juridique global, incluant des conditions particulières à remplir préalablement à tout traitement de données qui porterait sur des données de santé à caractère personnel. Ce renfort européen, associé à des dispositions plus générales sur la responsabilisation des responsables de traitement, est de nature à inciter

[1662] *Supra* n° 531 et 543.

[1663] *Supra* n° 468 à 473.

[1664] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1665] *Supra* n° 550.

[1666] Règlement 2016/679, *op. cit.*

les acteurs privés à but lucratif à être vertueux dans leur utilisation des données obtenues, mais il est aussi un facteur rassurant pour les individus qui pouvaient craindre que leurs données de santé soient exhibées sur la place publique et exploitées sans retenue à des fins commerciales. Au regard de la sévérité des textes français et européen, nous pouvons affirmer qu'à l'heure actuelle, il n'en est rien.

CONCLUSION GÉNÉRALE

572. L'enjeu principal de cette étude était d'analyser en profondeur les différents types d'accès aux données de santé à caractère personnel contenues dans les bases médico-administratives. Cette analyse a pour point de départ la création du SNIIRAM, qui est la base la plus importante et la plus connue puisqu'elle regroupe toutes les données de soins de ville, en 1998[1667]. Elle se termine avec l'examen de la situation découlant de la réforme intervenue en 2016[1668]. Pour parvenir à décrypter l'ensemble des dispositifs mis en œuvre au fil des années, nous avons procédé à l'analyse de la hiérarchisation, par les pouvoirs publics, de chacun des accès proposés en fonction de la nature des acteurs qui en font la demande. En effet, la distinction selon la nature des acteurs est le critère essentiel qui détermine les modalités d'accès aux données de santé.

573. Cette méthode nous a conduit à identifier trois grandes catégories d'acteurs, chacune faisant l'objet d'un traitement particulier par les dispositions législatives et réglementaires. La première catégorie concerne les acteurs publics, désignés par arrêté[1669] puis par décret[1670], qui bénéficient d'un accès permanent aux données de santé de l'assurance maladie dans des limites prévues par les textes. La deuxième catégorie, plus large et non exhaustive, inclut tous les acteurs publics qui ne bénéficient pas d'un accès permanent ainsi que les acteurs privés à but non lucratif : leur accès aux données de santé est alors soumis à une autorisation préalable délivrée par la CNIL. La troisième catégorie d'acteurs vise tous les acteurs privés à but lucratif qui ont été strictement interdits d'accès dès 2005[1671] mais qui ont finalement été admis dans le cercle des bénéficiaires de l'accès sélectif à l'occasion de la réforme de 2016.

[1667] Le Système national interrégimes de l'assurance maladie a été créé par la loi n° 98-1194 du 23 décembre 1998 *de financement de la sécurité sociale pour 1999*, *JORF*, n° 300, 27/12/1998.

[1668] Loi n° 2016-41 du 26 janvier 2016 *de modernisation de notre système de santé*, JORF n° 0022 du 27/01/2016.

[1669] Depuis l'arrêté du 11 avril 2002 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, JORF n° 89, 16/04/2002, jusqu'à celui du 6 octobre 2016 *relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie*, JORF n° 0244, 19/10/2016.

[1670] Décret n° 2016-1871 du 26 décembre 2016 *relatif au traitement de données à caractère personnel dénommé « système national des données de santé »*, JORF n° 0301, 28/12/2016.

[1671] Arrêté du 20 juin 2005 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, JORF n° 192 du 19/08/2005.

574. Une telle approche nous a permis de détailler, pour l'ensemble des demandeurs, le fonctionnement précis de chacune des modalités d'accès, ou d'interdiction, aux données de santé à caractère personnel notamment contenues dans le SNIIRAM élargi et de mettre en lumière les justifications avancées par les autorités pour appuyer leurs décisions. Ce travail semblait par ailleurs nécessaire au vu du peu de matière doctrinale publiée sur le sujet. Des enjeux majeurs entourent l'accès aux données de santé car si leur bon traitement permet d'améliorer le fonctionnement de l'ensemble des composantes du secteur sanitaire en France, ce traitement ne peut se faire sans prendre les précautions suffisantes pour assurer la protection de la vie privée des individus. Il ressort du décryptage des types d'accès aux données de santé que chacun d'eux présente une complexité importante. Cette complexité découle aussi bien de la superposition des textes juridiques dans le temps que de leurs modalités de mise en œuvre. Grâce à la connaissance des modalités d'accès aux données de santé des bases médico-administratives développée dans cette étude, nous avons travaillé, pour chacun des acteurs concernés, à démontrer dans quelle mesure le législateur a été conduit à proposer une réforme complète avec la loi du 26 janvier 2016[1672] qui a déjà fait l'objet de trois modifications majeures en 2018 et 2019. Ces nouveaux changements proviennent de l'adaptation, par la loi[1673] et par ordonnance[1674] du droit français au Règlement général relatif à la protection des données[1675], ainsi que du projet de loi relatif à l'organisation et à la transformation de notre système de santé[1676]. Les limites de chacun des accès ont été mises en exergue, ainsi que leurs dysfonctionnements éventuels et, pour certains (notamment l'interdiction d'accès imposée aux acteurs privés à but lucratif), l'absence de fondement concret pour permettre de comprendre dans quelle mesure la réforme a apporté des solutions et des améliorations.

575. La vision transversale du système d'accès aux données de santé qui est aujourd'hui la nôtre permet de constater que la distinction entre les trois grands ensembles d'acteurs demeure. Bien que les acteurs privés à but lucratif soient aujourd'hui bénéficiaires de la même procédure d'accès sélectif que les acteurs publics et les acteurs privés à but non lucratif, nous avons

[1672] Loi n° 2016-41 du 26 janvier 2016, *op. cit*.

[1673] Loi n° 2018-493 du 20 juin 2018, *op. cit*.

[1674] Ordonnance n° 2018-1125 du 12 décembre 2018, *op. cit.*

[1675] Règlement 2016/679, *op. cit.*

[1676] Projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019.

souligné que la réforme impose des contraintes supplémentaires non négligeables[1677] aux entreprises du secteur de la santé, laboratoires pharmaceutiques et organismes d'assurance, qui sont les acteurs privés à but lucratif les plus demandeurs de données de santé. La méthode de définition des modalités d'accès aux données de santé à caractère personnelles des bases médico-administratives est finalement restée fondamentalement la même : aujourd'hui encore, c'est en fonction de la nature de l'acteur que les opportunités d'accès qui lui sont offertes sont déterminées.

576. Si une chose doit être retenue de nos développements, c'est le changement total de paradigme dont a fait l'objet le système d'accès aux données de santé avec la réforme de 2016. Celui-ci consistait initialement en un mécanisme hautement cloisonné, très complexe, peu incitatif à demander un accès aux données de santé et excluant même une catégorie entière de bénéficiaires potentiels. Depuis la loi du 26 janvier 2016[1678], ce mécanisme se porte sur l'accessibilité des données de santé par la mise en œuvre d'une procédure plus simple – bien qu'elle soit encore difficile à appréhender – associée à des accès simplifiés divers qui devraient connaître un développement favorable, le tout empreint d'un regain de pédagogie à l'attention de tous les bénéficiaires. Ce bouleversement s'est accompagné d'un autre changement introduit par le droit européen : il s'agit de la responsabilisation des acteurs qui souhaitent traiter des données de santé. Le Règlement général relatif à la protection des données[1679] pose le principe de la *compliance*, traduisible par le mot « conformité » : cela consiste à créer un cadre légal permettant à tous les acteurs traitant des données à caractère personnel d'être autonomes dans leur pratique. Ces acteurs s'engagent à se mettre en conformité avec les dispositions légales et réglementaires. Cette plus grande liberté qui est offerte à tous les acteurs est doublée de la création de sanctions pécuniaires véritablement dissuasives en cas de non-conformité. Mais ces changements ne sont pas survenus sans difficultés, bien au contraire. C'est dès le début des années 2010 que des initiatives[1680] ont été lancées par des personnalités de tous horizons pour alerter les pouvoirs publics de l'effet contre-productif de l'inaccessibilité des données de santé au plus grand nombre. La multiplication des critiques à l'égard des dysfonctionnements du

[1677] La réforme crée des finalités de traitement interdites dédiées aux industriels de santé et aux organismes assureurs. Elle impose également des garanties supplémentaires à apporter si l'acteur privé à but lucratif souhaite effectuer lui-même le traitement des données de santé obtenues.

[1678] Loi n° 2016-41 du 26 janvier 2016, *op. cit.*

[1679] Règlement 2016/679, *op. cit.*

[1680] Notamment l'Initiative Transparence Santé qui a été dissoute en octobre 2014.

système d'accès aux données de santé, tel qu'il existait, a conduit les autorités à demander la production de rapports[1681] dont certains sont devenus emblématiques. C'est à l'issue de plusieurs années de concertations et de débats que la création du SNDS a été actée par le législateur. Le nouveau dispositif est organisé pour optimiser l'organisation des données de santé entre elles, pour faciliter leur manipulation tout en garantissant leur sécurité, et pour fluidifier les procédures permettant d'y accéder.

577. La mise en œuvre du nouveau système d'accès aux données de santé n'est pas encore synonyme de l'ouverture la plus totale qu'il est possible d'imaginer. En effet, de nombreuses briques du dispositif sont encore en phase d'élaboration parmi lesquelles la mise à disposition de l'ensemble des données de santé qui ne présentent aucun caractère réidentifiant, sous forme agrégée. Atteindre cet objectif demande un certain temps car il faut identifier les façons dont les données peuvent être traitées pour présenter un intérêt, une fois qu'elles sont agrégées, réaliser ce traitement d'agrégation puis les mettre à disposition. Une telle démarche repose également sur les requêtes des demandeurs de données de santé qui permettent de savoir quelles sont les informations à prioriser. L'accès aux données de santé à caractère personnel désormais contenues dans le SNDS est donc triple : le premier est l'accès ouvert aux jeux de données agrégées mis à disposition du public, le deuxième se fait via les différents accès simplifiés (encore en développement), le troisième est l'accès soumis à autorisation de la CNIL à travers la procédure d'accès sélectif.

578. Malgré les remous de ces dernières années, l'organisation de l'accès aux données de santé des bases médico-administratives est loin d'être stabilisée. Le nouveau projet de loi relatif à l'organisation et à la transformation du système de santé[1682] a, une fois de plus, modifié certaines règles afin d'élargir les possibilités d'accès, les types de données accessibles, tout en apportant des changements aux différents intervenants dans la procédure d'accès sélectif. La valorisation des données de santé à caractère personnel contenues dans les bases de données médico-administratives est finalement devenu un sujet incontournable qui est aujourd'hui au cœur de la politique nationale de santé. Chacune des évolutions dans le droit d'accès à ces

[1681] GOLDBERG M., Rapport du Haut Conseil de la Santé publique de mars 2012, *op. cit.* ; BRAS P.-L., *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.* ; GORCE G. et PILLET F., Rapport d'information au Sénat, *op. cit.*

[1682] Projet de loi relatif à l'organisation et à la transformation du système de santé enregistré à la présidence de l'Assemblée nationale le 13 février 2019.

données de santé est pensée en prenant en considération les exigences du droit au respect de la vie privée. L'intervention de la CNIL, invitée à délivrer son avis, est ainsi systématique en préalable à tous les projets de loi, d'ordonnance, de décret ou d'arrêté qui pourraient affecter les modalités d'accès et de traitement des données de santé à caractère personnel. Le législateur met tout en œuvre, depuis la réforme de 2016, pour concilier la protection de la vie privée avec l'élargissement de l'accès à ces données si sensibles. Un compromis équilibré semble être trouvé avec la nouvelle loi relative à l'organisation et à la transformation du système de santé : cet aboutissement est le fruit d'un dialogue construit et permanent entre toutes les parties prenantes.

BIBLIOGRAPHIE

[Ouvrages]

BELANGER Michel, *Droit européen général de la santé*, Les Etudes hospitalières, coll. Cahiers du CERDES, 2013, 308 p.

BELLEIL Arnaud, *E-privacy : le marché des données personnelles : protection de la vie privée à l'âge d'Internet*, Dunod, 2001, 202 p.

BERGOIGNAN-ESPER Claudine, DUPONT Marc, *Droit hospitalier*, 10e éd., D., coll. Cours, 2017, 1048 p.

BERGOIGNAN-ESPER Claudine, SARGOS Pierre, *Les grands arrêts du droit de la santé*, 2e éd., Dalloz-Sirey, 2016, 733 p.

BOUCHARDON Laurent, *La responsabilité des acteurs publics de santé*, Presses de l'école des hautes études en santé publique, 2010, 106 p.

BOURGEOIS Matthieu, avec la participation de BOUNEDJOUM Amira, *Droit de la donnée, Principes théoriques et approche pratique*, Lexis Nexis, 2017, 300 p.

BOUTEILLE-BRIGANT Magali, *Les indispensables du droit médical*, Ellipses, 2016, 254 p.

BROUDOUX Evelyne, CHARTRON Ghislaine, *Big data – open data : quelles valeurs ? Quels enjeux ? : actes du colloque "Document numérique et société"*, De Boeck supérieur, 2015, 282 p.

CADOUX Louise, *Voix, image et protection des données personnelles / Commission nationale de l'informatique et des libertés*, la Documentation française, 1996, 119 p.

CALLU Marie-France, GIRER Marion, ROUSSET Guillaume, *Dictionnaire de droit de la santé - Secteurs sanitaire, médico-social et social*, LexisNexis, 2017, 417 p.

DE FORGES Jean-Michel, *Le droit de la santé*, 8e éd., PUF, coll. Que sais-je ?, 2012, 128 p.

DEROCHE Philippe, *La vie privée*, Dalloez-Sirey, coll. Justice et Cassation, 2018, 373 p.

DESCHAMPS Christophe, DELENGAIGNE Xavier, *Organisez vos données personnelles – L'essentiel du Personal Knowledge Management*, Editions d'Organisation, 2011, 256 p.

EYNARD Jessica, *Les données personnelles : quelle définition pour un régime de protection efficace ?*, Michalon éd., 2013, 435 p.

de FARIA Maria Paula Marçal Grilo Lobato, *Données génétiques informatisées : un nouveau défi à la protection du droit à la confidentialité des données personnelles de santé*, Presses universitaires du Septentrion, 1999, 603 p.

FENOLL-TROUSSEAU Marie-Pierre, HAAS Gérard, *Internet et protection des données personnelles*, Litec, 2000, 206 p.

FOREST David, *Droit des données personnelles*, Gualino : Lextenso éd., 2011, 117 p.

HERVE Christian, STANTON-JEAN Michèle et MARTINENT Eric, *Les systèmes informatisés complexes en santé. Banque de données, télémédecine : normes et enjeux éthiques*, D., 2013, 282 p.

HOLCMAN Robert, *Le programme de médicalisation du système d'information (PMSI),* Management hospitalier, 2015, p. 553-568.

KESSOUS Emmanuel, *L'attention au monde : sociologie des données personnelles à l'ère du numérique*, Arman Colin, 2012, 319 p.

de LAMBERTERIE Isabelle et LUCAS Henri-Jacques, *Informatique, libertés et recherche médicale*, CNRS Editions, 2001, 283 p.

LAUDE Anne, MATHIEU Bertrand, TABUTEAU Didier, *Droit de la santé*, 3e éd., PUF, coll. Thémis Droit, 2012, 728 p.

LAUDE Anne, TABUTEAU Didier, *Les droits des malades*, PUF, coll. Que sais-je ?, 2016, 128 p.

LEJEUNE Yannick, à l'initiative de l'EPITA, *Big, fast, open data : décrire, décrypter et prédire le monde : l'avènement des données*, FYP, 2014, 191 p.

LOISEAU Pierre, *La maîtrise des dépenses de santé confrontée à la responsabilité médicale aux Etats-Unis et en France*, Presses universitaires d'Aix-Marseille, 2005, 402 p.

MATTATIA Fabrice, *Traitement des données personnelles : le guide juridique : la loi informatique et libertés et la CNIL, jurisprudences*, Eyrolles, 2013, 187 p.

MOQUET-ANGER Marie-Laure, *Droit hospitalier*, 5e éd., LGDJ, coll. Manuels, 2018, 576 p.

MORELLE Aquilino, TABUTEAU Didier, *La santé publique*, PUF, coll. Que sais-je ?, 2010, 128 p.

PANSIER Frédéric-Jérôme, GARAY Alain, *Le médecin, le patient et le droit*, Editions de l'école nationale de la santé publique, 1999, 223 p.

PIERRE-BEAUSSE Cyril, *La protection des données personnelles*, Ed. Promoculture, 2005, 378 p.

PONSEILLE Anne, *Professions, professionnels et établissements de santé face au droit pénal*, LEH Edition, 2015, 427 p.

REY Bénédicte, *La vie privée à l'ère du numérique*, Hermès Science Publications, coll. Traitement de l'information, 2012, 304 p.

ROCHELANDET Fabrice, *Economie des données personnelles et de la vie privée*, la Découverte, 2010, 125 p.

SUDRE Frédéric, *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Emile Bruylant, coll. Droit et justice, 2005, 336 p.

TRUCHET Didier, *Droit de la santé publique*, 9e éd., Dalloz, coll. Mémento, 2017, 317 p.

VOGEL Gaston, *Les grands principes du droit médical et hospitalier*, 2e éd., Promoculture, 2001, 211 p.

[Ouvrages collectifs]

CASTETS-RENARD Céline, dir., *Quelle protection des données personnelles en Europe ? : actes du colloque tenu le 14 Mars 2014 à la Faculté de droit de l'Université Toulouse 1 Capitole*, Larcier, 2015, 187 p.

CLEMENT Jean-Marie, MEMETEAU Gérard, *Le droit des données de santé*, Revue générale de droit médical, 2004, n° 4.

DOCQUIR Benjamin, dir., PUTTEMANS André, dir., *Actualités du droit de la vie privée*, Emile Bruylant, coll. UB3, 2009, 202 p.

FAURE Georges, dir., *La Loi du 4 mars 2002 : continuité ou nouveauté en droit médical ?*, Éditions CEPRISCA, 2003, 180 p.

FRAYSSINET Jean, HUET Jérôme, NERBONNE Sophie... et al., *La régulation des données personnelles*, Victoires éditions, 2009, 155 p.

GAUMOND-PRAT Hélène, dir., *Mélanges*, *Droit et Bioéthique*, en l'honneur de Jean MICHAUD, LEH Edition, 2012, 578 p.

GROSJEAN Alain, dir., *Enjeux européens et mondiaux de la protection des données personnelles*, Larcier, 2015, 465 p.

MARTINEZ Eric, VIALLA François, dir., *Les grands avis du Comité Consultatif National d'Ethique*, LGDJ, coll. Les grandes décisions, 2013, 816 p.

PEREZ ASINARI Maria Veronica, dir., PALAZZI Pablo, dir., *Défis du droit à la protection de la vie privée – Perspectives du droit européen et nord-américain*, Emile Bruylant, coll. Cahiers du CRID, 2009, 649 p.

SCHRAMECK Olivier, dir., *Santé et justice : quelles responsabilités ? : dix ans après la loi du 4 mars 2002 / colloque organisé par le Conseil d'Etat et la Cour de cassation les 20 et 21 octobre 2011*, la Documentation française, 2013, 405 p.

TABATONI Pierre, dir., *La protection de la vie privée dans la société d'information, Tome 3, 4 et 5, L'impact des systèmes électroniques d'information*, PUF, coll. Cahiers des sciences morales et politiques, 2002, 383 p.

VIALLA François, dir., *Jurisprudences du secteur social et médico-social*, Dunod, 2012, 516 p.

VIALLA François, dir., REYNIER Mathieu, MARTINENT Eric, coord., *Les grandes décisions du droit médical*, 2e éd., LGDJ, 2014, 896 p.

WEILL Claude, ADER Basile, BRUGUIERE Jean-Michel... et al., *Les nouvelles frontières de la vie privée : droits de la personnalité, protection des données personnelles : actes du Forum Légipresse du 25 septembre 2008, Maison du Barreau de Paris*, Victoires éditions, 2009, 138 p.

[Thèses]

CAVALIER Mathilde, « La propriété des données de santé », *thèse soutenue à l'Université Lyon 3 – Jean Moulin*, 14/12/2016, 491 p.

CONTIS Maïalen, *Secret médical et évolutions du système de santé,* Bordeaux, LEH éditions, 2005, 856 p.

MARLIAC-NEGRIER Claire, *La protection des données nominatives informatiques en matière de recherche médicale*, Thèse de doctorat en Droit public soutenue en 1999 à Clermont Ferrand 1, Presses Universitaires d'Aix – Marseille, 2001, 844 p.

STAMM Eric, sous la direction de Marie-France CALLU et de Bruno PY, *La transmission des données personnelles de santé : analyse et propositions d'évolution. Le cas du contrôle de l'assurance maladie*, thèse soutenue à l'université de Lyon 3, 2011, 508 p.

ZORN-MACREZ Caroline, *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, Thèse de doctorat en Droit privé et Sciences criminelles soutenue le 5 décembre 2009 à l'Université de Nancy 2, Presses Universitaires de Nancy, 2010, 502 p.

[Rapports et Avis]

BABUSIAUX Christian, BREAS Louis, ESLOUS Laurence, THOUVENIN Dominique, *Rapport, L'accès des assureurs complémentaires aux données de santé des feuilles de soins électroniques*, 26 mai 2003, 118 p.

BEGAUD Bernard, POLTON Dominique, VON LENNEP Franck, « Les données de vie réelle, un enjeu majeur pour la qualité des soins et la régulation du système de santé. L'exemple du médicament », *Rapport réalisé à la demande de Madame la Ministre de la santé Marisol Touraine*, mai 2017.

BRAIBANT Guy, *Données personnelles et société de l'information : transposition en droit*

français de la directive n° 95-46 / rapport au Premier Ministre, la Documentation française, 1998, 95 p.

BRAS Pierre-Louis, *Rapport sur la gouvernance et l'utilisation des données de santé*, septembre 2013, 128 p.

BURNEL Philippe et VON LENNEP Franck, *Rapport de la Commission open data en santé*, 9 juillet 2014, 122 p.

Comité consultatif national d'éthique :
- Avis n° 91, *Problèmes éthiques posés par l'informatisation de la prescription hospitalière et du dossier du patient*, avril 2006, 25 p.
- Avis n° 104, *Le Dossier médical personnel et l'informatisation des données de santé*, juin 2008, 16 p.

Comité Stratégique de Filière des Industries et Technologies de santé (CSF), « Promouvoir une démarche active visant à faciliter l'accès aux données de santé à des fins de santé publique, de recherche et de développement industriel », *Rapport du groupe CSF mesure 1-5*, 29/03/2017, 82 p.

Commission nationale consultative des droits de l'Homme, « Protection de la vie privée à l'ère numérique », *Avis*, 22/05/2018, 44 p.

Commission européenne, *Avis n° 13 du 30 juillet 1999 : Aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information*, Journal international de bioéthique, 2001/3, vol. 12, p. 113-117.

Commission nationale de l'informatique et des libertés :
- *26e rapport d'activité 2005*, la Documentation française, 2006, 125 p.
- *Rapport d'activité 2014*, la Documentation française, 2015, 94 p.
- *Rapport d'activité 2015*, la Documentation française, 2016, 100 p.
- *Délibération n° 201-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978*, demande d'avis n° 17023753, 30/11/2017.

Conférence Nationale de Santé, *Avis sur les données de santé informatisées,* 19 octobre 2010, 11 p.

Conseil d'Etat, « Avis sur un 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 », *Ampliation rectificative*, 11/12/2017, 15 p.

Cour des comptes, « Les données personnelles de santé gérées par l'Assurance maladie », *Communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale*, 03/2016, 167 p.

GOLDBERG Marcel, Rapport du Haut Conseil de la Santé publique de mars 2012, *Pour une meilleure utilisation des bases de données administratives et médico-administratives nationales pour la santé publique et la recherche*, 2012, 56 p.

GORCE Gaëtan et PILLET François, Rapport d'information au Sénat, *La protection des données personnelles dans l'open data : une exigence et une opportunité*, 16 avril 2014, 85 p.

Groupe de travail « article 29 », composé de représentants des autorités nationales chargées de la protection des données, du Contrôleur Européen de la Protection des Données et de la Commission européenne, Avis 4/2007, *La protection des données sur le concept des données à caractère personnel*, 20 juin 2007.

Haute autorité pour la transparence de la vie publique, « Open data & intégrité publique, Les technologies au service d'une démocratie exemplaire », *Contribution pour le sommet mondial du partenariat pour un Gouvernement ouvert*, 2016, 100 p.

Institut des données de santé :
- « Enjeux et étapes », *Rapport au Parlement*, 2010, 66 p.
- « Ouverture, qualité, partage : des avancées », *Rapport au Parlement*, 2015, 76 p.

Institut Montaigne, « Protection sociale : une mise à jour vitale », *Rapport*, 03/2018.

LEVY Maurice et JOUYET Jean-Pierre, Rapport de la Commission sur l'économie de l'immatériel, *L'économie de l'immatériel, la croissance de demain*, novembre 2006, 184 p.

Mission de préfiguration, « Rapport Health Data Hub », une mission pilotée par CUGGIA Marc (CHU Rennes), POLTON Dominique (INDS), WAINRIB Gilles (OWKIN) et rapportée par COMBES Stéphanie (DREES), 12/10/2018, 110 p.

Projet de loi relatif à la protection des données personnelles, *Etude d'impact*, 12/12/2017, 530 p.

Rapport d'information à l'Assemblée nationale sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française, n° 4544, 22 février 2017.

Rapport d'information déposé par la Commission des affaires sociales à l'Assemblée nationale 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, 21 février 2017.

TROJETTE Mohammed Adnène avec le concours de LOMBARD Rémy, Rapport au Premier ministre, *Ouverture des données publiques. Les exceptions au principe de gratuité sont-elles toutes légitimes ?*, juillet 2013, 121 p.

[Articles]

ADER Basile, « La protection de la vie privée en droit positif français », Legicom, n° 20, 1999/4, p. 5-8.

ANCIAUX Arnaud, FARCHY Joëlle, « Données personnelles et droit de propriété : quatre chantiers et un enterrement », *Revue internationale de droit économique*, 01/09/2015, n° 3, p. 307-331.

d'ANTIN Olivier, BROSSOLLET Luc, « Le domaine de la vie privée et sa délimitation jurisprudentielle », *Legicom*, n° 20, 1999/4, p. 9-19.

ALIX Pascal, « Le DPO et le secteur de la communication », *Legicom*, n° 59, 2017/2, p. 115-122.

ARBBOUSSET Hervé, « Mediator et indemnisation des victimes : retour sur une affaire d'Etat », *JCP administrations et collectivités territoriales*, 12/12/2011, n° 50.

ARIES Philippe et DUBY Guy (ss. dir. de), « Histoire de la vie privée », *Seuil*, 27/10/1999, 640 p.

Assurance maladie, « Mise en œuvre du système national d'information interrégimes – Texte non codifié », *JCP Social*, n° 13, 20/09/2005.

BALLET Philippe, BENEAT Anne-Lise, « Dématérialisation des données de santé : quels référentiels ? », *La Gazette du Palais*, 21/01/2011, n° 21-22, p. 22-25.

BENABOU Valérie-Laure, « L'extension du domaine de la donnée », *Legicom*, n° 59, 2017/2, p. 3-17.

BENOÎT-ROHMER Florence, « Chronique Union européenne et droits fondamentaux – L'adoption de mesures visant à renforcer la protection des données personnelles », *RTD Eur*., 2017, p. 355.

BELLEIL Arnaud, « La régulation économique des données personnelles ? », *Legicom*, 2009/1, n° 42, p. 143-151.

BERANGER Jérôme et BOUADI Ryad, « Approche éthico-juridique de l'usage des données médicales à caractère personnel », *Les Cahiers du numérique*, 2014/2, vol. 10, p. 93-123.

BERANGER Jérôme, « De l'étude des risques à la traduction des enjeux éthiques des Big Data en santé », *Journal International de Bioéthique*, 2017/3, vol. 28, p. 15-25.

BERLIN Dominique, « Union européenne – Conservation et accès des données personnelles », *JCP G*, 16/01/2017, n° 3.

BERTRAND Morgane, « La protection des données personnelles comme mode de régulation du big data en protection sociale complémentaire », *Revue française des affaires sociales*, 2017/4, p. 57-78.

BESLAY Nathalie, « Les applications de données médicales personnelles : approche juridique pratique », *RGDM*, 2004, n° 4, p. 35-40.

BEYNEIX Isabelle, « Le traitement des données personnelles par les entreprises : big data et vie privée, état des lieux », *JCP G*, 09/11/2015, n° 46-47, p. 2113-2119.

BICLET Philippe, « Hébergement et échange des données de santé », *Médecine et Droit*, 01/11/2010, n° 105, p. 159-160.

BILLARD Jacques, « Une transparence en trompe-l'œil », *Médium*, n° 55, 2018/2, p. 131-143.

BOGAERT Peter et MICHAUX Geneviève, « La protection administrative des données, l'hydre de Lerne du droit pharmaceutique européen », *Revue Trimestrielle de Droit Européen (RTDE)*, 01/01/2006, n° 1, p. 47-96.

BOTCHORICHVILI Nana, « Transferts de données personnelles hors de l'Union européenne – quelles nouveautés avec le RGPD ? », *Legicom*, n° 59, 2017/2, p. 39-46.

BOSSI Jeanne :
- « Comment organiser aujourd'hui en France la protection des données de santé », *RDSS*, 01/03/2010, n° 2, p. 208.
- « Le cadre juridique du partage d'informations dans les domaines sanitaire et médicosocial : état des lieux et perspectives », *Médecine et droit*, 01/01/2013, n° 118, p. 5-8.
- « La circulation des données de santé », *RGDM*, 2004, n° 4, p. 55-64.

BOUNEDJOUM Amira, SIMON François-Luc, « RGPD : quelles nouvelles règles en matière de responsabilité et quels impacts sur les contrats ? », *AJ Contrat*, 2018, p. 172.

BOURCIER Danièle, DE FILIPPI Primavera, « Vers un droit collectif sur les données de santé », *RDSS*, 2018, p. 444.

BOURGEOIS Matthieu, BOUNEDJOUM Amira :
- « L'émergence d'un droit des données », *Revue internationale de la compliance et de l'éthique des affaires*, 17/12/2015, n° 51-52, p. 12-13.
- « L'accès aux données », *Revue internationale de la compliance et de l'éthique des affaires*, 17/12/2015, n° 51-52, p. 14-15.
- « L'utilisation des données », *Revue internationale de la compliance et de l'éthique des affaires*, 17/12/2015, n° 51-52, p. 20-21.
- « La protection des données », *Revue internationale de la compliance et de l'éthique des affaires*, 17/12/2015, n° 51-52, p. 24-28.

BOURRET Rodolphe, DEBOST Claire, MARTINEZ Eric, VIALLA François, « Lorsque le respect des droits fondamentaux l'emporte [encore] sur la quête de la performance », *RDS*, 2014, n° 57, p. 864-868.

BOURRET Rodolphe, GIQUEL Chloé, MARTINEZ Eric, VIALLA François, « Les orientations du projet de loi de santé », *RDS*, 2014, n° 62, p. 1729 -1732.

BRACONNIER Stéphane (dir.), VARET Eléonore, PONS Yves, « La propriété des données

produites ou reçues par les cocontractants de l'Administration », *Contrats et Marchés publics*, 01/10/2015, n° 10, p. 85-86.

BRAS Pierre-Louis, « Union Européenne : Les systèmes de santé dans l'orbite de la gouvernance économique », *"Focus", Les Tribunes de la santé*, 2010/4, n° 29, p. 13-21.

BRECHAT Pierre-Henri, BRIOT Pascal, FOURY Christian, TEIL Alice, BRECHAT Nathalie, « Remporter les défis des systèmes de santé et d'Assurance maladie au XXIe siècle : l'expérience de la France et de l'Utah des Etats-Unis d'Amérique », *Journal de droit de la santé*, 01/01/2014, p. 19-30.

BRINGAUD Raphaël, « Les mutations de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés au nouvelles exigences communautaires de traitement des données personnelles en matière de santé », *RDS*, n° 82, 2018, p. 267-268.

BROUARD Benoît, « Utilisation des Big Data en santé : le cas des objets connectés », *Journal International de Bioéthique*, 2017/3, vol. 28, p. 27-30.

de BROUWER Frédéric, « Protection des données à caractère personnel : un nouveau cadre légal belge », *Revue de droit des affaires internationales*, 01/03/1999, p. 181-206.

CANTERO Isabelle :
- « Protection des données personnelles : un avenir rempli de nouvelles obligations ! », *Juris tourisme*, n° 207, 2018, p. 17.
- « Quel cadre pour le transfert des données personnelles hors de l'Union européenne ? », *Juris tourisme*, n° 207, 2018, p. 33.

CAPONETTI Lia, « Le cadre réglementaire européen en matière de services publics : législation, financement et contraintes », *Ciriec* (Centre international de recherches et d'information sur l'économie publique, sociale et coopérative), n° 2016/10.

CAPRIOLI Eric A., « Le Conseil d'Etat valide l'autorisation de la CNIL relative au traitement statistique de données de santé anonymisées au profit d'une entreprise privée », *Communication Commerce Electronique*, 01/07/2014, n° 7-8, p. 40-43.

CAPRIOLI Eric A. et CANTERO Isabelle, « Le choix d'un correspondant à la protection des données à caractère personnel (CPDCP) », *JCP E*, 22/06/2006, n° 25, p. 1104-1108.

CASTETS-RENARD Céline :
- « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data », *Revue Lamy de Droit de l'Immatériel*, 01/10/2014, supplément au n° 108, p. 38-45.
- « L'adoption du Privacy Shield sur le transfert des données personnelles », *Recueil Dalloz*, 04/08/2016, n° 28, p. 1696.
- « Adoption du Privacy Shield : des raisons de douter de la solidité de l'accord », *Dalloz IP/IT*, 18/10/2016, n° 10, p.444.

CHALTIEL Florence, « Le règlement général européen sur la protection des données », *Revue de l'Union européenne*, 2018, p. 249.

CHASSANG Gauthier, « E-santé, droit de l'union européenne et protection de la vie privée des personnes : vers l'émergence d'un « technodroit » spécifique au travers de la proposition de règlement général sur la protection des données personnelles ? », *Revue Lamy de Droit de l'Immatériel*, 01/10/2014, supplément au n° 108, p. 46-56.

CHEMTOB-CONCE Marie-Catherine, « La protection des données de santé à caractère personnel », *RGDM*, 01/06/2003, n° 10, p. 111-126.

CLEMENT-FONTAINE Mélanie :
- « La régulation de l'open data », *Legicom*, 01/03/2016, n° 56, p.113-120.
- « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *Legicom*, n° 59, 2017/2, p. 61-68.

CLUZEL-METAYER Lucie, « Les limites de l'open data », *AJDA*, 25/01/2016, n° 2, p. 102-107.

CNIL Veille, « « La CNIL dispose d'une capacité de régulation à « 360 degrés » grâce à une palette complète d'outils, essentielle à l'ère numérique ». – 3 questions à Isabelle Falque-Pierrotin, présidente de la CNIL », *JCP-G*, n° 42, 15/10/2018, 1096.

Conseil d'Etat, « Affaire du médiator : portée de la responsabilité de l'Etat », *Recueil Dalloz*, 24/11/2016, n° 40, p. 2346.

COUTELLEC Léo, WEIL-DUBUC Paul-Loup, « *Big data* ou l'illusion d'une synthèse par agrégation. Une critique épistémologique, éthique et politique », *Journal International de Bioéthique*, 2017/3, vol. 28, p. 63-79.

DAUBECH Lin, « La collecte des données de santé », *RGDM*, 2004, n° 4, p. 41-54.

DEBET A., « Protection des données personnelles – Libertés et protection des personnes, L. n° 2018-493, 20 juin 2018 – Etude », *JCP G*, n° 36, 03/09/2018, doctr. 907.

DEBOST Claire, « Publication du rapport sur la gouvernance et l'utilisation des données de santé, la promesse d'un entrebâillement de l'Open data dans le secteur de la santé ? », *RDS*, janvier 2014, n° 57, p. 947 à 949.

DEBOST Claire :
- « Quand les traitements de données relatives à l'état de santé sont légitimés par les plus hautes institutions françaises », *RDS*, 2015, n° 63, p. 128-129.
- « L'accès des industriels de la santé au Répertoire des Professionnels de Santé (RPPS) », *RDS*, 2014, n° 57, p. 917-918.

DELOUVEE Maxime, « Boire ou souscrire : il faut choisir ! », *RDS*, 2013, n° 52, p. 202-204.

DELPECH Xavier :
- « Numérique – Bientôt une loi sur la protection des données personnelles », *Juris tourisme*, n° 205, 2018, p. 11.
- « Associations – Réglementation – Publication de la loi relative à la protection des données personnelles », *Juris associations*, n° 583, 2018, p. 7.

DESMARAIS Pierre :
- « Quel régime pour la m-Health ? », *Communication Commerce Electronique*, 01/03/2013, n° 3, p. 15-18.
- « La réforme de l'open data suppose une approche globale ! », *JCP G*, 05/05/2014, n° 18, 528.
- « Open data santé, un rapport décevant pour un retard de transposition certain ? », *JCP A*, 08/09/2014, n° 36, 716.

DEVILLIER Nathalie :
- « Santé et Big data : l'émergence d'un droit d'infrastructure dans l'espace numérique », *Journal International de Bioéthique*, 2017/3, vol. 28, p. 51-56.
- « Les dispositions de la loi de modernisation de notre système de santé relatives aux données de santé », *Journal International de Bioéthique*, 2017/3, vol. 28, p. 57-61.

DOMIN Jean-Paul, « Le médecin, le patient et l'assureur : le développement de l'assurance en santé et ses conséquences sur la décision médicale », *Journal de gestion et d'économie médicales*, 4/2009, volume 27, p. 235-253.

DREES, « Intégration des causes de décès dans le SNDS », *site internet du SNDS*, https://www.snds.gouv.fr/SNDS/Actualites/Actu-12, 03/09/2018.

DREYFUS Nathalie, « Jusqu'où aller dans la collecte des données de santé ? », *L'Usine nouvelle*, n° 3405, semaine du 8 au 14 janvier 2015, p. 48. 47

DROUAULT-GARDRAT Paul et LOUVET Benoît, « Données personnelles, hébergeurs de données de santé : où en est-on ? », *Expertises des systèmes d'information*, 01/03/2013, n° 378, p. 94-96.

DUBOIS Lorette, GAULLIER Florence, « Publicité ciblée en ligne, protection des données à caractère personnel et eprivacy : un ménage à trois délicat », *Legicom*, n° 59, 2017/2, p. 69-102.

DUCROS Denis, NICOULES Valérie, CHEHOUD Haithem, BAYLE Annette, SOUCHE Arnaud, TANGUY Maëla, VALIERE Jean-Paul, CAYLA Françoise, GROSCLAUDE Pascale, « Les bases médico-administratives pour mesurer les inégalités sociales en santé », *Santé Publique,* 3/2015, Vol. 27, p. 383-394.

DUFOUR Olivia, « La constitutionnalisation du droit à la protection des données personnelles (à propos du rapport 2007 de la CNIL) », *La Gazette du Palais*, 28/05/2008, n° 149, p. 2-3.

EL BOUJEMAOUI Wafae, MAZARS Marie-France, « Maîtriser le socle du droit de la protection des données pour aborder l'application du Règlement européen (RGPD) », *Revue droit du travail*, 2018, p. 298.

ENCINAS de MUNAGORRI Rafael, « Santé et nouvelles technologies en Europe, synthèse et perspectives. Quelles recompositions du droit pour le XXIe siècle ? », *Revue Lamy droit de l'immatériel*, 01/12/2014, n° 110, p. 40-42.

ESPESSON-VERGEAT Béatrice, VASSALO Laurent, VIALLA François, BOLOTINA Marina, MAKLAKOVA Elena, BYK Christian, « La transparence : un instrument perfectible », *RGDM*, 01/06/2014, n° 51, p. 127-186.

EYNARD Jessica, « Une application systématique du RGPD ? », *Juris tourisme*, n° 207, 2018, p. 19.

FABER Stéphanie, « La transparence et le respect de la vie privée », *RGDM*, n° 51, 2014, p. 105-114.

FALISSARD Bruno, « Quelle inférence pour l'épidémiologie à l'heure des big data ? », *Revue française des affaires sociales*, 2017/4, p.127-132.

FAURAN Blandine, « Loi Informatique et Libertés et données de recherche dans le domaine de la santé », *La Gazette du Palais*, 09/06/2006, n° 160, p. 29-30.

FAUVARQUE-COSSON Bénédicte, MAXWELL Winston, « Protection des données personnelles décembre 2016 – mai 2018 », *D*. 2018, n° 19, p. 1033-1050.

FAUVARQUE-COSSON Bénédicte, « Protection des données personnelles », *D*., 2018, p. 1033.

FAVRO Karine, « La démarche de *compliance* ou la mise en œuvre d'une approche inversée », *Legicom*, n° 59, 2017/2, p. 21-28.

FERRAUD-CIANDET Nathalie, « Sécurité et confidentialité des données de santé dans l'Union européenne. Le cadre légal applicable aux dossiers médicaux électroniques nationaux », *Journal de droit européen*, 01/01/2009, n° 155, p. 12-14.

FRAYSSINET Jean, PEDROT Philippe, « La loi du 1er juillet 1994 relative au traitement des données nominatives ayant pour fin la recherche dans le domaine de la santé », *JCP G*, 21/12/1994, n° 51, p. 561-570.

FRAYSSINET Jean, « Traitement de données nominatives et recherche dans le domaine de la santé, analyse de la loi du 1er juillet 1994 », *Expertises des systèmes d'information*, 01/04/1995, n° 182, p. 145-149.

FRIEDRICH Clemmy Veille, « Droit à rectification : contrôle normal des décisions de la CNIL », *JCP-G*, n° 42, 15/10/2018, 1088.

GALLOUX Jean-Christophe et GAUMONT-PRAT Hélène :
- « Droits et libertés corporels. Janvier 2007-février 2008 », *D. 2008*, n° 21, p. 1435-1447.
- « Droits et libertés corporels, février 2008-décembre 2009 », *D. 2010*, n° 10, p. 604-619.
- « Droits et libertés corporels, janvier 2013 – janvier 2014 », *D. 2014*, p. 843.

GARCIA Jonathan, VERON Paul, « Le droit de la santé et la Question prioritaire de constitutionnalité : panorama mars 2010 – juin 2011 », *RDS*, 2011, n° 43, p. 483-503.

GAREL Pascal, « Santé en ligne : nouvelles étapes européennes », *La revue hospitalière de France*, n° 532, 2010/01-02, p. 35-36.

GIMBERT Virginie, CHAUFFAUT Delphine, « Les médicaments et leurs usages : comment favoriser une consommation adaptée ? », *note d'analyse du Commissariat général à la stratégie et à la prospective*, 03/2014, n° 09, 12 p.

GOLA Romain, « Le Règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *LEGICOM*, n° 59, 2017/2, p. 29-38.

GOURGUES Guillaume, MAZEAUD Alice, « Peut-on délibérer du Big Data en santé sans controverser ? Retour sur l'expérience d'un atelier citoyen français », *Revue française des affaires sociales*, 2017/4, p. 95-115.

GRANCHET Agnès, « Les nouvelles frontières de la vie privée », Légipresse, 01/11/2008, n° 256, p. 161-166.

GRIT Morgan :
- « Traitement des données de santé : allégement des formalités auprès de la Cnil », *RDS*, n° 79, 2017, p. 739-740.
- « Focus sur le règlement européen relatif à la protection des données à caractère personnel », *RDS*, n° 83, 2018, p. 340-341.
- « La CNIL met en demeure la CNAMTS pour manque de sécurité sur les traitements de données », *RDS*, n° 83, 2018, p. 489-490.
- « Lumière sur le projet de loi relatif à la protection des données personnelles », *RDS*, n° 84, 2018, p. 622-623.

GRYNBAUM Luc, « Loi « pour une République numérique », Ouverture des données et nouvelles contraintes », *JCP G*, 24/10/2016, n° 43-44, p. 1129.

GUERRIER Claudine, « La problématique juridique du scanner corporel », *Revue Lamy droit de l'immatériel*, 01/10/2011, n° 75, p. 76-85.

GUY Lambot, « Quand le juge administratif fait échec au droit de réutilisation des informations publiques », *JCP A*, 27/07/2015, n° 30-34, p. 2239.

HAGNERÉ Cyrille, « Le big data à l'agence centrale des organismes de sécurité sociale (ACOSS). Du concept à l'expérimentation », *Revue française des affaires sociales*, 2017/4, p. 141-149.

Institut de droit européen des Droits de l'Homme, « Les juridictions de l'Union européenne et les droits fondamentaux, Chronique de jurisprudence (2014) », *RTDH*, 01/07/2015, n° 103, p. 673-699.

JACQUE Jean-Paul, « Protection des données personnelles, Internet et conflits entre droits fondamentaux devant la Cour de justice », *RTDE*, 01/04/2014, n° 2, p. 283-288.

JEHL Joseph, « Conseil de l'Europe : tests génétiques aux fins d'assurance et protection des données », *JCP G*, 28/11/2016, n° 48, p. 1292.

JOB Jean-Marie, « La loi "Informatique et libertés" et les données de santé », *Revue Lamy droit de l'immatériel*, 01/01/2008, n° 34, p. 86-94.

KADAR Daniel, « L'hébergement des données de santé à caractère personnel : la question de l'agrément », *Journal des Sociétés*, 01/03/2013, n° 107, p. 26-37.

KALTENBACH Laure et LE GUAY Olivier, « Ces données personnelles qui valent de l'or »,

JCP E, 11/09/2014.

KASTLER Florian, « Union Européenne, Protection des données de santé, une réforme attendue », *« Focus », Les tribunes de la santé*, 2013/1, n° 38, p. 11-20.

KHODOSS Hélène, « L'exploitation des données de santé », *RGDM*, 30/09/2004, n° 4, p. 65-76.

KOUBI Geneviève, « *Le « méga-fichier » des titres électroniques sécurisés* », Etude, *JCP A*, 28/11/2016, n° 47.

de LAMBERTERIE Isabelle :
- « Protection de la vie privée et traitement des données relatives à la santé à l'heure européenne », *Médecine et droit*, 01/09/1996, n° 20, p. 6-12.
- « Qu'est-ce qu'une donnée de santé ? », *RGDM*, 30/09/2004, n° 4, p. 11-26.

LANGLET Virginie, « Nom de code : délégué à la protection des données », *Juris tourisme*, n° 207, 2018, p. 29.

LAUBIE Raphaëlle, « Le patient connecté ou les métamorphoses de la santé », *L'expansion Management Review*, 4/2011, n° 143, p. 24-31. A VERIFIER

LAUDE Anne :
- « Démocratie sanitaire, open data et Médiator », *Journal du droit de la santé et de l'Assurance maladie (JDSAM)*, Chronique 2, Droits des malades et bioéthique, n° 1 de 2014, p. 58 à 61.
- « De quelques problématiques relatives à l'ouverture des bases de données en santé », *Journal du droit de la santé et de l'Assurance maladie (JDSAM)*, Chronique 2, Droits des malades et bioéthique, 01/07/2014, n° 3, p. 30 à 34.
- « Introduction au colloque : Applis smartphone et santé : promesses et menaces », *Journal de droit de la santé et de l'Assurance maladie (JDSAM)*, 01/12/2014, p. 3-4.

LAVERDET Carole :
- « Données personnelles : bilan de 1995 et réforme de 2014 ? », *Revue Lamy du Droit de l'immatériel*, 01/05/2014, n° 104, p. 96 à 99.
- « Données personnelles : la sécurité des données à l'ère des objets connectés », *Expertises des systèmes d'information*, 01/06/2014, n° 392, p. 214-217.

LE BONNIEC Nina, « Vers une convergence des exigences constitutionnelles et européennes en matière de protection des données personnelles numériques », *JCP G*, n° 23, 04/06/2018, doctr. 655.

LE COZ Pierre, « Avis du CCNE à propos des questions soulevées par l'informatisation des données de santé », *RGDM*, 01/12/2010, n° 37, p. 199-204.

LE GAL Cécile, RAGE-ANDRIEU Virginie, « Hébergement des données de santé » et « Secret professionnel » dans la chronique « Droit de l'Internet », *JCP E*, 03/03/2011, n° 9, p. 1184.

LENOIR Noëlle, « Protection des données personnelles et responsabilités plurielles », *JCP-G*, n° 41, 08/10/2018, doctr. 1059.

LEROUX Vincent, « TIC et Gouvernance. Qualité, sécurité et continuité. Défis et bonnes pratiques », *Gestions hospitalières*, 2010/04, n° 495, p. 268-272.

LE ROY Marylou, ZOLYNSKI Célia, « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *Legicom*, n° 59, 2017/2, p. 105-113.

LESAULNIER Frédérique, « Internet, santé et données personnelles », *Médecine et Droit*, 01/01/2013, n° 118, p. 1-2.

LESSI Jean, conclusions du rapporteur public concernant la décision n° 385305, 1ère – 6ème chambre réunies, 20/05/2016.

LONGUET Christophe et al., « Comment améliorer le partage des données collectées lors des recherches menées dans les pays à ressources limitées ? Compte-rendu d'atelier, Veyrier-du-Lac, le 5 novembre 2015 », *Journal International de Bioéthique*, 2017/3, vol. 28, p. 31-38.

LOUIS Jean-Philippe, « Des hackers prennent en otage le système informatique d'un hôpital », *Les Echos*, 17/02/2016.

LOUVEAUX Sophie, « Application de la directive relative à la protection des données à caractère personnel à un projet de carte santé », *Lex électronica*, 01/09/1996, n° 2, p. 1-8.

LOUVET Benoît, « Données de santé. Réflexions à propos du Quantified Self », *Expertises des systèmes d'information*, 01/04/2015, n° 401, p. 149-152.

MACIEL-HIBBARD Marilia, « Protection des données personnelles et cyber(in)sécurité », *Politique étrangère*, 2018/2 (Eté), p. 55-66.

MAHMOUDI Nasséma, « Les nouvelles dispositions relatives aux données de santé à caractère personnel », *RDS*, n° 77, 2017, p. 470-471.

MAILLOLS-PERROY Anne-Catherine, « La protection des données de l'AMM », *RDS*, 2005, n° 5, 238-239.

MAINSIER-BOCHE Lorraine, « Hébergement des données de santé : bilan et perspectives de réforme », *Revue Lamy droit de l'immatériel*, 01/01/2015, n° 111, p. 37-43.

MAISL Herbert, « Informatique et libertés : de 1978 à 2004 », Communication Commerce électronique, 01/2005, n° 1.

MALLET-POUJOL Nathalie :
- « Droit à et droit sur l'information de santé », *RGDM*, 2004, n° 4, p. 77-96.
- « Protection des données personnelles et droit à l'information », *Legicom*, n° 59, 2017/2, p. 49-59.

MARINO Laure :
- « Le big data bouscule le droit », *Revue Lamy droit de l'immatériel*, 01/12/2013, n° 99, p. 55-58.
- « Le règlement européen sur la protection des données personnelles : une révolution ! » (PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 2016), *JCP-G*, 30/05/2016, n° 22, p. 628.

MARTIAL-BRAZ Nathalie, « La liberté d'accès des données de santé en question », *Les Petites Affiches*, 14/08/2014, n° 162, p. 13-18.

MARTINEZ Eric, « Le C.C.N.E., le "dossier médical personnel" (D.M.P.) et l'informatisation des données des santé (Avis n° 104 du C.C.N.E.) », *RDS*, 2008, n° 26, p. 695-702.

MATTATIA Fabrice, YAÏCHE Morgane :
- « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I) », *Revue Lamy droit de l'immatériel*, 01/04/2015, n° 114, p. 60-63.
- « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie II) », *Revue Lamy droit de l'immatériel*, 01/05/2015, n° 115, p. 63-65.
- « Être propriétaire de ses données personnelles : peut-on envisager un régime spécifique ? (partie II) », *Revue Lamy droit de l'immatériel*, 01/06/2015, n° 116, p. 41-44.

MENDOZA-CAMINADE Alexandra, « Big data et données de santé : quelles régulations juridiques ? », *Revue Lamy Droit de l'immatériel*, 01/06/2016, n° 127.

MEURIS Florence, « Les dangers du "soi quantifié" », *Communication Commerce Électronique*, 01/07/2014, n° 7-8, p. 2-2.

MESSI Pamela, « Big Brother : la surveillance de la population », *Les Tribunes de la santé*, 2010/4, n° 29, p. 69-74.

MICHEL David, « Le secret médical tire sa révérence en 2015 », *L'information psychiatrique*, 8/2015, vol. 91, p. 637-639.

MOREAUX Raphael, « Le Leem rejette l'idée d'une redevance pour l'accès au système national des données de santé », *TICpharma.com*, 25/01/2017.

MORLET-HAÏDARA Lydia et RAHAL-LÖFSKOG Délia, « La télémédecine et la protection des données de santé par la loi informatique et libertés », *RGDM*, n° 44, p. 333 à 346, septembre 2012.

MOURGUES Audrey, « Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires) JO n° 113 du 16 mai 2007 », *RDS*, 2007, n° 19, p. 669-670.

NIETO Adrien, « "Santé" et "Big data" : Google à l'origine d'une nouvelle ère d'encadrement des données personnelles de santé ? », *RDS*, 2015, n° 67, p. 649-650.

OCDE, « Strengthening health information infrastructure for health care quality governance, Good Practices, New Opportunities and Data Privacy Protection Challenges », *OECD Health policy Studies*, 2013.

OCHOA Nicolas, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA*, 01/11/2015, p. 1157-1173.

PAQUEL Norbert et BERTHAULT Denis, « Données de santé : Quoi ? Pour quoi ? Pour qui ? Comment ? », *La Gazette des communes*, 11/06/2013.

PARDAILHE-GALABRUN Annick, « La naissance de l'intime », *PUF*, 01/031/988, 528 p.

PASTOR Jean-Marc :
- « La protection des données personnelles va s'adapter au droit européen », *AJDA*, 2017, p. 2446.
- « Les nouvelles règles de protection des données personnelles », *AJDA*, 2018, p. 945.

PECHILLON Eric, « L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ? », *L'information psychiatrique*, 8/2015, volume 91, p. 645-649**.**

PERRAY Romain, « Traitement de données personnelles dans le cadre de recherches médicales : vers un allègement des formalités », *Revue Lamy droit de l'immatériel*, n° 24, 01/02/2007, p. 64-66.

PERRIN Gwendal, « Données de santé : le Conseil d'Etat repose la question de l'ouverture », *Argus de l'Assurance*, 23/05/2016.

PICARD Robert, « La santé participative est pour demain », *Annales des Mines – Réalités industrielles*, 2010/4, p. 15-22.

POLTON Dominique, RICORDEAU Philippe, « Le SNIIRAM et les bases de données de l'Assurance Maladie en 2011 », *CNAM*, 30/03/2011.

POLTON Dominique, « Le SNIIRAM et les bases de données de l'assurance maladie : fonctionnement, potentiel et limites », *CNAM*, 15/07/2013.

PROSSER William L., « Privacy », California Law Review 383, vol. 48, august 1960.

RAJOT Bénédicte, « Renforcement de la sécurité sanitaire du médicament et des produits de santé », *Responsabilité civile et assurances*, n° 1, 01/2012.

RIAL-SEBBAG Emmanuelle, « La gouvernance des Big data utilisées en santé, un enjeu national et international », *Journal International de Bioéthique*, 2017/3, vol. 28, p. 39-50.

REY Bénédicte, « Les intelligences numériques des informations personnelles. Vers un changement de perspective pour garantir le droit à la vie privée ? », *Les Cahiers du numérique*, 2014/1, vol. 10, p. 9-18.

RICHARD Jacky, « Le numérique et les données personnelles : quels risques, quelles potentialités ? », *RDP*, 01/01/2016, n° 1, p. 87-100.

RODRIGUES Jean-Marie, « Le Projet de médicalisation du Système d'Information – PMSI- : Méthode définition organisation », *Gestions Hospitalières*, 03/1983, n° 224, p. 205-209.

ROMANENS Jean-Louis, « Projet de loi relative à la santé : chronique d'une vie annoncée », *RDS*, 2015, n° 64, p. 201-212.

ROTOULLIE Jean Charles, « Responsabilité de la puissance publique – Mediator : responsabilité de l'Etat à partir de 1999 et faute des laboratoires Servier – Veille », *JCPG*, 21/11/2016, n° 47.

ROZENFELD Sylvie :
- « Open data : un mouvement inéluctable », *Expertises des systèmes d'information*, 01/11/2013, n° 385, p. 369-373.
- « La santé : des données très connectées », *Expertises des systèmes d'information*, 01/03/2015, n° 400, p. 91-95.

SAINT-AUBIN Thomas, « Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data). Les droits de l'opérateur de données sur son patrimoine numérique informationnel », *Revue Lamy droit de l'immatériel*, 01/03/2014, n° 102, p. 94-101.

SAINT-PAU Jean-Christophe, « Droit au respect de la vie privée. Définition conceptuelle du droit subjectif », *Jurisclasseur Communication*, Fascicule 34, 16/03/2016.

SAMARCQ Nicolas, BRIOIS Sébastien, « Données de santé à caractère personnel : les enjeux de la diffusion des TIC », *Expertises des systèmes d'information*, 01/11/2010, 352, p. 382-387. PAYANT

SAOUT Christian, « La crise de confiance dans le système de santé », *Les Tribunes de la santé*, 1/2009, n° 22, p. 119-132.

SAURET Jacques, « Economie des nouveaux systèmes d'information en santé », *Les Tribunes de la santé*, 2010/4, n° 29, p. 59-68.

SAUVE Jean-Marc, TABUTEAU Didier, DECOU-PAOLINI Rémi, VASILIU Irina, MIGNARD Jean-Pierre, BRAS Pierre-Louis, GIRARD Mylène, POLTON Dominique, DAUTIEU Thomas, STASSE François, METTENDORFF Martial, MADDALONE Patrick, SAOUT Christian, FOMBEUR Pascale, LAUDE Anne, MARTINEL Agnès, LUCAS Jacques, COMBREXELLE Jean-Denis, « Santé et protection des données », *Les entretiens du Conseil d'Etat en droit social*, colloque organisé le 01/12/2017 à Paris, actes non publiés.

SEGUR Philippe, « Confidentialité des données médicales à propos des enquêtes de santé », *AJDA*, 26/04/2004, n° 16, p. 858-862.

SERRE Jean-Louis, « Le CCTIRS : passé et présent. L'INDS & le CEREES : futur », *ADELF*, 09/09/2016.

de SILGUY Stéphanie, « Les objets connectés, un risque pour la protection de nos données personnelles », *Revue Lamy de Droit civil*, 01/10/2014, n° 119, p. 66 à 69.

SMALLWOOD Olivier, « L'amélioration de la qualité des soins par le truchement de l'informatisation de la santé », *RDS*, 2008, n° 25, p. 622-624.

TABUTEAU Didier, « Le secret médical et l'évolution du système de santé », *D.*, 12/11/2009, n° 39, p. 2629-2633.

TANGHE Hélène, GIBERT Paul-Olivier, « L'enjeu de l'anonymisation à l'heure du Big Data », *Revue française des affaires sociales*, 2017/4, p. 79-93.

TERESI Laurent :
- « Ouverture des données publiques les orientations de la Commission des lois du Sénat », *JCP A*, 27/07/2015, n° 30, p. 2241.
- « La CADA expose (enfin) sa doctrine en matière de tarification de la réutilisation des informations publiques », *JCPA*, 27/07/2015, n° 30-34, p. 2240.
- « L'open data et le droit de l'Union européenne », *Actualité juridique droit administratif (AJDA)*, 25/01/2016, n° 2, p. 87-91.

TERRIER Emmanuel :
- « La jurisprudence et la loi du 4 mars 2002 : impulsion ou anticipation ? », RGDM, 01/02/2004, p. 13-21.
- « Secret médical et Assurance vie : légitimation du refus de transmission des informations », *RDS*, 2005, n° 4, p. 134-136.

THIBERT Cécile, « Les données personnelles de santé accessibles aux assurances et laboratoires », *Le Figaro.fr*, 30/05/2016.

THIERACHE Corinne, « L'agrégation des données ouvertes dans le cadre de plateformes : les objets connectés dans le domaine de la santé », *Legicom*, 01/03/2016, n° 56, p.101-109.

THONNET Michèle, « L'e-santé, une mise en œuvre prometteuse et délicate », *Les Tribunes de la santé*, 4/2005, n° 9, p.61-73.

TILMAN Laora, « La délicate question de la propriété des données de santé », *RGDM*, 01/12/2014, n° 53, p. 49 à 54.

TILMAN Laora et FRIMAT Paul, « TIC et santé au travail : la protection des données de santé », *JCP S*, 26/11/2013, n° 48, p. 1453.

TOUZEIL-DIVINA Mathieu, « Les données à caractère personnel sont… strictement personnelles », *JCPG*, 27/06/2016, n° 26.

UNESCO International Bioethics Committee, « Preliminary draft report of the IBC on Big data and health », *Journal International de Bioéthique*, 2017/3, vol. 28, p. 81-111.

VACARIE Isabelle :
- « L'hébergement des données de santé : entre contrat et statut », *RDSS*, 2002, p. 695.
- « La finalité des traitements de données de santé », *RGDM*, 30/09/2004, n° 4, p. 27-34.

VARET Vincent, « L'ouverture des informations publiques au regard de la propriété intellectuelle », *Legicom*, 01/03/2016, n° 56, p.25-40.

VIALLA François, « Le droit au respect de la vie privée à l'épreuve de la relation de soin », Mélanges en l'honneur du professeur Claire NEIRINCK, *LexisNexis*, coll. Mélanges, 01/08/2015, p. 133-156.

VERON Michel, « Données à caractère personnel relatives à la santé », *Droit pénal*, 01/07/2014, n° 7, p. 26-28.

VESSIER Armelle, « Droit au respect de la vie privée ; Note sous Cour européenne des droits de l'homme, première section, 21 juin 2011, requête numéro 30194/09 », *Journal du droit international (Clunet)*, 01/07/2012, n° 2012-3, p. 1036-1038.

VILLEDIEU Anne-Laure, « Protection des bases de données : la délicate preuve d'investissements spécifiques ; Notes sous Cour de cassation, première Chambre civile, 12 novembre 2015, pourvoi numéro 14-14.501 », *Option Finance*, 08/02/2016, n° 1352, p.29.

VINEY François, « La loi relative à la protection des données personnelles », *AJ Famille*, 2018, p. 366.

VOSS W. Gregory, « Le concept des données à caractère personnel : divergences transatlantiques Safe Harbor et Privacy Shield », *Dalloz IP/IT*, 10/03/2016, n° 3, p.119.

VULLIET-TAVERNIER Sophie, « De l'anonymat dans le traitement des données de santé », *Médecine et Droit*, 01/01/2010, n° 100-101, p. 22-25.

WAREN Samuel D. et BRANDEIS Louis D., « The Right To Privacy », *Harward Law review*, vol. 4, 1890, P192-220.

WMA General Assembly, « WMA Declaration of Taipei on ethical considerations regarding health databases and biobanks. Adopted by the 53rd WMA General Assembly, Taipei, Taiwan, October 2016 », *Journal International de Bioéthique*, 2017/3, vol. 28, p. 113-117.

WEINBAUM Noémie, DELAMORINIERE Marie, « Le statut des données dans les contrats de Market data », *Expertises des systèmes d'information*, 01/10/2014, n° 395, p. 340-345.

WYBER Stephen, « Care.data : une expérience d'économie politique des données de santé en Angleterre », *Informations sociales*, 2015/5, n° 191, p.96-104.

ZORN-MACREZ Caroline, « "Chronique martienne" des données de santé numérisées. Brèves observations sur une réglementation surréaliste », *RDS*, 2010, n° 36, p. 331-342.

[Autres]

Assemblée générale de l'Institut des données de santé, Charte de déontologie, 12/12/2008.

Assemblée médicale mondiale, « Déclaration de l'AMM sur les considérations éthiques concernant les bases de données de santé et les biobanques » adoptée par la 53e Assemblée générale à Washington, Etats-Unis, en 2002 et révisée par la 67e Assemblée générale à Taipei, Taiwan, le 22/10/2016.

CCMSA, « Chiffres utiles de la MSA », *Edition 2017*, 2017.

Initiative de Budapest pour l'accès ouvert lancée lors du congrès des 1er et 2 décembre 2001 par les institutions les plus avancées dans le domaine des archives ouvertes et diffusée le 14 février 2002.

Initiative Transparence Santé, « Liberté pour les données de santé », *Manifeste*, 2013.

Institut des données de santé, « Processus d'élaboration de l'arrêté permettant l'utilisation des données anonymisées de l'assurance maladie obligatoire ».

Institut des données de santé, « Accès aux données du SNIIRAM : mode d'emploi ».

Institut des données de santé, « Worklfow sur les demandes d'utilisation des données du SNIIRAM », 03/05/2017.

Institut national des données de santé :
- « Worklfow sur les demandes d'utilisation des données du SNDS », 04/06/2018.
- « Workflow sur les demandes d'utilisation des données du SNDS », 06/11/2018.
- « Etudes sous MR », 25/11/2018.

Insee, « Tableaux de l'économie française », *Collection Insee Références*, édition 2016.

Déclaration de Berlin sur le libre accès à la connaissance définie lors du congrès de Berlin du 22 octobre 2003 tenu à la société Max-Planck.

RSI, « L'essentiel du RSI », *Edition 2016 – Données 2015*, Septembre 2016.

VAN ROEKEGHEM Frédéric, GIN François, LIGER Dominique, COHEN-SOLAL Jean-Martin, LEQUOY Jean-François, FAURE Jean-Louis, Charte d'engagements entre l'Assurance Maladie Obligatoire et les assureurs maladie complémentaires pour le partage et la mise en commun des données de remboursement agrégées ou individuelles anonymisées issues de leurs systèmes d'information, 07/10/2010, 4 p.

[Décisions de justice et délibérations]

Cour européenne des droits de l'Homme

CEDH, 8 janvier 2009, n° 29002/06, Schlumpf c/ Suisse.

Conseil constitutionnel

Conseil constitutionnel, 22 mars 2012, n° 2012-652 DC.

Conseil constitutionnel, 7 décembre 2000, *Loi d'orientation pour l'outre-mer*, n° 2000-435 DC.

Conseil constitutionnel, 21 décembre 1999, n° 99-422 DC.

Conseil constitutionnel, 16 décembre 1999, n° 99-421 DC.

Conseil constitutionnel, 9 novembre 1999, n° 99-419 DC.

Conseil constitutionnel, 23 juillet 1999, n° 99-416 DC.

Conseil constitutionnel, 18 janvier 1995, n° 94-352 DC.

Conseil Constitutionnel, 25 juillet 1979, n° 79-105 DC.

Tribunal des conflits

Tribunal des conflits, 8 février 1873, 00012, recueil Lebon, Blanco.

Conseil d'Etat

Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, recueil Lebon, Celtipharm.

Conseil d'Etat, 10e et 9e sous-sections réunies, 26 mai 2014, n° 354903, recueil Lebon, Société IMS Health c/ CNIL.

Conseil d'Etat, 13 juin 1980, 17995, recueil Lebon, Madame Bonjean.

Conseil d'Etat, Assemblée, 28 mai 1954, 28238 28493 28524 30237 30256, recueil Lebon, Barel.

Conseil d'Etat Section, 9 mars 1951, 92004, recueil Lebon, Société des concerts du conservatoire.

Conseil d'Etat Section, 30 mai 1930, 06781, recueil Lebon, Chambre syndicale du commerce en détail de Nevers.

Conseil d'Etat, 4 mars 1910, 29373, recueil Lebon, Thérond.

Conseil d'Etat, 6 février 1903, 07496, recueil Lebon, Terrier.

Conseil d'Etat, 10 janvier 1902, 94624, recueil Lebon, Compagnie Nouvelle du Gaz de Déville-lès-Rouen.

Conseil d'Etat, 29 mars 1901, 94580, recueil Lebon, Casanova.

Première instance

T. civ. Seine, 16 juin 1858, DP, 1858, jurisprudence, p.62.

Commission nationale l'informatique et des libertés - CNIL

Délibération n° 2019-11 du 31 janvier 2019 modifiant la délibération n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

Délibération n° 2018-348 du 8 novembre 2018 habilitant des agents de la CNIL à procéder à des missions de vérification.

Délibération n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

Délibération n° 2018-320 du 20 septembre 2018 habilitant des agents de la CNIL à procéder à des missions de vérification.

Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPO).

Délibération n° 2018-317 du 20 septembre 2018 portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPO).

Délibération n° 2018-290 du 12 juillet 2018 habilitant des agents de la CNIL à procéder à des missions de vérification.

Délibération n° 2018-284 du 21 juin 2018 portant avis sur un projet de décret pris pour l'application de la 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 (saisine n° AV 18012134).

Délibération n° 2018-257 du 7 juin 2018 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 dispositions par l'ATIH par l'intermédiaire d'une solution sécurisée (MR-006).

Délibération n° 2018-256 du 7 juin 2018 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).

Délibération n° 2018-155 du 3 mai 2018 portant homologation de la méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre de la recherche n'impliquant pas la personne humaine, des études et évaluations dans le domaine de la santé (MR-004).

Délibération n° 2018-154 du 3 mai 2018 portant homologation de la méthodologie de référence relative au traitement des données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé ne nécessitant pas le recueil du consentement de la personne concernée (MR-003) et abrogeant la délibération n° 2016-263 du 21 juillet 2016.

Délibération n° 2018-153 du 3 mai 2018 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé avec recueil du consentement de la personne concernée (MR-001) et abrogeant la délibération n° 2016-262 du 21 juillet 2016.

Délibération n° 2018-134 du 12 avril 2018 portant homologation de conditions de mise à disposition de l'échantillon généraliste des bénéficiaires (EGB) et des bases de données thématiques appelées « datamarts » du Système National d'Information Inter Régimes de l'Assurance Maladie (SNIIRAM).

Décision n° MED-2018-006 du 8 février 2018 mettant en demeure la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés.

Délibération n° 2018-026 du 25 janvier 2018 habilitant des agents de la CNIL à procéder à des missions de vérification.

Décision du 6 janvier 2018 portant habilitation de certains agents de la Commission nationale de l'informatique et des libertés à effectuer les visites ou les vérifications portants sur les traitements relevant de l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978.

Délibération n° 2017-287 du 23 novembre 2017 habilitant des agents de la CNIL à procéder à des missions de vérification.

Délibération n° 2017-197 du 6 juillet 2017 habilitant des agents de la CNIL à procéder à des missions de vérification.

Délibération n° 2017-150 du 9 mai 2017 habilitant des agents de la CNIL à procéder à des missions de vérification.

Délibération n° 2016-316 du 13 octobre 2016 portant avis sur un projet de décret en Conseil d'Etat relatif au Système national des données de santé.

Délibération n° 2016-263 du 21 juillet 2016 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé ne nécessitant pas le recueil du consentement exprès ou écrit de la personne concernée (MR-003).

Délibération n° 206-262 du 21 juillet 2016 portant modification de la méthodologie de référence pour les traitements de données personnelles opérés dans le cadre des recherches biomédicales (MR-001).

Délibération n° 2015-256 du 16 juillet 2015 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des études non interventionnelles de performances en matière de dispositifs médicaux de diagnostic in vitro (MR-002).

Délibération n° 2011-246 du 8 septembre 2011 autorisant la mise en œuvre par la société CELTIPharm d'un traitement de données à caractère personnel ayant pour finalité la réalisation d'études épidémiologiques à partir de données issues des feuilles de soins électroniques anonymisées à bref délai.

Délibération n° 2007-194 du 10 juillet 2007 autorisant la mise en place généralisée par la Caisse nationale d'assurance maladie des travailleurs salariés d'un traitement permettant aux médecins d'accéder aux données relatives aux prestations servies aux bénéficiaires de l'assurance maladie. Historique des remboursements ou WEB MEDECIN.

Décision du 5 janvier 2006 portant homologation d'une méthodologie de référence pour les traitements de données personnelles opérées dans le cadre des recherches biomédicales (méthodologie de référence MR-001).

Délibération n° 01-54 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 oeuvre du Système National d'Information Inter-Régimes de l'Assurance Maladie NIIRAM).

Délibération n° 01-011 du 8 mars 2001 portant adoption d'une recommandation sur les sites de santé destinés au public.

[Textes normatifs]

Droit international

Convention sur la cybercriminalité du 23 novembre 2001, Conseil de l'Europe.

Convention de sauvegarde des droits de l'homme et libertés fondamentales du 4 novembre 1950.

Préambule à la Constitution de l'Organisation mondiale de la Santé, tel qu'adopté par la Conférence internationale sur la Santé, New York, 19 juin -22 juillet 1946 ; signé le 22 juillet 1946 par les représentants de 61 Etats. (Actes officiels de l'Organisation mondiale de la Santé, n° 2, p. 100) et entré en vigueur le 7 avril 1948.

Droit européen

Règlement

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

Directives

Directive 2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public.

Directive 2003/98/CE du 17 novembre 2003 concernant la réutilisation des informations du secteur public.

Directive 95/46/CE 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.

Groupes de travail

Groupe de travail « Article 29 » sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 », adoptées le 4 avril 2017 et modifiées en dernier lieu le 4 octobre 2017.

Groupe de travail « Article 29 » sur la protection des données, « Lignes directrices concernant les délégués à la protection des données (DPD) », adoptées le 13 décembre 2016 et modifiées en dernier lieu le 5 avril 2017.

Groupe de travail « Article 29 » sur la protection des données, « Working Document on the processing of personal data relating to health in electronic health records (EHR) », février 2007.

Droit français

Lois

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, JORF n° 0141 du 21/06/2018.

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF n° 0235 du 08/10/2016.

Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, JORF n° 0022 du 27/01/2016.

Loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public, JORF n° 0301 du 29/12/2015.

Loi n° 2014-344 du 17 mars 2014 relative à la consommation, JORF n° 0065 du 18/03/2014.

Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine, JORF n° 0056 du 06/03/2012.

Loi n° 2011-2012 du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé, JORF n° 0302 du 30/12/2011.

Loi n° 2011-334 du 29 mars 2011 relative au Défenseur des droits, JORF n° 0075 du 30 mars 2011.

Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, JORF n° 0167 du 22/07/2009.

Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, JORF n° 0190 du 17/08/2004.

Loi n° 2004-806 du 9 août 2004 relative à la politique de santé, JORF n° 0185 du 11/08/2004.

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n° 0182 du 07/08/2004.

Loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle, JORF n° 0172 du 28/07/1999.

Loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale pour 1999, JORF n° 300 du 27/12/1998.

Loi n° 94-548 du 1 juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n° 152 du 02/07/1994.

Loi n° 92-1336 du 16 décembre 1992 relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur, JORF n° 0298 du 23/12/1992.

Loi n° 91-748 du 31 juillet 1991 portant réforme hospitalière, JORF n° 179 du 02/08/1991.

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, dite loi "CADA" (Commission d'accès aux documents administratifs), JORF du 18/07/1978.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF 07/01/1978.

Loi du 11 mai 1868 sur la presse.

Loi du 26 mai 1819 relative aux crimes et aux délits commis par la voie de presse ou par tout autre moyen de communication.

Ordonnances et rapports associés

Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, JORF n° 0288 du 13/12/2018.

Rapport au Président de la République relatif à l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, JORF n° 0288 du 13/12/2018.

Ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, JORF n° 0011 du 13/01/2017.

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 13/01/2017.

Ordonnance n° 2017-45 du 19 janvier 2017 relative aux conditions d'accès aux données couvertes par le secret médical ou le secret industriel et commercial de l'Autorité de sûreté nucléaire et de l'Institut de radioprotection et de sûreté nucléaire et à la mutualisation de certaines fonctions d'agences sanitaires nationales, JORF n° 0017 du 20/01/2017.

Rapport au Président de la République relatif à l'ordonnance n° 2017-45 du 19 janvier 2017 relative aux conditions d'accès aux données couvertes par le secret médical ou le secret industriel et commercial de l'Autorité de sûreté nucléaire et de l'Institut de radioprotection et de sûreté nucléaire et à la mutualisation de certaines fonctions d'agences sanitaires nationales, JORF n° 0017 du 20/01/2017.

Ordonnance n° 2016-462 du 14 avril 2016 portant création de l'Agence nationale de santé publique, JORF n° 0089 du 15/04/2016.

Ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration, JORF n° 0248 du 25/10/2015.

Ordonnance n° 2000-548 du 15 juin 2000 relative à la partie Législative du code de la santé publique, JORF n° 0143 du 22/06/2000.

Décrets

Décret n° 2018-1056 du 29 novembre 2018 complétant le décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé », JORF n° 0278 du 01/12/2018.

Décret n° 2018-687 du 1er août 2018 pris pour l'application de la 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, JORF n° 0177 du 03/08/2018.

Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel, JORF n° 0049 du 28/02/2018.

Décret n° 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé, JORF n° 0075 du 29/03/2017.

Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé », JORF n° 0301 du 28/12/2016.

Décret n° 2016-1872 du 26 décembre 2016 modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n° 0301 du 28/12/2016.

Décret n° 2016-1537 du 16 novembre 2016 relatif aux recherches impliquant la personne humaine, JORF n° 0267 du 17/11/2016.

Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité, JORF n° 0254 du 30/10/2016.

Décret n° 2016-1036 du 28 juillet 2016 relatif au principe et aux modalités de fixation des redevances de réutilisation des informations du secteur public, JORF n° 0176 du 30/07/2016

Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires), JORF n° 0113 du 16/05/2007.

Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n° 0247 du 22/10/2005.

Décret n° 2003-959 du 7 octobre 2003 portant création du Haut Conseil pour l'avenir de l'assurance maladie, JORF du 08/10/2003.

Décret n° 2002-1284 du 22 octobre 2002 relatif à l'organisation et au fonctionnement de l'Agence technique de l'information sur l'hospitalisation, modifiant le code de la santé publique, JORF, n° 250 du 25/10/2002.

Décret n° 2000-1282 du 26 décembre 2000 portant création de l'Agence technique de l'information sur l'hospitalisation et modifiant le code de la santé publique, JORF n° 301 du 29/12/2000.

Décret n° 95-682 du 9 mai 1995 pris pour l'application du chapitre V bis de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et modifiant le décret n° 78-774 du 17 juillet 1978, JORF n° 0110 du 11/05/1995.

Arrêtés

Arrêté du 10 janvier 2018 portant approbation d'un avenant modifiant la convention constitutive du groupement d'intérêt public (Institut national des données de santé », JORF n° 0014 du 18/01/2018.

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, JORF n° 0172 du 25/07/2017.

Arrêté du 5 mai 2017 portant nomination au Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé, JORF n° 0110 du 11/05/2017.

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 », JORF n° 0096 du 23/04/2017.

Arrêté du 18 avril 2017 modifiant l'arrêté du 6 février 2009 modifié portant création d'un traitement de données à caractère personnel dénommé « Répertoire partagé des professionnels intervenant dans le système de santé » (RPPS), JORF n° 0093 du 20/04/2017.

Arrêté du 6 avril 2017 portant fixation du modèle décrivant les caractéristiques des traitements portant sur des données individuelles du système national de santé, JORF n° 0090 du 15/04/2017.

Arrêté du 6 avril 2017 portant fixation du modèle décrivant les informations concernant les habilitations à accéder aux données du système national de santé, JORF n° 0090 du 15/04/2017.

Arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé, JORF, n° 0071 du 24/03/2017.

Arrêté du 6 octobre 2016 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, JORF n° 0244 du 19/10/2016.

Arrêté du 14 février 2014 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, JORF n° 0052 du 02/03/2014.

Arrêté du 19 juillet 2013 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, JORF n° 0187 du 13/08/2013.

Arrêté du 7 septembre 2012 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, JORF n° 0245 du 20/10/2012.

Arrêté du 11 juillet 2012 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, JORF n° 0171 du 25/07/2012.

Arrêté du 1er décembre 2011 relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie, JORF n° 0019 du 22/01/2012.

Arrêté du 6 février 2009 portant création d'un traitement de données à caractère personnel dénommé « Répertoire partagé des professionnels de santé » (RPPS), JORF n° 0034 du 10/02/2009.

Arrêté du 16 octobre 2008 relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie, JORF n° 0252 du 28/10/2008.

Arrêté du 30 avril 2007 portant approbation du groupement d'intérêt public « Institut des données de santé », JORF n° 109 du 11/05/2007.

Arrêté du 26 septembre 2006 modifiant l'arrêté du 20 juin 2005 relatif à la mise en oeuvre du Système national d'information interrégimes de l'assurance maladie, JORF n° 244 du 20/10/2006.

Arrêté du 20 juin 2005 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, JORF n° 192 du 19/08/2005.

Arrêté du 11 avril 2002 relatif à la mise en œuvre du Système national d'information inter-régimes de l'assurance maladie, JORF n° 89 du 16/04/2002.

Arrêté du 22 juillet 1996 relatif au recueil et au traitement des données d'activité médicale, visées à l'article L. 710-6 du code de la santé publique, par les établissements de santé visés à l'article L. 710-16-2 du même code et à la transmission, visée à l'article L. 710-7 du code de la santé publique, aux agences régionales de l'hospitalisation, aux organismes d'assurance maladie et à l'Etat d'informations issues de ce traitement, JORF n° 173 du 26/07/1996.

Arrêté du 20 septembre 1994 relatif au recueil et au traitement des données d'activité médicale et de coût, visées à l'article L. 710-5 du code de la santé publique, par les établissements de santé publics et privés visés aux articles L. 714-1, L. 715-5 du code de la santé publique et aux articles L. 162-23, L. 162-23-1 et L. 162-25 du code de la sécurité sociale et à la transmission aux services de l'Etat et aux organismes d'assurance maladie d'informations issues de ces traitements, JORF n° 242 du 18/10/1994.

Circulaires

Circulaire DH/PMSI relative à la généralisation du programme de médicalisation des systèmes d'information (PMSI) et à l'organisation de l'information médicale dans les hôpitaux publics, n° 303, 24/07/1989.

Circulaire DH/DSS/95 relative à la généralisation du dispositif technique, expérimenté en région Languedoc-Roussillon, de mesure de l'activité et des coûts des établissements hospitaliers sous compétence tarifaire de l'Etat, à l'aide des informations provenant du système d'information médicalisé, n° 23, 10/05/1995.

Protocoles

Protocole inter-régimes du 8 juin 2012 relatif au système national d'information interrégime de l'assurance maladie, BO Santé – Protection sociale – Solidarité n° 2013/8 du 15/09/2013.

Avenant n° 1 du 16 mai 2005 au protocole inter-régimes du 15 octobre 2001 relatif au système national d'information interrégime de l'assurance maladie, BO Santé – Protection sociale – Solidarité n° 2005/10 du 15/11/2005.

Protocole inter-régimes du 15 octobre 2001 relatif au système national d'information interrégime de l'assurance maladie, BO Santé – Protection sociale – Solidarité n° 2002/14 du 07/04/2002.

Vocabulaire

Vocabulaire de l'informatique, JORF n° 0193 du 22/08/2014.

Vocabulaire de l'informatique et du droit, JORF n° 0103 du 03/05/2014.

[Sites internet]

Sites nationaux

assemblee-nationale.fr

atih.sante.fr

cada.fr

cnil.fr

etalab.gouv.fr

gouvernement.fr/action/la-loi-de-sante

health-data-hub.fr

indsante.fr

insee.fr

senat.fr

snds.gouv.fr

transparence.sante.gouv.fr

Sites de documentation

bdsp.ehesp.fr (Banque de données en santé publique de l'Ecole des Hautes Etudes en Santé Publique)

bnds.fr (Bibliothèque numérique de droit de la santé et d'éthique médicale)

cairn.info.fr

dalloz.fr

doctrinalplus.fr

droit-medical.com

lamyline.lamy.fr

laquatradure.net

lexisnexis.com

opendatasante.com (site d'Initiative transparence santé)

INDEX

Les nombres renvoient aux numéros de paragraphe

-A-

Accès :

- Coût : 62, 416 s., 555.
- Demandeurs privés à but lucratif :
    - Arguments favorables : 485 s., 489 s., 538 s., 542 s. 556 s.
    - Autorisation :
        - Procédure Initiale :
            - Exceptions officielles : 468 s., 474 s.
            - Fondement : 456 s., 487.
        - Procédure Nouvelle :
            - Finalités exclues : 496.
            - Fondement : 494 s.
        - Utilisation : 548 s.
    - Interdiction :
        - Fragilités : 465, 471, 502 s., 513 s., 518 s.
        - Principe : 255, 462 s.
- Permanent :
    - Bénéfices : 106, 122 s.
    - Bénéficiaires :
        - Liste : 104 s.
        - Sélection : 178 s., 227.
    - Expérimentation : 107.
    - Sécurité : 192 s., 223 s.
    - Utilisation : 205 s.
- Sélectif :
    - Bénéficiaires : 222, 252 s.
    - Délais :
        - Officiels : 324 s., 333 s., 386.
        - Réels : 379 s., 387 s., 429 s.
    - Finalités :
        - Autorisées : 275 s.
        - Interdites : 281 s.
    - Principes : 283 s.
    - Procédure :
        - Initiale : 302 s.
            - Complexité : 366 s.
        - Nouvelle : 331 s.
            - Complexité : 403 s., 411 s., 433.
    - Sécurité : 302, 436 s.

    - Utilisation : 361 s.
- Simplifiés :
    - Méthodologies de référence : 325, 413, 553.
    - Réformés : 413, 420 s., 551 s.

-B-

Base de données :

- Bénéfice : 94.
- Contenu :
    - PMSI (définition) : 23.
    - SNIIRAM (définition) : 22.
    - SNDS : 414 s.,
- Finalité :
    - PMSI : 23.
    - SNIIRAM : 95
    - SNDS : 161
- Volume : 22, 93, 238, 373,

Big data **:** v. Donnée / Données massives

-C-

CNIL :

- Agents :
    - Habilitation : 315, 320.
    - Nombre : 398, 434.
- Contrôle : 311 s., 434.

Conseil :

- Constitutionnel : 56 s.
- d'Etat : 490 s., 501 s., 510.

Correspondant « informatique et libertés » :

- Caractéristiques : 265.
- Missions : 263.

-D-

Délégué à la protection des données :

- Caractéristiques : 265.
- Missions : 266 s., 339.

- Nomination :
    - Acte : 130 s., 263 s.
    - Obligation : 264 s.
- Sous-traitant : 265.

Donnée :

- Notion : 10 s.
- Agrégée :
    - Accès : 143.
- Conservation :
    - Durée : 140, 148 s.
- Croisement : 142, 150.
- Donnée à caractère personnel :
    - Notion : 28 s.
    - Anonymisée : 36 s., 139 s., 472, 490 s.
    - Nominative : 32 s.
- Donnée de santé :
    - Notion : 16 s.
    - Anonyme : 40 s.
    - Caractère personnel : 27 s.
    - Complexe : 372 s.
    - Nominative : 273 s., 291.
    - Organisation : 372 s., 396 s.
    - Protection : 58 s.
    - Publique : 44 s.
- Données massives :
    - Notion : 77 s.
    - Risque : 79 s., 528 s.
- Données ouvertes :
    - Notion : 69 s.
    - Risques : 524 s.

-E-

EGB (Echantillon Généraliste des Bénéficiaires) :

- Notion : 148.
- Accès : 552.
- Elargissement : 164.
- Finalité : 158.

Ethique : 49 s., 192, 284 s., 529.

-I-

Intérêt public :

- Groupement : 110, 306, 362.
- Objectif : 122 s., 145 s., 157, 274, 331, 464 s.

-M-

Mediator : 2, 149, 186, 542.

-O-

***Open data* :** v. Donnée / Données ouvertes

Organismes complémentaires d'assurance maladie : 474 s., 487 s.

-P-

Pharmacovigilance : 50, 217, 278.

PMSI : v. Base de données

Principe de précaution : 521, 524 s.

Profondeur : 151.

Pseudonymisation :

- Notion : 36 s.
- Risque : 153.

- R-

RGPD :

- Contenu :
  - Donnée de santé à caractère personnel : 19 s.
  - Protection de la vie privée : 5.
  - Protection des données personnelles : 263 s.
  - Sanctions : 292 s.
- Impact : 337 s., 556 s.

- S-

Santé : 13 s.

Sanction : 288 s.

Sécurité :

- Absence d'évaluation : 519 s.
- Audit : 438, 561.
- Piratage : 194, 543.
- Référentiel : 152.
- Secret professionnel : 286, 291, 320.

Service :

- Intérêt général (d') ou Intérêt économique général (d') : 100.

SNDS : v. Base de données

SNIIRAM : v. Base de données

-T-

Transparence :

- Notion : 72 s.
- Opportunités : 49 s.
- Risques : 53 s.

-V-

Vie privée :

- Notion : 54 s.
- Protection :
    - Notion : 1 s., 55 s.
    - Défense : 112.

ANNEXES

Annexe 1 : Arrêté du 11 avril 2002 relatif à la mise en œuvre du système national d'information inter-régimes de l'assurance maladie p. 472

Annexe 2 : Arrêté du 20 juin 2005 relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie p. 476

Annexe 3 : Arrêté du 19 juillet 2013 relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie p. 480

Annexe 4 : Décret n°2016-1871 relatif au traitement de données à caractère personnel dénommé « système national des données de santé » p. 484

Annexe 5 : Conseil d'Etat, 1ère-6e chambre réunies, 20 mai 2016, n° 385305, recueil Lebon, Celtipharm p. 492

Annexe 6 : Schémas du circuit des demandes d'accès au SNDS p. 496

Annexe 7 : Schémas des procédures d'accès simplifiées au SNDS p. 498

ANNEXE 1 : Arrêté du 11 avril 2002 relatif à la mise en œuvre du système national d'information inter-régimes de l'assurance maladie

NOR: MESS0220842A

ELI: https://www.legifrance.gouv.fr/eli/arrete/2002/4/11/MESS0220842A/jo/texte

La ministre de l'emploi et de la solidarité,
Vu le code de la santé publique, notamment ses articles L. 6113-8 et L. 6113-9 ;
Vu le code de la sécurité sociale, notamment ses articles L. 115-2, L. 115-4, L. 161-28, L. 161-28-1 à L. 161-28-4 et L. 161-29 ;
Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière statistique ;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
Vu la loi n° 93-8 du 4 janvier 1993 relative aux relations entre les professions de santé et l'assurance maladie ;
Vu l'avis du comité interministériel de coordination mentionné à l'article R. 114-1 du code de la sécurité sociale en date du 1er octobre 2001 ;
Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 18 octobre 2001 portant le numéro 01-054,
Arrête :

Article 1 En savoir plus sur cet article...

Est approuvé le protocole du 15 octobre 2001 définissant les modalités de gestion et de renseignement du système national d'information inter-régimes de l'assurance maladie (SNIIRAM), signé par la Caisse nationale de l'assurance maladie des travailleurs salariés, la Caisse centrale de mutualité sociale agricole et la Caisse nationale d'assurance maladie et maternité des travailleurs non salariés des professions non agricoles.

Article 2 En savoir plus sur cet article...

Les traitements mis en oeuvre dans le cadre du système national d'information inter-régimes de l'assurance maladie ont pour finalités :
1° D'améliorer la qualité des soins, notamment par la comparaison des pratiques aux référentiels, au sens de l'article L. 162-12-15 du code de la sécurité sociale, et moyennes professionnels ;
2° De contribuer à une meilleure gestion de l'assurance maladie, notamment par :
- la connaissance des dépenses de l'ensemble des régimes d'assurance maladie par circonscription géographique, par nature de dépense, par catégorie de professionnels responsables de ces dépenses et par professionnel ou établissement ;
- l'évaluation des transferts entre enveloppes correspondant aux objectifs sectoriels de dépenses fixés, en fonction de l'objectif national de dépenses d'assurance maladie, dans le cadre de la loi annuelle de financement de la sécurité sociale ;
- l'analyse quantitative des déterminants de l'offre de soins et la mesure de leurs impacts sur

l'évolution des dépenses d'assurance maladie ;
3° De transmettre aux prestataires de soins les informations pertinentes relatives à leur activité, à leurs recettes et, s'il y a lieu, à leurs prescriptions.

Article 3 En savoir plus sur cet article...

Les informations nécessaires à l'établissement du système national d'information inter-régimes de l'assurance maladie sont transmises par les organismes gérant un régime de base d'assurance maladie et, pour ce qui concerne les informations relatives à l'activité hospitalière, par la direction de l'hospitalisation et de l'organisation des soins au ministère de l'emploi et de la solidarité.
Ces informations, détaillées à l'annexe 1 du protocole, concernent :
- l'identification des organismes de prise en charge ;
- les caractéristiques des décomptes de remboursement ;
- les numéros d'anonymat de l'assuré et du bénéficiaire, le sexe, l'année et le mois de naissance, le département et la commune de résidence ;
- les informations relatives aux prestations servies :
- nature détaillée des actes, biens et services présentés au remboursement ;
- dates de soins et de remboursement ;
- mode de prise en charge ;
- informations médico-administratives (notamment le numéro d'affection de longue durée au sens de l'article D. 322-1 du code de la sécurité sociale, le numéro de maladie professionnelle, les codes de pathologie suivant la codification internationale des maladies en vigueur, les dates de grossesse, le numéro de dent) ;
- montant, cotation et coefficient de la prestation ;
- le numéro d'identification du professionnel et, le cas échéant, de l'établissement de rattachement, le sexe, la date de naissance, la spécialité médicale, la nature d'exercice, le statut conventionnel, la caisse de rattachement, département et commune d'établissement ;
- les informations relatives à l'activité des établissements de santé : résumés de sorties anonymes établis dans le cadre du programme de médicalisation des systèmes d'information au sens de l'article L. 6113-7 du code de la santé publique, et les informations de séjour pour les établissements financés par dotation globale ;
- les données comptables.
Les données individuelles concernant les bénéficiaires sont conservées pendant deux ans au-delà de l'année en cours.

Article 4 En savoir plus sur cet article...

Les destinataires des informations contenues dans le système national d'information inter-régimes de l'assurance maladie sont, à raison de leurs fonctions et selon les règles d'habilitation détaillées à l'annexe 2 du protocole :
1° Pour l'ensemble des informations visées à l'article 3 : les médecins-conseils 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 nommément désignés, suivant leur rattachement administratif, par les directeurs ou les agents comptables des caisses et des unions.
Seuls les médecins-conseils et les personnels placés sous leur responsabilité, nommément désignés par les médecins responsables selon l'organisation des régimes, sont autorisés à effectuer des recherches mettant en oeuvre simultanément plus d'une des trois variables sensibles (code commune, date des soins, mois et année de naissance) avec d'autres données ;

2° Pour, sous forme exclusivement de statistiques agrégées, les données relatives aux bénéficiaires de l'assurance maladie et, sous forme individuelle, l'ensemble des données relatives aux professionnels de santé ou aux établissements de santé, à l'exclusion de toute donnée d'identification des professionnels de santé :
- les agents du ministère de l'emploi et de la solidarité ou de ses services déconcentrés nommément désignés par les directeurs d'administration centrale ou des services déconcentrés de ce ministère ;
- les agents des agences régionales de l'hospitalisation nommément désignés par les directeurs de ces agences ;
- les agents habilités et nommément désignés par le directeur des exploitations, de la politique sociale et de l'emploi au ministère chargé de l'agriculture pour les données relatives aux ressortissants des régimes de protection sociale agricole ;
3° Pour, sous forme exclusivement agrégée, les données relatives aux bénéficiaires de l'assurance maladie, aux professionnels de santé ou aux établissements de santé : les agents du ministère de l'économie, des finances et de l'industrie nommément désignés par le directeur du budget ou le directeur de la prévision, d'une part, et, d'autre part, les membres du conseil pour la transparence des statistiques de l'assurance maladie ;
4° Pour les données relatives à leur activité, leurs recettes ou leurs prescriptions : l'ensemble des prestataires de soins ; les professions médicales et les pharmaciens ayant seuls accès aux informations médico-administratives (numéro d'affection de longue durée) au sens de l'article D. 322-1 du code de la sécurité sociale, numéro de maladie professionnelle, codes de pathologie suivant la codification internationale des maladies en vigueur) ;
5° Pour, exclusivement sous forme de statistiques agrégées, les données relatives aux bénéficiaires de l'assurance maladie et, sous forme individuelle, l'ensemble des données relatives aux professionnels de santé de leur région, à l'exclusion de toute donnée d'identification : les unions régionales de médecins libéraux.
Toute autre demande d'accès à des données individuelles relatives aux bénéficiaires devra faire l'objet d'une demande d'autorisation auprès de la CNIL dans les conditions prévues aux articles 40-11 à 40-15 de la loi du 6 janvier 1978 susvisée.

Article 5 En savoir plus sur cet article...

Pour la mise en oeuvre du système, il est créé une base de données nationale dont la gestion technique est confiée à la Caisse nationale de l'assurance maladie des travailleurs salariés.
Afin de garantir l'anonymat des personnes ayant bénéficié des prestations de soins, les données transmises ne comportent pas l'identité de ces personnes. Un numéro d'anonymat est établi par codage informatique irréversible à partir du numéro d'inscription au répertoire national d'identification des personnes physiques.
Ce procédé d'anonymisation s'opère à un double niveau, une première fois avant transmission des informations par les régimes à la base nationale et, une deuxième fois, préalablement à leur enregistrement dans la base de données nationale. Ce même procédé est appliqué aux numéros d'identification des titulaires de pensions d'invalidité et de rentes d'accidents du travail ou de maladies professionnelles ainsi qu'aux numéros d'entrée des patients. Toutes les données sensibles sont chiffrées lors de leur sauvegarde.
Lors des transferts vers la base nationale, les informations sont transmises selon un mode sécurisé recourant à des procédures de chiffrement et d'authentification.
Un annuaire sécurisé, créé et mis à jour par une infrastructure de gestion de clés, des personnes habilitées à accéder au système national d'information inter-régimes de l'assurance maladie, dont la gestion technique est confiée à la Caisse nationale de l'assurance maladie des

travailleurs salariés, est établi pour contrôler toutes les autorisations d'accès.
Des dispositifs de journalisation des interrogations sont mis en oeuvre pour contrôler les accès au système. Des procédures d'exploitation systématique de ces journaux sont élaborées de manière à permettre l'audit des accès au système.

Article 6 En savoir plus sur cet article...

Le droit d'accès et de rectification des données s'exerce pour les professionnels de santé auprès de la caisse dont ils relèvent au titre de leur activité principale.

Article 7 En savoir plus sur cet article...

Conformément aux dispositions du deuxième alinéa de la loi du 6 janvier 1978 susvisée, le droit d'opposition ne s'applique pas au présent traitement.

Article 8 En savoir plus sur cet article...

Le protocole et ses annexes seront publiés au Bulletin officiel Solidarité-Santé du ministère de l'emploi et de la solidarité.

Article 9 En savoir plus sur cet article...

Le directeur de la sécurité sociale, le directeur général de la santé, la directrice générale de l'action sociale, le directeur de l'hospitalisation et de l'organisation de soins, la directrice de la recherche des études de l'évaluation et des statistiques au ministère de l'emploi et de la solidarité, la directrice du budget et le directeur de la prévision au ministère de l'économie, des finances et de l'industrie et le directeur des exploitations, de la politique sociale et de l'emploi au ministère de l'agriculture et de la pêche sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 11 avril 2002.

ANNEXE 2 : Arrêté du 20 juin 2005 relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE LA SANTÉ ET DES SOLIDARITÉS

Arrêté du 20 juin 2005 relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie

NOR : *SANS0522353A*

Le ministre de la santé et des solidarités,

Vu le code de la santé publique, notamment ses articles L. 4113-7, L. 6113-8 et L. 6113-9 ;

Vu le code de la sécurité sociale, notamment ses articles L. 115-2, L. 115-4, L. 161-28, L. 161-28-1 et L. 161-29 ;

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière statistique ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par 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 ;

Vu la loi n° 93-8 du 4 janvier 1993 relative aux relations entre les professions de santé et l'assurance maladie ;

Vu la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie ;

Vu l'arrêté du 11 avril 2002 relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 14 juin 2005,

Arrête :

Art. 1er. – Est aprouvé l'avenant du 16 mai 2005 au protocole du 15 octobre 2001 définissant les modalités de gestion et de renseignement du système national d'information interrégimes de l'assurance maladie (SNIIRAM), signé par la Caisse nationale de l'assurance maladie des travailleurs salariés, la Caisse centrale de mutualité sociale agricole et la Caisse nationale d'assurance maladie et maternité des travailleurs non salariés des professions non agricoles.

Art. 2. – L'article 2 de l'arrêté du 11 avril 2002 susvisé est remplacé par les dispositions suivantes :

« *Art. 2.* – Les traitements mis en œuvre dans le cadre du système national d'information interrégimes de l'assurance maladie ont pour finalités :

« 1° D'améliorer la qualité des soins, notamment par :

« – la comparaison des pratiques aux référentiels, accords de bons usages ou contrats de bonne pratique, au sens des articles L. 162-12-15, L. 162-12-17, L. 162-12-18, et L. 162-12-20 du code de la sécurité sociale, et moyennes professionnels ;

« – l'évaluation des comportements de consommation de soins ;

« – l'analyse des caractéristiques et des déterminants de la qualité des soins ;

« 2° De contribuer à une meilleure gestion de l'assurance maladie, notamment par :

« – la connaissance des dépenses de l'ensemble des régimes d'assurance maladie par circonscription géographique, par nature de dépense, par catégorie de professionnels responsables de ces dépenses et par professionnel ou établissement ;

« – l'évaluation des transferts entre enveloppes correspondant aux objectifs sectoriels de dépenses fixés, en fonction de l'objectif national de dépenses d'assurance maladie, dans le cadre de la loi de financement de la sécurité sociale ;

« – l'analyse quantitative des déterminants de l'offre de soins et la mesure de leurs impacts sur l'évolution des dépenses d'assurance maladie ;

« 3° De contribuer à une meilleure gestion des politiques de santé, notamment par :

« – l'identification des parcours de soins des patients ;

Texte précédent Page suivante Texte suivant

« – le suivi et l'évaluation de l'état de santé des patients et leurs conséquences sur la consommation de soins ;
« – l'analyse de la couverture sociale des patients ;
« – la surveillance de la consommation de soins en fonction de différents indicateurs de santé publique ou de risque ;

« 4° De transmettre aux prestataires de soins les informations pertinentes relatives à leur activité, à leurs recettes et, s'il y a lieu, à leurs prescriptions. »

Art. 3. – L'article 3 de l'arrêté du 11 avril 2002 susvisé est ainsi modifié :

1° Au premier alinéa, les mots : « au ministère de l'emploi et de la solidarité » sont remplacés par les mots : « chargé de la santé et de l'assurance maladie » ;

2° Après le neuvième alinéa, il est inséré un alinéa ainsi rédigé :

« – les informations relatives au parcours de soins » ;

3° Le dernier alinéa est complété par les mots : « , excepté lors de constitution d'échantillons » ;

4° Il est ajouté deux alinéas ainsi rédigés :

« Un échantillon généraliste de ces données 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.

« D'autres échantillons de ces données peuvent être réalisés, conformément aux dispositions du chapitre X de la loi du 6 janvier 1978 susvisée. Ils sont soumis à l'approbation préalable du conseil d'administration de l'Institut des données de santé excepté lorsqu'ils sont réalisés pour le compte d'organismes d'assurance maladie obligatoires ou lorsqu'ils ont déjà fait l'objet d'un avis du Conseil national de l'information statistique. »

Art. 4. – L'article 4 de l'arrêté du 11 avril 2002 susvisé est remplacé par les dispositions suivantes :

« *Art. 4.* – Pour tout traitement de données individuelles relatives aux bénéficiaires de l'assurance maladie, seuls les médecins-conseils et les personnels placés sous leur responsabilité, nommément désignés par les médecins responsables selon l'organisation des régimes, sont 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.

« Les destinataires des informations contenues dans le système national d'information interrégimes de l'assurance maladie sont, à raison de leurs fonctions et selon les règles d'habilitation détaillées à l'annexe 2 du protocole :

« 1° Pour l'ensemble des informations énumérées à l'article 3 : les médecins-conseils et les personnels placés sous leur responsabilité ainsi que les agents administratifs des caisses des différents régimes de base d'assurance maladie ou de la Caisse nationale de solidarité pour l'autonomie et des unions régionales des caisses d'assurance maladie nommément désignés, suivant leur rattachement administratif, par les directeurs ou les agents comptables des caisses et des unions ;

« 2° Pour l'ensemble des informations énumérées à l'article 3, sous forme exclusivement de statistiques agrégées ou, pour l'échantillon généraliste, sous forme individualisée, les données relatives aux bénéficiaires de l'assurance maladie comprenant l'ensemble des données relatives aux professionnels de santé ou aux établissements de santé, à l'exclusion de toute donnée d'identification des professionnels de santé :

« – les agents du ministère chargé de l'assurance maladie, de la santé, de l'action sociale des personnes handicapées et de la dépendance ou de ses services déconcentrés nommément désignés par les directeurs d'administration centrale ou des services déconcentrés de ce ministère ;
« – les agents des agences sanitaires sous tutelle du ministère chargé de l'assurance maladie et de la santé nommément désignés par les directeurs de ces agences, notamment l'Institut de veille sanitaire (InVS) et l'Agence française de sécurité sanitaire des produits de santé (AFSSAPS) ;
« – les agents des agences régionales de l'hospitalisation nommément désignés par les directeurs de ces agences ;
« – les agents habilités et nommément désignés par le directeur général de la forêt et des affaires rurales au ministère chargé de l'agriculture, pour les données relatives aux ressortissants des régimes de protection sociale agricole ;
« – les agents du ministère chargé de l'économie, des finances et de l'industrie nommément désignés par le directeur du budget ou par le directeur de la prévision ;
« – les membres du Haut Conseil pour l'avenir de l'assurance maladie nommément désignés par leur président ;
« – les membres de l'Institut des données de santé nommément désignés par le président de leur conseil d'administration ;
« – les membres de l'Union nationale des professions de santé nommément désignés par leur président ;

« 3° Pour les données relatives à leur activité, leurs recettes ou leurs prescriptions : l'ensemble des prestataires de soins ; les professions médicales et les pharmaciens ayant seuls accès aux informations médico-

Texte précédent Page précédente Page suivante Texte suivant

administratives (numéro d'affection de longue durée au sens de l'article D. 322-1 du code de la sécurité sociale, numéro de maladie professionnelle, codes de pathologie suivant la codification internationale des maladies en vigueur) ;

« 4° Pour l'ensemble des informations énumérées à l'article 3, à l'exclusion de l'échantillon généraliste, les données relatives aux professionnels de santé de leur région, à l'exclusion de toute donnée d'identification :

« – les membres des unions régionales de médecins libéraux nommément désignés par leur président ;

« 5° Pour l'ensemble des informations énumérées à l'article 3, exclusivement sous forme de statistiques agrégées, ou sous forme individualisée sur l'échantillon généraliste, les données relatives aux bénéficiaires de l'assurance maladie comprenant l'ensemble des données relatives aux professionnels de santé ou aux établissements de santé, à l'exclusion de toute donnée d'identification des professionnels de santé :

« – les chercheurs habilités et nommément désignés par le président de l'Institut de recherche et de documentation en économie de la santé ;

« – les agents habilités et nommément désignés par le président du conseil d'administration du centre technique d'appui et de formation des centres d'examens de santé ;

« – les chercheurs des services chargés de l'assurance maladie, de la santé, de l'action sociale, des personnes handicapées ou de la dépendance, habilités et nommément désignés par le président du conseil d'administration de l'Institut national de la santé et de la recherche médicale ;

« – les chercheurs des services chargés de l'assurance maladie, de la santé, de l'action sociale, des personnes handicapées ou de la dépendance habilités et nommément désignés par le président du conseil d'administration du Centre national de la recherche scientifique.

« Le traitement des informations énumérées à l'article 3 demandé par tout autre organisme de recherche, des universités, écoles ou autres structures d'enseignement liés à la recherche que ceux mentionnés au paragraphe précédent est soumis à l'approbation du conseil d'administration de l'Institut des données de santé. Aucun organisme de recherche, université, école ou autre structure d'enseignement lié à la recherche poursuivant un but lucratif ne peut accéder aux informations de l'article 3. La CNIL, conformément aux dispositions du chapitre X de la loi du 6 janvier 1978 susvisée, autorise ces traitements. »

Art. 5. – L'avenant et ses annexes modifiés seront publiés au *Bulletin officiel solidarité-santé* du ministère de la santé et des solidarités.

Art. 6. – Le directeur de la sécurité sociale est chargé de l'exécution du présent arrêté, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 20 juin 2005.

Pour le ministre et par délégation :
Le directeur de la sécurité sociale,
D. LIBAULT

Texte précédent Page précédente Texte suivant

ANNEXE 3 : Arrêté du 19 juillet 2013 relatif à la mise en œuvre du Système national d'information interrégimes de l'assurance maladie

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTÉ

Arrêté du 19 juillet 2013 relatif à la mise en œuvre du Système national d'information interrégimes de l'assurance maladie

NOR : *AFSS1318985A*

La ministre des affaires sociales et de la santé,

Vu le code de la santé publique, notamment ses articles L. 4113-7, L. 6113-8 et L. 6113-9 ;

Vu le code de la sécurité sociale, notamment ses articles L. 115-4, L. 161-28, L. 161-28-1 et L. 161-29 ;

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière statistique ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 93-8 du 4 janvier 1993 relative aux relations entre les professions de santé et l'assurance maladie ;

Vu la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 27 juin 2013,

Arrête :

Art. 1er. – Est approuvé le protocole du 8 juin 2012 et ses annexes définissant les modalités de gestion et de renseignement du Système national d'information interrégimes de l'assurance maladie (SNIIRAM), signé par 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.

Art. 2. – Les traitements mis en œuvre dans le cadre du Système national d'information interrégimes de l'assurance maladie ont pour finalités :

1° D'améliorer la qualité des soins, notamment par :

- la comparaison des pratiques aux référentiels, accords de bons usages ou contrats de bonne pratique, au sens des articles L. 162-12-15, L. 162-12-17, L. 162-12-18, et L. 162-12-20 du code de la sécurité sociale, et moyennes professionnels ;
- l'évaluation des comportements de consommation de soins ;
- l'analyse des caractéristiques et des déterminants de la qualité des soins ;

2° De contribuer à une meilleure gestion de l'assurance maladie, notamment par :

- la connaissance des dépenses de l'ensemble des régimes d'assurance maladie par circonscription géographique, par nature de dépense, par catégorie de professionnels responsables de ces dépenses et par professionnel ou établissement ;
- l'évaluation des transferts entre enveloppes correspondant aux objectifs sectoriels de dépenses fixés, en fonction de l'objectif national de dépenses d'assurance maladie, dans le cadre de la loi de financement de la sécurité sociale ;
- l'analyse quantitative des déterminants de l'offre de soins et la mesure de leurs impacts sur l'évolution des dépenses d'assurance maladie ;

3° De contribuer à une meilleure gestion des politiques de santé, notamment par :

- l'identification des parcours de soins des patients ;
- le suivi et l'évaluation de l'état de santé des patients et leurs conséquences sur la consommation de soins ;
- l'analyse de la couverture sociale des patients ;
- la surveillance de la consommation de soins en fonction de différents indicateurs de santé publique ou de risque ;

4° De transmettre aux prestataires de soins les informations pertinentes relatives à leur activité, à leurs recettes et, s'il y a lieu, à leurs prescriptions.

Art. 3. – Les informations nécessaires à l'établissement du Système national d'information interrégimes de l'assurance maladie (SNIIRAM) sont transmises par les organismes gérant un régime de base d'assurance maladie et, pour ce qui concerne les informations relatives à l'activité hospitalière, par l'Agence technique de l'information sur l'hospitalisation (ATIH).

Ces informations, détaillées à l'annexe 1 du protocole, concernent :

– l'identification des organismes de prise en charge ;
– les caractéristiques des décomptes de remboursement ;
– les numéros d'anonymat de l'assuré et du bénéficiaire, le sexe, l'année et le mois de naissance, le cas échéant, la date de décès, le département et la commune de résidence ;
– les informations relatives aux prestations servies :
– la nature détaillée des actes, biens et services présentés au remboursement ;
– les dates de soins et de remboursement ;
– le mode de prise en charge ;
– les informations relatives au parcours de soins ;
– les informations médico-administratives (notamment le numéro d'affection de longue durée au sens de l'article D. 322-1 du code de la sécurité sociale, le numéro de maladie professionnelle, les codes de pathologie suivant la codification internationale des maladies en vigueur, les dates de grossesse, le numéro de dent) ;
– les montant, cotation et coefficient de la prestation ;
– le numéro d'identification du professionnel et, le cas échéant, de l'établissement de rattachement, le sexe, la date de naissance, la spécialité médicale, la nature d'exercice, le statut conventionnel, la caisse de rattachement, département, commune et localisation infracommunale d'implantation ;
– les informations relatives à l'activité des établissements de santé : résumés de sorties anonymes établis dans le cadre du programme de médicalisation des systèmes d'information au sens de l'article L. 6113-7 du code de la santé publique et les informations de séjour pour les établissements financés par dotation globale. La durée de conservation de ces données est de dix ans au-delà de l'année en cours. Passé ce délai, ces données sont archivées pour une durée de dix ans ;
– les données comptables.

Les données individuelles concernant les bénéficiaires sont conservées pendant trois ans au-delà de l'année en cours, excepté lors de constitution d'échantillons. Passé ce délai, ces données sont archivées pour une durée de dix ans.

Un échantillon généraliste de ces données 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.

D'autres échantillons de ces données peuvent être réalisés, conformément aux dispositions du chapitre X de la loi du 6 janvier 1978 susvisée. Ils sont soumis à l'approbation préalable du bureau de l'Institut des données de santé, excepté lorsqu'ils sont réalisés pour le compte d'organismes d'assurance maladie obligatoires ou lorsqu'ils ont déjà fait l'objet d'un avis du Conseil national de l'information statistique.

Art. 4. – I. – Pour tout traitement de données individuelles relatives aux bénéficiaires de l'assurance maladie, seuls sont autorisés 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) avec d'autres données :

– les médecins-conseils de l'assurance maladie et les personnels habilités placés sous leur responsabilité, nommément désignés par les médecins responsables selon l'organisation des régimes d'assurance maladie ;
– à titre expérimental et pour une durée de trois ans, les médecins de l'Institut de veille sanitaire et les personnels habilités placés sous leur responsabilité, nommément désignés par le directeur de l'Institut de veille sanitaire, autorité médicale de l'institut, dans la mesure où ces variables sont strictement nécessaires à l'accomplissement des missions de surveillance et d'alerte sanitaires.

II. – Dans le cadre de la charte d'engagements pour la mise à disposition et les principes d'utilisation des données issues du SNIIRAM dans les ARS entre les membres de l'UNCAM, le ministère des affaires sociales et de la santé et l'Union nationale des professionnels de santé, pour tout traitement de données individuelles relatives :

– aux bénéficiaires de l'assurance maladie, seuls les médecins membres du personnel des agences régionales de santé (ARS), nommément désignés par les directeurs généraux des ARS, sont autorisés à effectuer des recherches sur le champ de leur compétence régionale ;
– aux professionnels de santé, seuls les médecins membres du personnel des agences régionales de santé (ARS), nommément désignés par les directeurs généraux des ARS, sont autorisés, sur le champ de leur compétence régionale, à effectuer des recherches localisées (code commune et données infracommunales).

III. – Les destinataires des informations contenues dans le Système national d'information interrégimes de l'assurance maladie sont, à raison de leurs fonctions et selon les règles d'habilitation détaillées à l'annexe 2 du protocole :

1° Pour l'ensemble des informations énumérées à l'article 3, les médecins-conseils et les personnels habilités placés sous leur responsabilité ainsi que les agents administratifs habilités des caisses des différents régimes de base d'assurance maladie ou de la Caisse nationale de solidarité pour l'autonomie nommément désignés, suivant leur rattachement administratif, par les directeurs ou les agents comptables des caisses ;

2° Pour l'ensemble des informations énumérées à l'article 3, dans la mesure strictement nécessaire à l'accomplissement des missions de l'organisme et à l'exclusion de toute donnée d'identification des professionnels de santé :

- les agents habilités de l'Institut de veille sanitaire (InVS) nommément désignés par leur directeur, sont autorisés à effectuer des recherches localisées (code commune et données infra-communales) ;
- les agents habilités de la Haute Autorité de santé (HAS) nommément désignés par leur président ;
- les agents habilités de l'Agence nationale de sécurité du médicament et des produits de santé nommément désignés par leur directeur ;
- sur le champ de leur compétence régionale, les médecins des Agences régionales de santé nommément désignés par les directeurs généraux ;
- l'expérimentation d'utilisation de données identifiantes des professionnels de santé encadrée par la charte d'engagements pour la mise à disposition et les principes d'utilisation des données issues du SNIIRAM dans les ARS, doit faire l'objet, conformément aux dispositions du chapitre X de la loi du 6 janvier 1978 susvisée, d'une autorisation de la CNIL ;

3° Pour l'ensemble des informations énumérées à l'article 3, exclusivement sous forme de statistiques agrégées ou sous forme individualisée sur l'échantillon généraliste, les données relatives aux bénéficiaires de l'assurance maladie comprenant l'ensemble des données relatives aux professionnels de santé ou aux établissements de santé, à l'exclusion de toute donnée d'identification des professionnels de santé :

- les agents du ministère chargé de l'assurance maladie, de la santé, de l'action sociale des personnes handicapées et de la dépendance ou de ses services déconcentrés nommément désignés par les directeurs d'administration centrale ou des services déconcentrés de ce ministère ;
- les agents des agences sanitaires sous tutelle du ministère chargé de l'assurance maladie et de la santé nommément désignés par les directeurs de ces agences, notamment l'Agence technique de l'information sur l'hospitalisation (ATIH), l'Agence de biomédecine et les agences régionales de santé (ARS) ;
- les agents habilités et nommément désignés par le directeur général des politiques agricole, agroalimentaire et des territoires au ministère chargé de l'agriculture, pour les données relatives aux ressortissants des régimes de protection sociale agricole ;
- les agents des ministères chargés de l'économie, des finances et du budget, nommément désignés par le directeur général du Trésor ou le directeur du budget ;
- les membres du Haut Conseil pour l'avenir de l'assurance maladie (HCAAM) nommément désignés par leur président ;
- les membres de l'Institut des données de santé (IDS) nommément désignés par leur président ;
- les membres de l'Union nationale des professions de santé (UNPS) nommément désignés par leur président ;
- les chercheurs habilités et nommément désignés par le président de l'Institut de recherche et de documentation en économie de la santé (IRDES) ;
- les agents habilités et nommément désignés par le président du conseil d'administration du centre technique d'appui et de formation des centres d'examens de santé (CETAF) ;
- les chercheurs des services chargés de l'assurance maladie, de la santé, de l'action sociale, des personnes handicapées ou de la dépendance, habilités et nommément désignés par le directeur général de l'Institut national de la santé et de la recherche médicale (INSERM) ;
- les chercheurs des services chargés de l'assurance maladie, de la santé, de l'action sociale, des personnes handicapées ou de la dépendance habilités et nommément désignés par le président du conseil d'administration du Centre national de la recherche scientifique (CNRS) ;
- les agents de l'Institut national du cancer (INCA) nommément désignés par leur directeur ;
- les agents du fonds CMU nommément désignés par leur directeur ;
- les membres de l'Observatoire français des drogues et de la toxicomanie (OFDT) nommément désignés par leur président ;
- les membres de l'UNOCAM signataires de la charte d'engagements entre l'assurance maladie obligatoire et les assureurs maladie complémentaires pour le partage et la mise en commun des données de remboursement agrégées ou individuelles anonymisées issues de leurs systèmes d'information, présentée en annexe 6, nommément désignés par le président de l'Institut des données de santé.

Le traitement des informations énumérées à l'article 3 demandé par tout autre organisme de recherche, des universités, écoles ou autres structures d'enseignement liés à la recherche que ceux mentionnés au paragraphe précédent est soumis à l'approbation du bureau de l'Institut des données de santé. Aucun organisme de

recherche, université, école ou autre structure d'enseignement lié à la recherche poursuivant un but lucratif ne peut accéder aux informations de l'article 3. La CNIL, conformément aux dispositions du chapitre X de la loi du 6 janvier 1978 susvisée, autorise ces traitements.

4° Pour les données relatives à leur activité, leurs recettes ou leurs prescriptions, l'ensemble des prestataires de soins ; les professions médicales et les pharmaciens ayant seuls accès aux informations médico-administratives (numéro d'affection de longue durée au sens de l'article D. 322-1 du code de la sécurité sociale, numéro de maladie professionnelle, codes de pathologie suivant la codification internationale des maladies en vigueur) ;

5° Pour l'ensemble des informations énumérées à l'article 3, à l'exclusion de l'échantillon généraliste, sous forme de statistiques agrégées, les données relatives aux bénéficiaires de l'assurance maladie comprenant l'ensemble des données relatives aux professionnels de santé de leur région, à l'exclusion de toute donnée d'identification :

– les membres des unions régionales des professionnels de santé (URPS) nommément désignés par leur président ;

6° Pour l'ensemble des informations énumérées à l'article 3, à l'exclusion de l'échantillon généraliste, sous forme de statistiques agrégées, les données relatives aux bénéficiaires de l'assurance maladie comprenant l'ensemble des données relatives aux professionnels de santé ou aux établissements de santé à l'exclusion de toute donnée d'identification des professionnels de santé :

– les structures adhérant aux membres de l'Institut des données de santé ou les constituant, à l'exclusion des membres de l'UNOCAM, nommément désignées par le président de l'IDS.

7° Pour l'ensemble des informations énumérées à l'article 3, à l'exclusion de l'échantillon généraliste, sous forme de statistiques agrégées, les données relatives aux bénéficiaires de l'assurance maladie comprenant l'ensemble des données relatives aux professionnels de santé ou aux établissements de santé à l'exclusion de toute donnée d'identification :

– les 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 pour le partage et la mise en commun des données de remboursement agrégées ou individuelles anonymisées issues de leurs systèmes d'information, présentée en annexe 6.

Art. 5. – Pour la mise en œuvre du système, il est créé une base de données nationale dont la gestion technique est confiée à la Caisse nationale de l'assurance maladie des travailleurs salariés.

Afin de garantir l'anonymat des personnes ayant bénéficié des prestations de soins, les données transmises ne comportent pas l'identité de ces personnes. Un numéro d'anonymat est établi par codage informatique irréversible à partir du numéro d'inscription au répertoire national d'identification des personnes physiques.

Ce procédé d'anonymisation s'opère à un double niveau, une première fois avant transmission des informations par les régimes à la base nationale et, une deuxième fois, préalablement à leur enregistrement dans la base de données nationale. Ce même procédé est appliqué aux numéros d'identification des titulaires de pensions d'invalidité et de rentes d'accidents du travail ou de maladies professionnelles ainsi qu'aux numéros d'entrée des patients. Toutes les données sensibles sont chiffrées lors de leur sauvegarde.

Lors des transferts vers la base nationale, les informations sont transmises selon un mode sécurisé recourant à des procédures de chiffrement et d'authentification.

Un annuaire sécurisé, créé et mis à jour par une infrastructure de gestion de clés, des personnes habilitées à accéder au Système national d'information interrégimes de l'assurance maladie, dont la gestion technique est confiée à la Caisse nationale de l'assurance maladie des travailleurs salariés, est établi pour contrôler toutes les autorisations d'accès.

Des dispositifs de journalisation des interrogations sont mis en œuvre pour contrôler les accès au système. Des procédures d'exploitation systématique de ces journaux sont élaborées et mises en œuvre de manière à permettre l'audit des accès au système.

Art. 6. – Le droit d'accès et de rectification des données à caractère personnel prévu par les articles 39 et 40 s'exerce, pour les professionnels de santé, auprès de la caisse dont ils relèvent au titre de leur activité principale.

Art. 7. – Conformément aux dispositions du dernier alinéa de l'article 38 de la loi du 6 janvier 1978 susvisée, le droit d'opposition ne s'applique pas au présent traitement.

Art. 8. – Le protocole et ses annexes seront publiés au *Bulletin officiel* solidarité-santé du ministère des affaires sociales et de la santé.

Art. 9. – L'arrêté du 11 juillet 2012 relatif à la mise en œuvre du Système national d'information interrégimes de l'assurance maladie est abrogé.

Art. 10. – Le directeur de la sécurité sociale est chargé de l'exécution du présent arrêté, qui sera publié au *Journal officiel* de la République française.

Fait le 19 juillet 2013.

Pour la ministre et par délégation :
Le directeur de la sécurité sociale,
T. FATOME

ANNEXE 4 : Décret n° 2016-1871 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTÉ

Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »

NOR : *AFSE1625287D*

Publics concernés : *personnes dont les données sont susceptibles d'être utilisées à des fins de recherches, études, évaluations dans le domaine de la santé et utilisateurs autorisés à traiter ces données.*

Objet : *modalités de mise en œuvre du système national des données de santé.*

Entrée en vigueur : *le texte entre en vigueur à compter du 1er avril 2017.*

Notice : *le décret décrit les modalités de gouvernance et de fonctionnement du système national des données de santé (SNDS) qui a vocation à regrouper les données de santé de l'assurance maladie obligatoire, des établissements de santé, les causes médicales de décès, les données issues des Maisons départementales des personnes handicapées ainsi qu'un échantillon de données de remboursement d'assurance maladie complémentaire. Le présent décret fixe en outre la liste des organismes, établissements et services bénéficiant d'accès permanents aux données du SNDS en raison de leurs missions de service public ainsi que les modalités de ces accès. Ce texte prévoit également des possibilités d'accès ponctuel aux données du SNDS. Enfin, il prévoit l'information des personnes auxquelles les données se rapportent, et leurs droits d'accès, de rectification et d'opposition qui s'exercent auprès de la caisse d'assurance maladie dont dépend la personne.*

Références : *les dispositions du décret sont prises en application de l'article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé. Les dispositions du code de la santé publique modifiées par le présent décret peuvent être consultées sur le site Légifrance (http://www.legifrance.gouv.fr).*

Le Premier ministre,

Sur le rapport de la ministre des affaires sociales et de la santé,

Vu le code de l'action sociale et des familles, notamment son articles L. 247-2 ;

Vu le code général des collectivités territoriales, notamment son article L. 2223-42 ;

Vu le code de la santé publique, notamment ses articles L. 1461-3, L. 1461-4 et L. 1461-7 ;

Vu le code de la sécurité sociale, notamment son article L. 161-28-1 ;

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière statistique ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, et notamment son article 193 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu l'avis du conseil de la Caisse nationale de l'assurance maladie des travailleurs salariés en date du 20 septembre 2016 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 13 octobre 2016 ;

Le Conseil d'Etat (section sociale) entendu,

Décrète :

Art. 1er. – Le livre IV de la première partie du code de la santé publique est complété par un titre VI ainsi rédigé :

« TITRE VI

« MISE À DISPOSITION DES DONNÉES DE SANTÉ

« CHAPITRE Ier

« Système national des données de santé

« Section 1

« Organisation du système national des données de santé

« *Art. R. 1461-1.* – Le traitement de données à caractère personnel dénommé système national des données de santé (SNDS), institué à l'article L. 1461-1, est mis en œuvre par la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS) dans les conditions fixées par le présent chapitre.

« Il a pour finalité, en application des dispositions de l'article L. 1461-1, de mettre à disposition des données qu'il rassemble dans les conditions définies aux articles L. 1461-2 à L. 1461-6 afin de contribuer :

« 1° A l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité, l'orientation des usagers dans le système de santé, en permettant la comparaison des pratiques de soins, des équipements et des tarifs des établissements et des professionnels de santé ;

« 2° A la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale, en favorisant l'identification des parcours de soins des patients, le suivi et l'évaluation de leur état de santé et de leur consommation de soins et de services d'accompagnement social, l'analyse de la couverture sociale des patients, la surveillance de la consommation de soins en fonction d'indicateurs de santé publique ou de risques sanitaires ;

« 3° A la connaissance des dépenses de santé, des dépenses de l'assurance maladie et des dépenses médico-sociales, en permettant d'analyser les dépenses des régimes d'assurance maladie par circonscription géographique, par nature de dépense, par catégorie de professionnels ou de prescripteurs et par professionnel ou établissement, les dépenses d'assurance maladie au regard des objectifs sectoriels de dépenses fixés, dans le cadre de l'objectif national de dépenses d'assurance maladie, par les lois de financement de la sécurité sociale, l'analyse quantitative des déterminants de l'offre de soins et la mesure de leurs impacts sur l'évolution des dépenses d'assurance maladie ;

« 4° A l'information des professionnels de santé, des structures et des établissements de santé ou médico-sociaux sur leur activité, en permettant la transmission aux prestataires de soins des informations pertinentes relatives à leur activité, à leurs recettes et, s'il y a lieu, à leurs prescriptions et la mise à la disposition de leurs représentants de données ne faisant pas apparaître l'identité des professionnels de santé ;

« 5° A la surveillance, à la veille et à la sécurité sanitaires, en développant l'observation de l'état de santé des populations, l'évaluation et la production d'indicateurs relatifs à l'état de santé de la population et l'analyse de leur variation dans le temps et dans l'espace, la détection d'événements de santé inhabituels pouvant représenter une menace pour la santé publique et l'évaluation de leurs liens éventuels avec des facteurs d'exposition et l'évaluation d'actions de santé publique ;

« 6° A la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale.

« *Art. R. 1461-2.* – Pour garantir le respect des dispositions du I de l'article L. 1461-4, les données à caractère personnel, présentes dans le système national des données de santé, sont rattachées à chaque personne concernée par un pseudonyme. Ce pseudonyme est produit selon les modalités mentionnées au 1° de l'article R. 1461-7.

« Le rattachement des données d'une même personne provenant de sources différentes est réalisé, selon des modalités fixées par le directeur général de la Caisse nationale de l'assurance maladie des travailleurs salariés, en concertation avec les organismes gérant les bases de données formant les composantes du système national des données de santé.

« *Art. R. 1461-3.* – I. – La Caisse nationale de l'assurance maladie des travailleurs salariés met les données qu'elle rassemble, dans le cadre du système national des données de santé, à disposition des responsables des traitements prévus aux 1° et 2° du I de l'article L. 1461-3.

« L'Institut national de la santé et de la recherche médicale peut, en tant que coordinateur national d'infrastructures de recherche utilisant des données de santé, être chargé, dans le cadre d'une convention conclue avec la Caisse nationale de l'assurance maladie des travailleurs salariés, d'assurer la réalisation des extractions et la mise à disposition effective de données du système national des données de santé, pour des traitements mis en œuvre à des fins de recherche, d'étude ou d'évaluation. La convention précise le service de l'Institut chargé d'assurer ces opérations, les conditions de suivi des demandes de mise à disposition de données, des extractions de données réalisées, des personnels habilités à réaliser des extractions ainsi que les mesures de sécurité mises en œuvre.

« II. – Sans préjudice des dispositions du I, les organismes gérant les composantes du système national des données de santé mentionnées aux 1° à 5° de l'article L. 1461-1 mettent à disposition, dans les conditions prévues aux articles L. 1461-1 à L. 1461-6, les données issues des systèmes d'information dont ils assurent la gestion.

« *Art. R. 1461-4.* – I. – Les catégories de données réunies au sein du système national des données de santé sont les suivantes :

« 1° Les informations relatives aux bénéficiaires de soins et de prestations médico-sociales :

« *a)* Le pseudonyme, constitué d'un code non signifiant obtenu par un procédé cryptographique irréversible du numéro d'inscription au Répertoire national d'identification des personnes physiques ;

« *b)* Le sexe, le mois et l'année de naissance, le rang de naissance et le lieu de résidence, à l'exclusion de toute adresse ;

« *c)* Les informations médico-administratives, notamment, s'il y a lieu, celles liées aux affections de longue durée figurant sur la liste mentionnée à l'article D. 160-4 du code de la sécurité sociale, et aux maladies professionnelles ;

« *d)* Le cas échéant, les informations relatives au décès :

« *i)* La date du décès ;

« *ii)* La commune et le lieu du décès ;

« *iii)* Les causes et les circonstances du décès ;

« *iv)* La situation familiale et la profession à la date du décès ;

« 2° Les informations relatives aux organismes d'assurance maladie obligatoire et, s'il y a lieu, aux organismes d'assurance maladie complémentaire intervenant dans la prise en charge financière du bénéficiaire des soins et prestations :

« *a)* L'identification des organismes ;

« *b)* Les caractéristiques de la prise en charge par l'assurance maladie obligatoire et, le cas échéant, les organismes d'assurance maladie complémentaire ;

« 3° Les informations relatives à la prise en charge sanitaire, médico-sociale et financière associées à chaque bénéficiaire :

« *a)* Les informations relatives aux prestations servies pour des soins de ville : nature des actes, biens et services, codes des actes médicaux, des dispositifs médicaux, des actes de pharmacie, biologie et de transport sanitaire, date des soins, date de grossesse ;

« *b)* Les informations relatives aux prestations et séjours réalisés en établissement de santé ou en établissement et service médico-social, y compris les soins externes et l'accueil aux urgences, ainsi que les diagnostics médicaux associés à la description de la prise en charge ;

« *c)* Le montant de l'acte ou de la prestation, sa cotation ou coefficient, le tarif appliqué et la part prise en charge par l'assurance maladie obligatoire, le cas échéant la modulation ou l'exonération du ticket modérateur et son motif, ainsi que la date de remboursement ou de paiement ;

« *d)* Les données comptables relatives aux prestations prises en charge par l'assurance maladie obligatoire ;

« *e)* Le type de contrat, la nature des risques couverts et les informations relatives à la couverture assurée par l'assurance maladie complémentaire s'il y a lieu ;

« 4° Les informations relatives aux professionnels et services de santé intervenant dans la prise en charge des bénéficiaires mentionnés au I :

« *a)* Le numéro d'identification du professionnel et, le cas échéant, de l'établissement de rattachement ;

« *b)* Le sexe, la date de naissance ;

« *c)* La profession et, s'il y a lieu, la spécialité, le mode d'exercice, le statut conventionnel, la caisse de rattachement ;

« *d)* Le lieu de réalisation de l'acte par le professionnel de santé ;

« 5° Les informations médico-sociales relatives à la situation des personnes en situation de handicap transmises à la Caisse nationale de solidarité pour l'autonomie dans le cadre du système d'information mentionné à l'article L. 247-2 du code de l'action sociale et des familles :

« *a)* Les données relatives au handicap et à la prise en charge des personnes concernées ;

« *b)* Les données concernant les décisions mentionnées à l'article L. 241-6 du code de l'action sociale et des familles ;

« *c)* Les données relatives aux suites réservées aux orientations prononcées par la commission des droits pour l'autonomie des personnes handicapées, notamment auprès des établissements et services susceptibles d'accueillir ou d'accompagner les personnes concernées ;

« 6° Les informations relatives aux arrêts de travail et aux prestations en espèces : les données relatives aux arrêts de travail, au versement d'indemnités journalières pour les risques maladie, maternité, paternité, accidents du travail et maladies professionnelles et au versement de pensions d'invalidité, de rentes consécutives à un accident du travail ou à une maladie professionnelle ou de capitaux décès.

« Les numéros d'identification des professionnels de santé mentionnés au *a* du 4° sont conservés et gérés par la Caisse nationale de l'assurance maladie des travailleurs salariés, au sein du système national des données de santé, dans des tables distinctes de celles dans lesquelles figurent les autres données du système national des données de santé, conformément aux dispositions du I de l'article L. 1461-4.

« Le système national des données de santé ne comporte aucune autre donnée que celles de ses composantes énumérées à l'article L. 1461-1. La liste précise de ces données et les caractéristiques des échantillons constitués en application de l'article R. 1461-5 sont publiées par le directeur général de la Caisse nationale de l'assurance maladie des travailleurs salariés sur le site du système national des données de santé (www.snds.gouv.fr). Son actualisation fait l'objet d'une information de la Commission nationale de l'informatique et des libertés.

« II. – Les données individuelles mentionnées aux 1° à 6° du I portent sur la totalité des bénéficiaires de l'assurance maladie. Elles sont conservées pendant une durée de dix-neuf ans en plus de l'année au cours de laquelle elles ont été recueillies. Passé ce délai, ces données sont archivées de façon à rester utilisables pour une durée de dix ans.

« *Art. R. 1461-5.* – Sont constitués à partir du système national des données de santé :

« 1° Des jeux de données anonymes mis à disposition du public dans les conditions prévues au premier alinéa de l'article L. 1461-2 ;

« 2° Des jeux de données agrégées et semi-agrégées adaptés à différents types de recherches, d'études ou d'évaluation. Les données semi-agrégées sont individualisées pour les professionnels ou les établissements de santé et agrégées pour les bénéficiaires des soins ;

« 3° Des échantillons généralistes représentatifs de l'ensemble des bénéficiaires de l'assurance maladie, comprenant tout ou partie des données relatives aux personnes les constituant.

« *Art. R. 1461-6.* – Afin de mettre à disposition les données du système national des données de santé en application de l'article R. 1461-3, sont habilités à accéder aux données du système national des données de santé, nécessaires à l'exercice de leurs missions :

« 1° Les personnels ou les prestataires de la Caisse nationale de l'assurance maladie des travailleurs salariés agissant en tant que responsable du traitement, habilités et nommément désignés par son directeur général en raison de leurs missions ;

« 2° Les personnels ou les prestataires de l'Institut national de la santé et de la recherche médicale dont les missions le justifient, habilités et nommément désignés par son président-directeur général agissant en application de la convention mentionnée à l'article R. 1461-3.

« *Art. R. 1461-7.* – Les règles de la gestion sécurisée du système national des données de santé, définies dans un référentiel de sécurité arrêté par les ministres chargés de la santé, de la sécurité sociale et du numérique après avis de la Commission nationale de l'informatique et des libertés sont établies dans le respect des principes suivants :

« 1° Pseudonymisation :

« *a)* Le système national des données de santé ne comporte aucune donnée directement identifiante : ni le nom ni le prénom ni l'adresse ni le numéro d'inscription au Répertoire national d'identification des personnes physiques des personnes. Un pseudonyme, constitué d'un code non signifiant obtenu par un procédé cryptographique irréversible du numéro d'inscription au Répertoire national d'identification des personnes physiques tel que prévu au 1° du I de l'article R. 1461-4, est associé aux données se rapportant à chaque personne ;

« *b)* Le procédé cryptographique irréversible mentionné ci-dessus est utilisé pour alimenter le système national des données de santé et pour apparier les données extraites du système national des données de santé et des données relatives à des bénéficiaires de l'assurance maladie figurant dans d'autres systèmes. Cette procédure est organisée de sorte que nul ne puisse disposer à la fois de l'identité des personnes, notamment de leur numéro d'inscription au Répertoire national d'identification des personnes physiques, d'une part, et du pseudonyme mentionné au III de l'article R. 1461-1, d'autre part. Les personnes intervenant dans cette procédure sont tenues au secret professionnel ;

« 2° Traçabilité :

« Les modalités de conservation et d'utilisation des données permettent d'en contrôler les usages et de fournir des preuves en cas d'usage non autorisé.

« *Art. R. 1461-8.* – Les personnes autorisées à accéder aux données du système national des données de santé dans le cadre d'une autorisation délivrée par la Commission nationale de l'informatique et des libertés en application des dispositions du II de l'article L. 1461-3 et du chapitre IX de la loi n° 78-17 du 6 janvier 1978 sont nommément désignées et habilitées conformément aux dispositions de l'article 34 et, le cas échéant, de l'article 35, de ladite loi.

« *Art. R. 1461-9.* – I. – Les modalités d'information des personnes auxquelles les données se rapportent sont fixées aux articles 32 et 57 de la loi n° 78-17 du 6 janvier 1978 et aux articles 35 et 36 du décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

« II. – Les droits d'accès, de rectification et d'opposition s'exercent, dans les conditions définies aux articles 92 à 95 du décret n° 2005-1309 du 20 octobre 2005 modifié, auprès du directeur de l'organisme gestionnaire du régime d'assurance maladie obligatoire auquel la personne est rattachée.

« III. – Le droit d'opposition prévu aux premier et troisième alinéas de l'article 56 de la loi n° 78-17 du 6 janvier 1978 précitée porte sur l'utilisation des données dans les traitements mentionnés au 1° du I de

l'article L. 1461-3 du code de la santé publique. Il ne s'applique pas aux traitements prévus au 2° du I du même article.

« *Art. R. 1461-10.* – I. – Les ministres chargés des affaires sociales et de la santé fixent les orientations de développement du système national des données de santé. Ils réunissent, à cet effet, un comité stratégique comprenant des représentants des organismes responsables des bases de données alimentant le système national des données de santé, le président de l'Institut national des données de santé et une personnalité qualifiée.

« II. – Pour la mise en œuvre du système national des données de santé, la Caisse nationale de l'assurance maladie des travailleurs salariés réunit un comité de pilotage opérationnel afin de planifier et de coordonner les actions engagées. Ce comité est composé de représentants de la direction de la recherche, des études, de l'évaluation et des statistiques, de l'Agence technique de l'information sur l'hospitalisation, de l'Institut national de la santé et de la recherche médicale, de la Caisse nationale de solidarité pour l'autonomie et des organismes d'assurance maladie complémentaires contribuant à l'alimentation du système national des données de santé.

« III. – Un arrêté des ministres chargés des affaires sociales, de la santé et de la recherche fixe la composition, les missions et les modalités de fonctionnement des comités mentionnés aux I et II.

« Section 2

« Accès permanent de certains services publics au système national des données de santé

« *Art. R. 1461-11.* – I. – Les services de l'Etat, les établissements publics et les organismes chargés d'une mission de service public, mentionnés à l'article R. 1461-12, sont autorisés à traiter des données à caractère personnel du système national des données de santé, dans des limites définies aux articles R. 1461-13 et R. 1461-14, en fonction des exigences des missions de service public qu'ils remplissent.

« L'étendue de cette autorisation est définie :

« 1° Par la profondeur historique des données utilisées, l'aire géographique ou les caractéristiques d'une population déterminée au regard des finalités sanitaires ou sociales du traitement ;

« 2° Par la possibilité ou non d'utiliser de manière simultanée dans un même traitement, en sus des autres informations relatives aux soins et à la prise en charge, plusieurs variables, dénommées identifiants potentiels, dont la combinaison accroît le risque de réidentification. Ces identifiants potentiels sont la période de naissance exprimée en mois et année, le code de la commune de résidence et les données infracommunales de localisation, la date des soins, la date du décès et le code de la commune de décès.

« Pour chaque traitement effectué sur le fondement des dispositions du III de l'article L. 1461-3, seules les données nécessaires à ce traitement qui entrent dans le champ de l'autorisation dont dispose, en application des articles R. 1461-13 et R. 1461-14, le service, l'établissement ou l'organisme qui le met en œuvre, peuvent être utilisées.

« II. – Pour les traitements de données autorisés sur le fondement des dispositions du III de l'article L. 1461-3, seuls les organismes de l'assurance maladie obligatoire et les agences régionales de santé peuvent disposer sur leur champ de compétence territoriale, en tant que de besoin, du numéro d'identification du professionnel de santé. Les autres organismes peuvent avoir accès à un pseudonyme construit à partir de ce numéro.

« *Art. R. 1461-12.* – Les services de l'Etat, les établissements publics et les organismes chargés d'une mission de service public autorisés à traiter des données à caractère personnel du système national des données de santé en application du III de l'article L. 1461-3 sont les suivants :

« 1° La direction de la recherche, des études, de l'évaluation et des statistiques, la direction générale de la santé et la direction générale de l'offre de soins, la direction de la sécurité sociale, la direction du budget et le service de santé des armées ;

« 2° Les agences régionales de santé ;

« 3° Les caisses nationales des régimes de l'assurance maladie obligatoire, les organismes locaux et régionaux de l'assurance maladie obligatoire ;

« 4° La Caisse nationale de solidarité pour l'autonomie ;

« 5° La Haute Autorité de santé ;

« 6° L'Autorité de sûreté nucléaire ;

« 7° L'Agence nationale de santé publique ;

« 8° L'Agence nationale de sécurité du médicament et des produits de santé ;

« 9° L'Agence de biomédecine ;

« 10° L'Institut de radioprotection et de sûreté nucléaire ;

« 11° L'Institut national du cancer ;

« 12° L'Etablissement français du sang ;

« 13° L'Agence technique de l'information sur l'hospitalisation ;

« 14° L'Agence nationale d'appui à la performance des établissements de santé et médico-sociaux ;

« 15° L'Institut national des données de santé ;

« 16° L'Institut de recherche et documentation en économie de la santé ;

« 17° L'Institut national d'études démographiques ;

« 18° L'Observatoire français des drogues et toxicomanies ;

« 19° Le Haut Conseil pour l'avenir de l'assurance maladie ;

« 20° Le Fonds de financement de la couverture maladie universelle ;

« 21° Les observatoires régionaux de la santé ;

« 22° Les unions régionales de professionnels de santé ;

« 23° Les équipes de recherche de l'Institut national de la santé et de la recherche médicale ;

« 24° Les équipes de recherche des centres hospitaliers universitaires et des centres de lutte contre le cancer ;

« 25° Les équipes de recherche et de formation de l'Ecole des hautes études en santé publique.

« *Art. R. 1461-13.* – Les traitements mentionnés à l'article R. 1461-11 portent sur des données du système national des données de santé dont la profondeur historique maximale est de :

« 1° 19 ans, en plus de l'année en cours, pour l'Agence nationale de santé publique, l'Agence nationale de sécurité du médicament et des produits de santé, l'Agence de la biomédecine, l'Institut national du cancer, l'Etablissement français du sang et la Haute Autorité de santé ;

« 2° 9 ans, en plus de l'année en cours, pour la direction de la recherche, des études, de l'évaluation et des statistiques du ministère chargé de la santé et des affaires sociales, l'Institut de recherche et documentation en économie de la santé, les agences régionales de santé, la Caisse nationale de l'assurance maladie des travailleurs salariés, la Caisse nationale de solidarité pour l'autonomie et l'Agence technique de l'information sur l'hospitalisation ;

« 3° 5 ans, en plus de l'année en cours, pour les autres services de l'Etat, établissements ou organismes autorisés à traiter des données à caractère personnel du système national des données de santé en application des dispositions du III de l'article L. 1461-3.

« Par dérogation aux quatre alinéas précédents, lorsque le traitement porte sur un échantillon généraliste mentionné au 3° de l'article R. 1461-5, la profondeur historique des données traitées est de 19 ans plus l'année en cours.

« *Art. R. 1461-14.* – Les traitements mentionnés à l'article R. 1461-11 portent sur des catégories de données du système national des données de santé qui ne peuvent excéder les limites suivantes :

« 1° L'ensemble des données individuelles du système national des données de santé avec croisement des identifiants potentiels, les échantillons généralistes avec croisement des identifiants potentiels, les données semi-agrégées, individualisées pour les professionnels ou établissements de santé et agrégées pour les bénéficiaires, et les données agrégées présentant un risque résiduel de réidentification, pour la direction de la recherche, des études, de l'évaluation et des statistiques, la direction générale de la santé et la direction générale de l'offre de soins, les caisses nationales des régimes de l'assurance maladie obligatoire, la Caisse nationale de solidarité pour l'autonomie, la Haute Autorité de santé, l'Agence nationale de santé publique, l'Agence nationale de sécurité du médicament et des produits de santé, l'Agence de biomédecine, l'Institut national du cancer, l'Etablissement français du sang, l'Agence technique de l'information sur l'hospitalisation, l'Institut national des données de santé, l'Institut de recherche et documentation en économie de la santé et l'Institut national d'études démographiques ;

« 2° L'ensemble des données individuelles du système national des données de santé avec croisement des identifiants potentiels sur leur champ de compétence territoriale, le cas échéant, interrégionale, en ce qui concerne le lieu de résidence du bénéficiaire ou le lieu de réalisation de l'acte par le professionnel de santé, l'ensemble des données issues des systèmes d'informations mentionnés à l'article L. 6113-7 avec croisement des identifiants potentiels, les échantillons généralistes avec croisement des identifiants potentiels, les données semi-agrégées, individualisées pour les professionnels ou établissements de santé et agrégées pour les bénéficiaires ainsi que les données agrégées présentant un risque résiduel de réidentification, pour les agences régionales de santé, les organismes locaux et régionaux de l'assurance maladie obligatoire et les observatoires régionaux de santé ;

« 3° L'ensemble des données individuelles du système national des données de santé avec croisement des identifiants potentiels sur le champ des personnes affiliées à la Caisse nationale militaire de sécurité sociale, les échantillons généralistes avec croisement des identifiants potentiels, les données semi-agrégées, individualisées pour les professionnels ou établissements de santé et agrégées pour les bénéficiaires, et les données agrégées présentant un risque résiduel de réidentification, pour le service de santé des armées ;

« 4° Les échantillons généralistes avec croisement des identifiants potentiels, les données semi-agrégées, individualisées pour les professionnels ou établissements de santé et agrégées pour les bénéficiaires, et les données agrégées présentant un risque résiduel de réidentification, pour les équipes de recherche de l'Institut national de la santé et de la recherche médicale, des centres hospitaliers universitaires et des centres de lutte contre le cancer ainsi que pour les équipes de recherche et de formation de l'Ecole des hautes études en santé publique ;

« 5° Les échantillons généralistes avec au maximum l'utilisation de deux identifiants potentiels, les données semi-agrégées, individualisées pour les professionnels ou établissements de santé et agrégées pour les bénéficiaires, et les données agrégées présentant un risque résiduel de réidentification, pour la direction de la sécurité sociale, la direction du budget, l'Autorité de sûreté nucléaire, l'Institut de radioprotection et de sûreté nucléaire, le Haut Conseil pour l'avenir de l'assurance maladie, le Fonds de financement de la couverture maladie universelle, l'Observatoire français des drogues et toxicomanies et l'Agence nationale d'appui à la performance des établissements de santé et médico-sociaux ;

« 6° Les données semi-agrégées, individualisées pour les professionnels ou établissements de santé et agrégées pour les bénéficiaires, et les données agrégées présentant un risque résiduel de réidentification, pour les unions régionales de professionnels de santé.

« *Art. R. 1461-15.* – Lorsque les besoins d'un traitement particulier ou d'une catégorie de traitements de données du système national des données de santé excèdent l'étendue de l'autorisation dont bénéficie, sur le fondement des dispositions du III de l'article L. 1461-3, le service de l'Etat, l'établissement ou l'organisme qui entend le mettre en œuvre, ce dernier soumet à la Commission nationale de l'informatique et des libertés une demande d'autorisation dans les conditions mentionnées au II de l'article L. 1461-3.

« *Art. R. 1461-16.* – Les responsables des services de l'Etat, des établissements ou des organismes mentionnés à l'article R. 1461-12 habilitent, sous leur responsabilité, au sein de la structure qu'ils dirigent ou, le cas échéant, dans le cadre d'un contrat de sous-traitance et dans le respect des dispositions de l'article 35 de la loi n° 78-17 du 6 janvier 1978, des personnes nommément désignées pour accéder aux données du système national des données de santé.

« Le nombre des personnes habilitées est limité à ce qui est strictement nécessaire pour assurer l'exécution des traitements de données autorisés. Ces personnes doivent avoir été spécialement formées, dans le cadre de leurs fonctions, pour l'accomplissement de leurs missions.

« *Art. R. 1461-17.* – Chacun des services de l'Etat, des établissements publics ou des organismes chargés d'une mission de service public mentionnés à l'article R. 1461-12 désigne un correspondant informatique et liberté qui tient à jour la liste et les caractéristiques des traitements portant sur des données individuelles du système national des données de santé et mis en œuvre dans le cadre de l'autorisation de traiter ces données dont il bénéficie sur le fondement des dispositions du III de l'article L. 1461-3.

« Cette liste et les caractéristiques des traitements, présentées conformément à un modèle établi par arrêté des ministres chargés de la santé et de la sécurité sociale et consultable sur le site du système national des données de santé, sont transmises annuellement au comité stratégique mentionné à l'article R. 1461-10 et à la Commission nationale de l'informatique et des libertés.

« *Art. R. 1461-18.* – Chacun des services de l'Etat, des établissements publics ou des organismes chargés d'une mission de service public mentionnés à l'article R. 1461-12 tient à jour des documents indiquant la ou les personnes compétentes en son sein pour délivrer l'habilitation à accéder aux données du système national des données de santé, la liste des personnes habilitées à accéder à ces données, leurs profils d'accès respectifs et les modalités d'attribution, de gestion et de contrôle des habilitations, conformément à un modèle établi par arrêté des ministres chargés de la santé et de la sécurité sociale et consultable sur le site du système national des données de santé.

« Ces documents sont communiqués à la Commission nationale de l'informatique et des libertés, sur sa demande.

« *Art. R. 1461-19.* – Un comité des services, des établissements et organismes bénéficiant d'une autorisation de traiter des données du système national des données de santé sur le fondement des dispositions du III de l'article L. 1461-3 est animé par l'Agence nationale de santé publique. Il est consulté régulièrement par le comité stratégique mentionné à l'article R. 1461-10. »

Art. 2. – I. – Le présent décret entre en vigueur le 1er avril 2017.

II. – Dans un délai maximal de trois ans à compter de la date mentionnée au I, chaque service, établissement ou organisme mentionné à l'article R. 1461-12 établit un rapport d'évaluation de l'étendue de l'autorisation au regard de ses missions à l'aide, notamment, de la liste mentionnée à l'article R. 1461-17. Ce rapport est communiqué à la Commission nationale de l'informatique et des libertés.

III. – Dans l'attente de l'installation de l'Institut national des données de santé, le comité stratégique mentionné à l'article R. 1461-10 comprend, outre des représentants des organismes responsables des bases de données alimentant le système national des données de santé et une personnalité qualifiée, le président de l'Institut des données de santé.

Art. 3. – La ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche, le ministre de l'économie et des finances et la ministre des affaires sociales et de la santé sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait le 26 décembre 2016.

BERNARD CAZENEUVE

Par le Premier ministre :

La ministre des affaires sociales et de la santé,
MARISOL TOURAINE

La ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche,
NAJAT VALLAUD-BELKACEM

Le ministre de l'économie et des finances,
MICHEL SAPIN

ANNEXE 5 : Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, recueil Lebon, Celtipharm

Conseil d'État N° 385305
ECLI:FR:CECHR:2016:385305.20160520
Mentionné dans les tables du recueil Lebon
1ère - 6ème chambres réunies
M. Frédéric Puigserver, rapporteur
M. Jean Lessi, rapporteur public
SCP ODENT, POULET, avocats

lecture du vendredi 20 mai 2016

REPUBLIQUE FRANCAISE
AU NOM DU PEUPLE FRANCAIS

Texte intégral

Vu la procédure suivante :

Par une requête sommaire, deux mémoires complémentaires et un mémoire en réplique, enregistrés les 23 octobre 2014, 29 décembre 2014, 10 décembre 2015 et 9 mars 2016 au secrétariat du contentieux du Conseil d'Etat, la société Celtipharm demande au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir la décision implicite de rejet résultant du silence gardé par le ministre des affaires sociales, de la santé et des droits des femmes sur sa demande du 19 juillet 2014 tendant à l'abrogation de l'arrêté du 19 juillet 2013 relatif à la mise en oeuvre du Système national d'information interrégimes de l'assurance maladie ;

2°) d'enjoindre au ministre des affaires sociales, de la santé et des droits des femmes d'abroger cet arrêté.

Vu les autres pièces du dossier ;

Vu :
- la Constitution, notamment son article 21 ;
- le code de la sécurité sociale ;
- la loi n° 78-17 du 6 janvier 1978 ;
- la loi n° 98-1194 du 23 décembre 1998 ;
- la loi n° 2004-806 du 9 août 2004 ;
- la décision du 27 février 2015 par laquelle le Conseil d'Etat statuant au contentieux n'a pas renvoyé au Conseil constitutionnel la question prioritaire de constitutionnalité soulevée par la société Celtipharm ;
- le code de justice administrative ;

Après avoir entendu en séance publique :
- le rapport de M. Frédéric Puigserver, maître des requêtes,
- les conclusions de M. Jean Lessi, rapporteur public ;

La parole ayant été donnée, avant et après les conclusions, à la SCP Odent, Poulet, avocat de

la société Celtipharm ;

1. Considérant qu'eu égard aux moyens qu'elle invoque, la société Celtipharm doit être regardée comme demandant l'annulation pour excès de pouvoir de la décision implicite de rejet résultant du silence gardé par le ministre des affaires sociales, de la santé et des droits des femmes sur sa demande du 19 juillet 2014, tendant à l'abrogation de l'arrêté du 19 juillet 2013 relatif à la mise en oeuvre du Système national d'information interrégimes de l'assurance maladie, en tant seulement qu'elle concerne les dispositions du 3° du III de l'article 4 de cet arrêté en vertu desquelles les organismes de recherche, universités, écoles ou autres structures d'enseignement liées à la recherche poursuivant un but lucratif ne peuvent accéder aux informations prévues à son article 3 ;

Sur l'irrecevabilité opposée par le ministre des affaires sociales, de la santé et des droits des femmes :

2. Considérant que la société requérante a pour objet, notamment, en vertu de l'article III de ses statuts, " la création, le développement, la gestion et l'actualisation de bases de données ou de connaissances, dans l'univers de la pharmacie (...), la diffusion et le transit des informations afférentes en France et à l'étranger " et la " mise à disposition des informations publiques, professionnelles et commerciales sur tous sites " ; que, par suite, contrairement à ce que soutient le ministre, cette société justifie d'un intérêt lui donnant qualité pour agir contre la décision attaquée dans la mesure mentionnée au point 1 ;

Sur la légalité de la décision attaquée :

3. Considérant, en premier lieu, que la loi du 23 décembre 1998 de financement de la sécurité sociale pour 1999 a prévu la création d'un système national d'information interrégimes de l'assurance maladie (SNIIRAM), devant être mis en place par les organismes gérant un régime de base d'assurance maladie, qui lui transmettent les données nécessaires ; qu'aux termes de l'article L. 161-28-1 du code de la sécurité sociale : " (...) Les modalités de gestion et de renseignement du système national d'information interrégimes de l'assurance maladie, 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, sont approuvées par un arrêté du ministre chargé de la sécurité sociale (...) pris après avis motivé de la Commission nationale de l'informatique et des libertés (...) " ;

4. Considérant que l'arrêté du 19 juillet 2013 du ministre des affaires sociales et de la santé relatif à la mise en oeuvre du SNIIRAM, pris après avis de la Commission nationale de l'informatique et des libertés, approuve, à son article 1er, le protocole du 8 juin 2012 et ses annexes définissant les modalités de gestion et de renseignement du système, passé entre les caisses d'assurance maladie mentionnées à l'article L. 161-28-1 du code de la sécurité sociale, et définit, à ses articles 2 à 7, les finalités du traitement ainsi mis en oeuvre, la liste des informations nécessaires, rassemblées dans une base de données nationale, les destinataires de ces informations, ainsi que les droits d'accès à ces informations, de rectification et d'opposition ; qu'à ce titre, le III de l'article 4 de cet arrêté prévoit que les destinataires des informations contenues dans le SNIIRAM sont, à raison de leurs fonctions et selon des règles d'habilitation définies par le protocole, en particulier, en vertu du 3°, certains organismes de recherche, en précisant que : " (...) Le traitement des informations (...) demandé par tout autre organisme de recherche, des universités, écoles ou autres structures d'enseignement liés à la

recherche (...) est soumis à l'approbation du bureau de l'Institut des données de santé. Aucun organisme de recherche, université, école ou autre structure d'enseignement lié à la recherche poursuivant un but lucratif ne peut accéder aux informations de l'article 3. La CNIL, conformément aux dispositions du chapitre X de la loi du 6 janvier 1978 susvisée, autorise ces traitements " ;

5. Considérant qu'en adoptant les dispositions en cause du 3° du III de l'article 4 de l'arrêté du 19 juillet 2013, en vertu desquelles les organismes de recherche, universités, écoles ou autres structures d'enseignement liées à la recherche poursuivant un but lucratif ne peuvent accéder aux informations mentionnées à son article 3, le ministre des affaires sociales et de la santé ne s'est pas borné à approuver les modalités de gestion et de renseignement du SNIIRAM, dont les destinataires habilités à recevoir communication des données qu'il rassemble, définies conjointement par le protocole passé entre les caisses d'assurance maladie ; que, contrairement à ce que fait valoir le ministre en défense, ces dispositions ne se déduisent pas de l'annexe II du protocole, dont l'objet est seulement d'identifier, pour certains utilisateurs, l'autorité compétente pour accéder aux informations contenues dans le SNIIRAM ; qu'il a ainsi lui-même fixé une telle règle ; que, dès lors, ces dispositions ne trouvent pas leur fondement légal dans les dispositions précitées de l'article L. 161-28-1 du code de la sécurité sociale ; que si le ministre se prévaut de l'article 3.5 du protocole, qui prévoit la fixation par arrêté ministériel des destinataires des informations contenues dans le SNIIRAM, une telle clause ne saurait fonder légalement sur ce point la compétence du ministre chargé de la sécurité sociale ; qu'aucun autre texte législatif ou réglementaire, notamment la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ne donne compétence à ce ministre pour déterminer les organismes de recherche ou d'enseignement pouvant accéder aux données du SNIIRAM ; que, dès lors, ces dispositions sont entachées d'incompétence ;

6. Considérant, en second lieu, que le chapitre X de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, en vigueur à la date de la décision attaquée, régit 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 ; qu'en vertu de son article 63, les données " issues des systèmes d'information des caisses d'assurance maladie, ne peuvent être communiquées à des fins statistiques d'évaluation ou d'analyse des pratiques et des activités de soins et de prévention que sous la forme de statistiques agrégées ou de données par patient constituées de telle sorte que les personnes concernées ne puissent être identifiées. / Il ne peut être dérogé aux dispositions de l'alinéa précédent que sur autorisation de la Commission nationale de l'informatique et des libertés dans les conditions prévues aux articles 64 à 66 (...) " ; qu'aux termes du premier alinéa de l'article 64 de la même loi, alors en vigueur : " Pour chaque demande, la commission vérifie les garanties présentées par le demandeur pour l'application des présentes dispositions et, le cas échéant, la conformité de sa demande à ses missions ou à son objet social. Elle s'assure de la nécessité de recourir à des données à caractère personnel et de la pertinence du traitement au regard de sa finalité déclarée d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention. Elle vérifie que les données à caractère personnel dont le traitement est envisagé ne comportent ni le nom, ni le prénom des personnes concernées, ni leur numéro d'inscription au Répertoire national d'identification des personnes physiques. En outre, si le demandeur n'apporte pas d'éléments suffisants pour attester la nécessité de disposer de certaines informations parmi l'ensemble des données à caractère personnel dont le traitement est envisagé, la commission peut interdire la communication de ces informations par l'organisme qui les détient et n'autoriser le traitement que des données ainsi réduites " ;

7. Considérant que ces dispositions ne restreignent pas la qualité des personnes susceptibles de solliciter, à des fins d'évaluation des pratiques de soins et de prévention, la communication d'informations issues du SNIIRAM sous forme de statistiques agrégées ou de données insusceptibles, même par recoupement avec d'autres données, d'identifier les personnes concernées ; que si elles soumettent à l'autorisation de la Commission nationale de l'informatique et des libertés, qui doit notamment vérifier les garanties présentées par le demandeur, la communication de données susceptibles de permettre une telle identification, elles n'excluent pas qu'une personne poursuivant un but lucratif puisse bénéficier d'une autorisation, dès lors que toutes les conditions en seraient remplies ; que les dispositions de l'article L. 161-28-1 du code de la sécurité sociale citées ci-dessus ne prévoient pas plus une telle exclusion ; qu'ainsi, en prévoyant que les organismes de recherche, universités, écoles ou autres structures d'enseignement liées à la recherche poursuivant un but lucratif ne pourraient accéder aux informations mentionnées à son article 3, l'arrêté du 19 juillet 2013 a ajouté une condition non prévue par la loi ; qu'il est, pour ce motif, également entaché d'illégalité ;

8. Considérant qu'il résulte de ce qui précède, sans qu'il soit besoin d'examiner les autres moyens de la requête, que la décision attaquée doit être annulée en tant qu'elle concerne les dispositions du 3° du III de l'article 4 de l'arrêté du 19 juillet 2013 relatif à la mise en oeuvre du SNIIRAM, en vertu desquelles les organismes de recherche, universités, écoles ou autres structures d'enseignement liées à la recherche poursuivant un but lucratif ne peuvent accéder aux informations prévues à son article 3 ;

Sur les conclusions à fin d'injonction :

9. Considérant que l'annulation de la décision attaquée implique nécessairement que le ministre chargé de la sécurité sociale abroge les dispositions du 3° du III de l'article 4 de l'arrêté du 19 juillet 2013 relatif à la mise en oeuvre du SNIIRAM en ce qu'elles prévoient que les organismes de recherche, universités, écoles ou autres structures d'enseignement liées à la recherche poursuivant un but lucratif ne peuvent accéder aux informations mentionnées à son article 3 ; qu'il y a lieu, par suite, d'enjoindre au ministre d'y procéder dans un délai de quatre mois à compter de la notification de la présente décision ;

D E C I D E :

Article 1er : La décision implicite par laquelle le ministre des affaires sociales, de la santé et des droits des femmes a refusé d'abroger l'arrêté du 19 juillet 2013 relatif à la mise en oeuvre du Système national d'information interrégimes de l'assurance maladie est annulée en tant qu'elle concerne les dispositions du 3° du III de l'article 4 de cet arrêté en vertu desquelles les organismes de recherche, universités, écoles ou autres structures d'enseignement liées à la recherche poursuivant un but lucratif ne peuvent accéder aux informations mentionnées à son article 3.
Article 2 : Il est enjoint au ministre des affaires sociales et de la santé d'abroger les dispositions du 3° du III de l'article 4 de l'arrêté du 19 juillet 2013 relatif à la mise en oeuvre du Système national d'information interrégimes de l'assurance maladie en ce qu'elles prévoient que les organismes de recherche, universités, écoles ou autres structures d'enseignement liées à la recherche poursuivant un but lucratif ne peuvent accéder aux informations mentionnées à son article 3, dans un délai de quatre mois à compter de la notification de la présente décision.
Article 3 : La présente décision sera notifiée à la société Celtipharm et à la ministre des affaires sociales et de la santé.

ANNEXE 6 : Schémas du circuit des demandes d'accès au SNDS

Schéma publié par le SNDS de 2016 à 2018

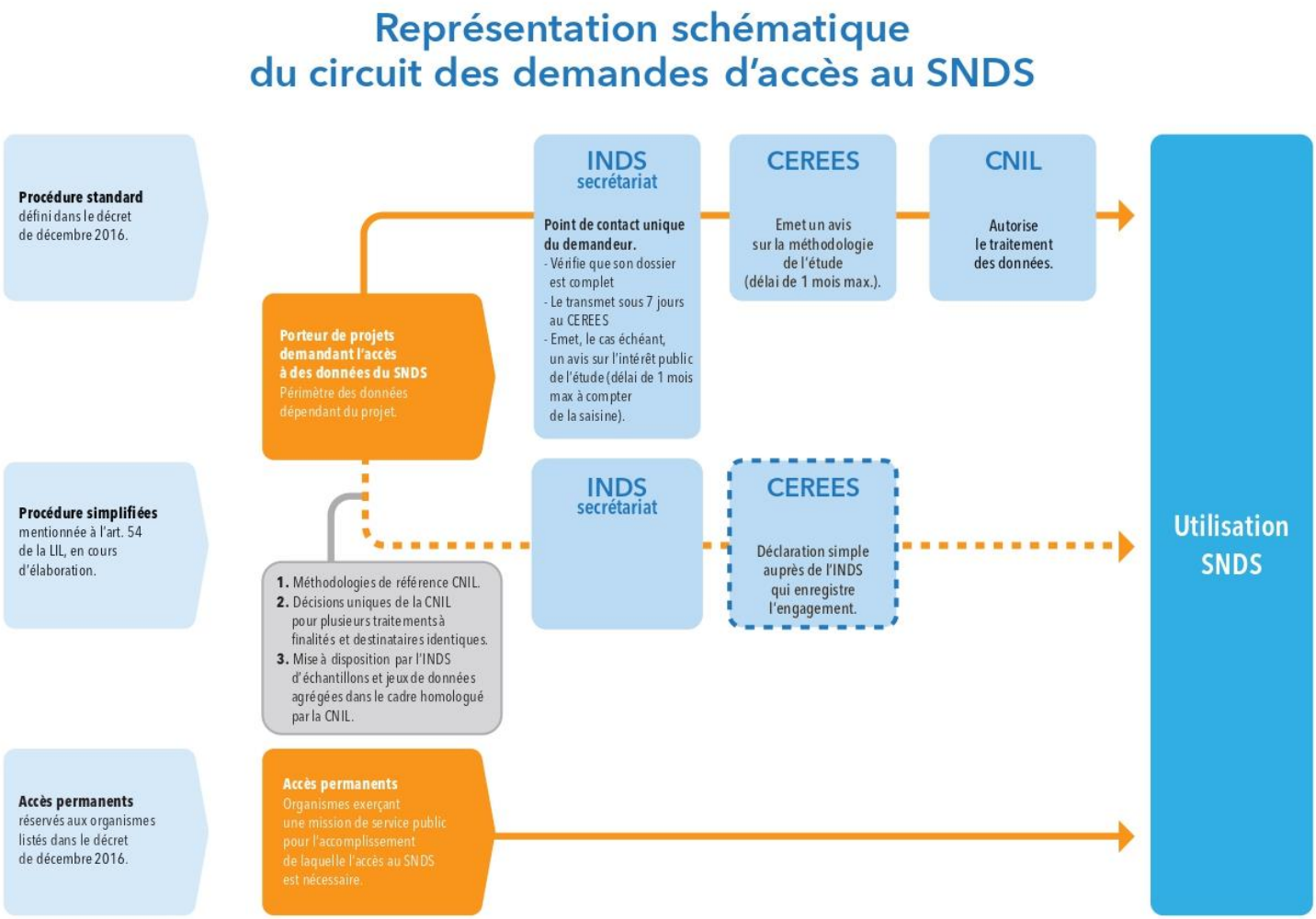
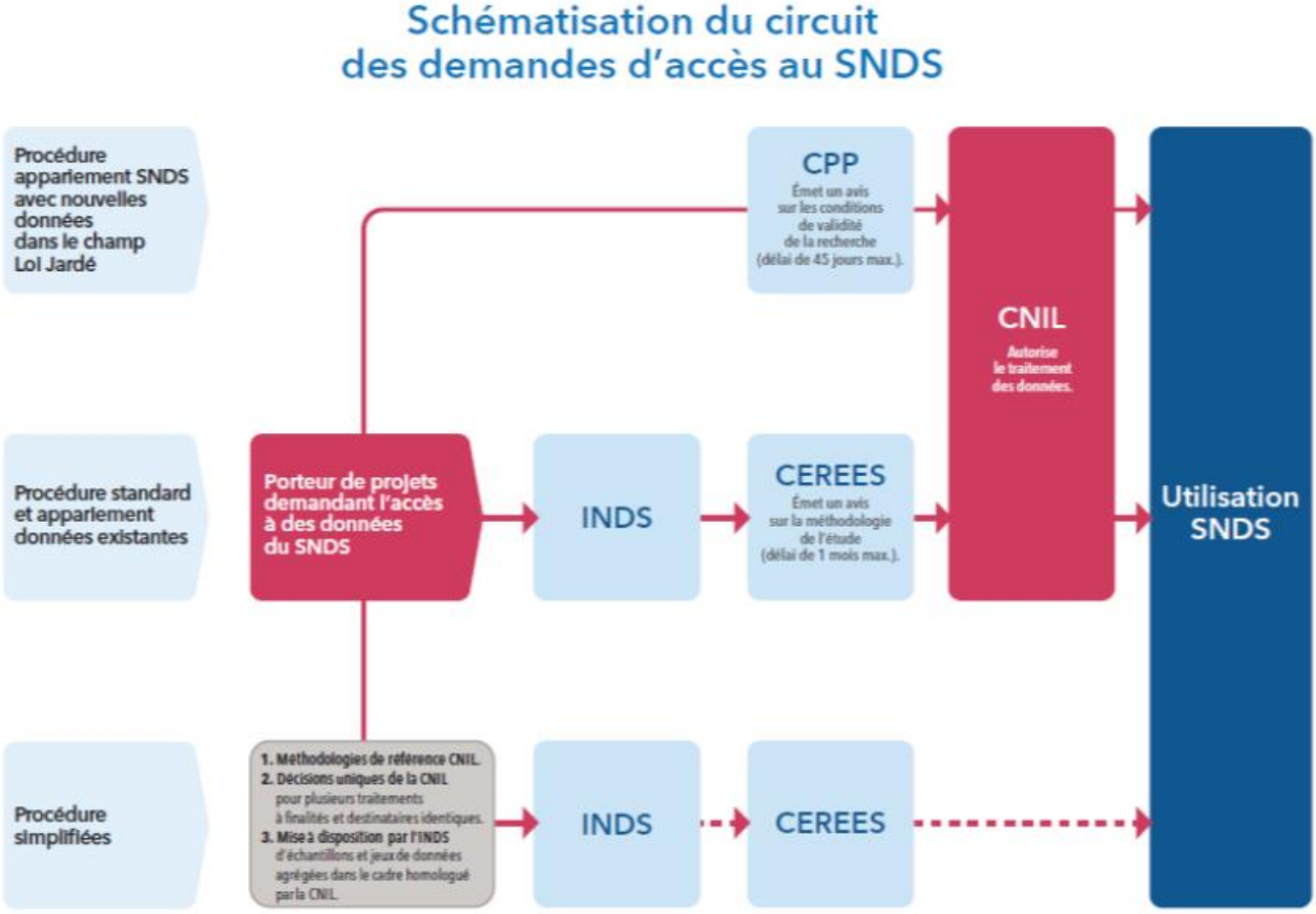


Schéma publié par le SNDS en 2019



ANNEXE 7 : Schémas des procédures d'accès simplifiées au SNDS

Schéma publié par le SNDS de 2016 à 2018

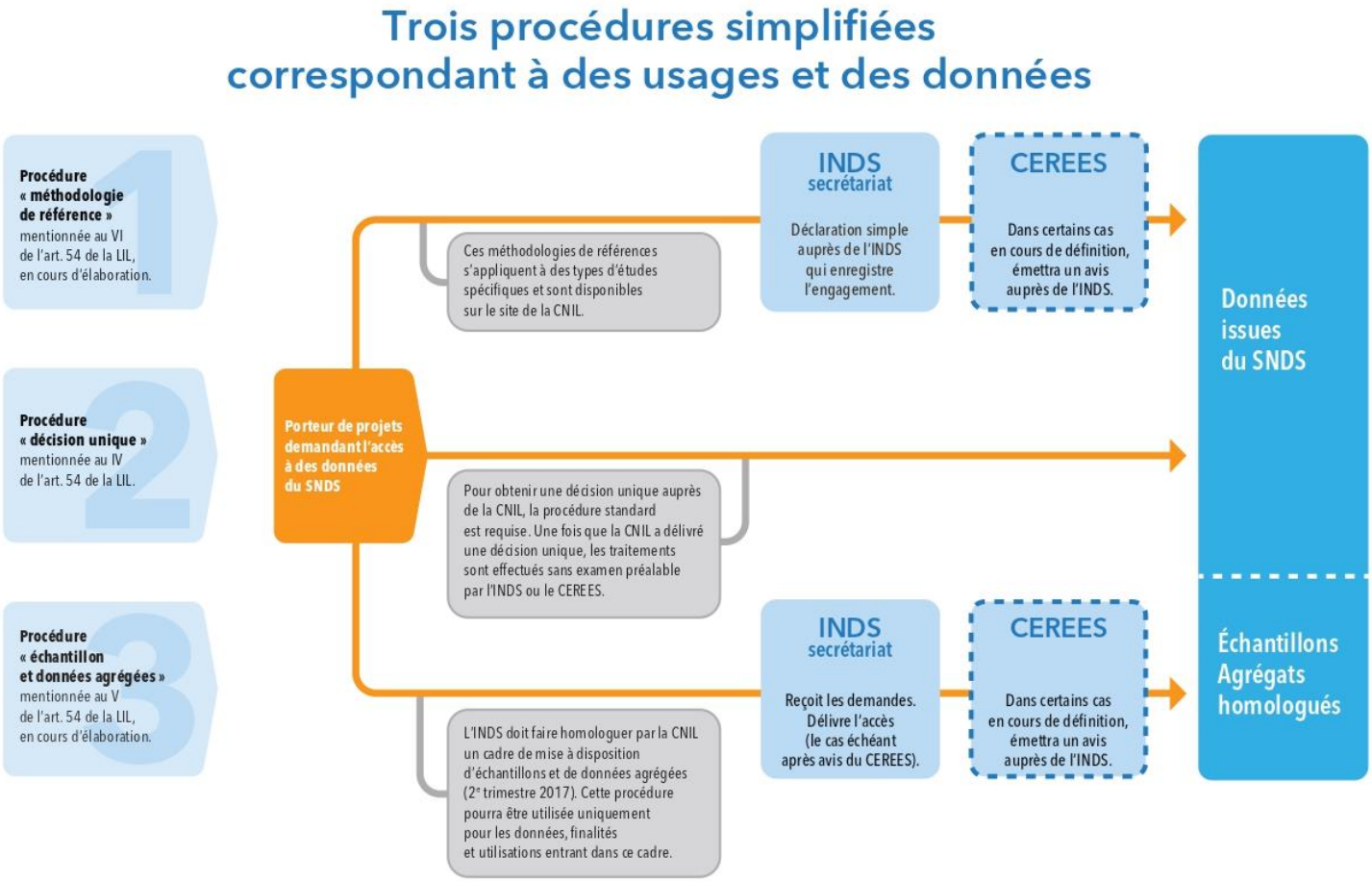


Schéma publié par le SNDS en 2019

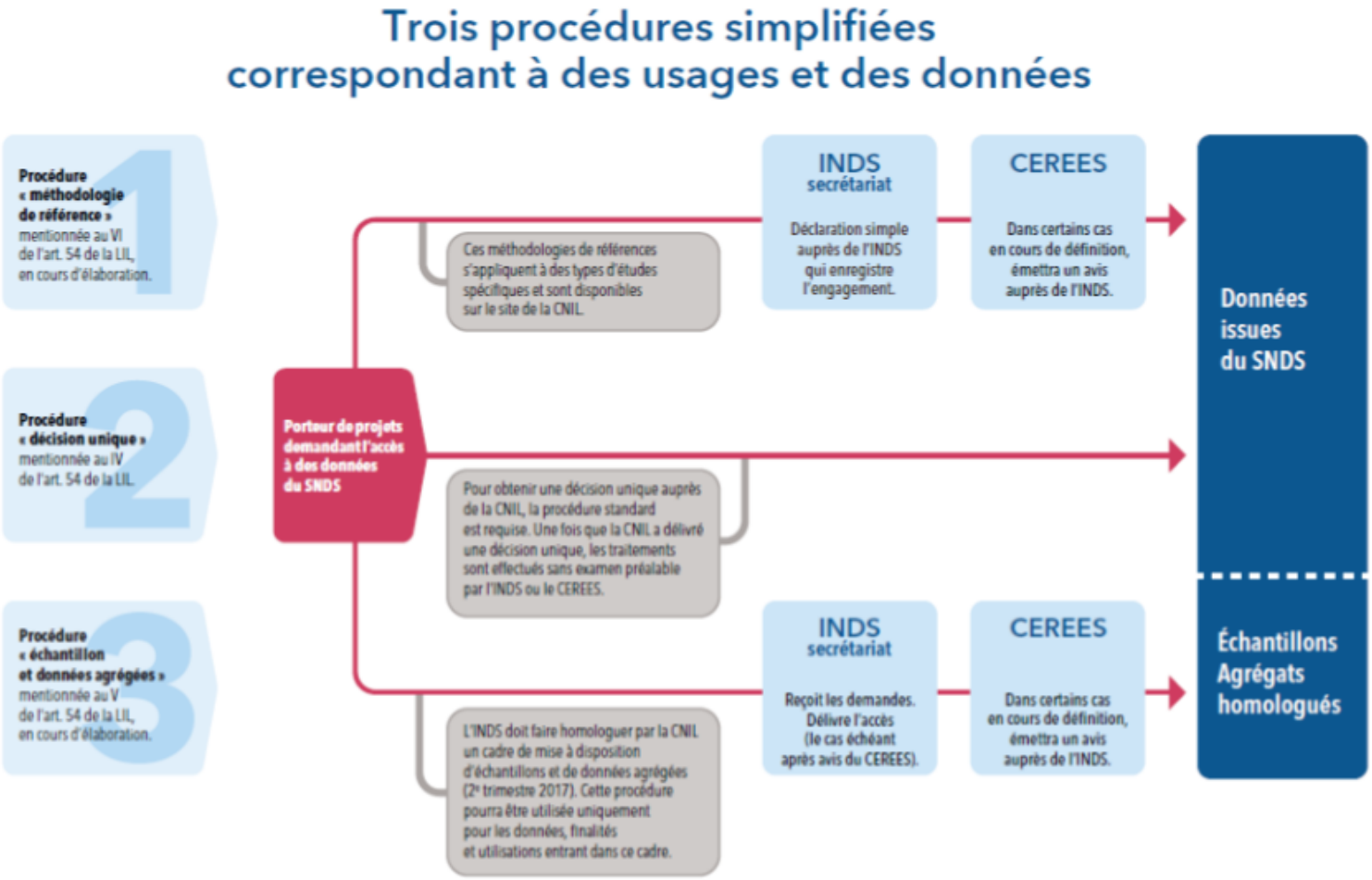


TABLE DES MATIÈRES

REMERCIEMENTS **5**

SOMMAIRE **7**

LISTE DES PRINCIPALES ABRÉVIATIONS **9**

INTRODUCTION **17**

Paragraphe 1 : La donnée de santé, une notion aux visages multiples 21
A) La donnée de santé, l'association de deux termes distincts 21
1) La donnée, une information transformée 21
2) La santé, une thématique vaste 23
3) La donnée de santé, une notion récemment définie 24
4) La donnée de santé au cœur des bases médico-administratives 27
B) Les données de santé : des données multi-catégorielles 30
1) La donnée de santé à caractère personnel 31
2) La donnée de santé anonyme 35
3) La donnée publique de santé 36
Paragraphe 2 : La donnée de santé : une notion aux nombreux enjeux 37
A) Les données de santé entre transparence et vie privée 38
1) Les opportunités de la transparence des données de santé 38
2) Les risques de la transparence des données de santé 41
3) La transparence des données de santé affectée par la succession des réformes 47
B) Les données de santé au cœur du monde numérique moderne 49
1) La revendication d'un open data en santé 49
2) Le big data en santé au service de l'économie numérique 52
C) Les données de santé au centre de l'attention d'une multiplicité d'acteurs 55
D) La structure thématique de l'étude 58

PARTIE I : LA TRANSPARENCE PERMANENTE DES DONNÉES DE SANTE RÉSERVÉE À DES ACTEURS PUBLICS PRIVILÉGIÉS **61**

TITRE I : L'ACCÈS PERMANENT AUX DONNÉES DE SANTÉ JUSTIFIÉ PAR LE MEILLEUR FONCTIONNEMENT DU SERVICE PUBLIC *67*
CHAPITRE I : L'ACCES PERMANENT OUVERT UNIQUEMENT À DES ACTEURS PRIVILÉGIÉS DU SERVICE PUBLIC 71
SECTION 1 : LES ACTEURS CENTRAUX DU SERVICE PUBLIC SEULS BÉNÉFICIAIRES DE L'ACCÈS PERMANENT 71
Paragraphe 1 : L'hésitante évolution des bénéficiaires de l'accès permanent 71
Paragraphe 2 : La réforme pertinente et maîtrisée de l'accès permanent 79
SECTION 2 : LES ACTEURS CENTRAUX DU SERVICE PUBLIC CONTRÔLÉS DANS LEUR USAGE DE L'ACCÈS PERMANENT 84
Paragraphe 1 : L'utilité avérée de l'accès permanent 84
Paragraphe 2 : Le contrôle individuel du bénéfice de l'accès permanent 86
CONCLUSION DU CHAPITRE I 91
CHAPITRE II : L'ACCÈS PERMANENT PRUDEMMENT OUVERT AU NOM DE LA SÉCURITÉ DES DONNÉES 93
SECTION 1 : LA PRUDENCE : LA SÉCURISATION PRIORITAIRE DES DONNÉES DE SANTÉ 93
Paragraphe 1 : Le double contrôle des données accessibles en permanence 94
Paragraphe 2 : La nécessaire mise à l'épreuve de la sécurisation des données 98
SECTION 2 : L'ÉLARGISSEMENT PERTINENT MAIS ERRATIQUE DES DONNÉES DE SANTÉ ... 104
Paragraphe 1 : L'ouverture prudente des données de santé en accès permanent 105
Paragraphe 2 : L'élargissement instable des données en accès permanent 109
CONCLUSION DU CHAPITRE II 115

CONCLUSION DU TITRE I *117*

TITRE II : L'ACCÈS PERMANENT AUX DONNÉES DE SANTÉ LIMITÉ PAR LA PROTECTION DE LA VIE PRIVÉE *119*

CHAPITRE I : L'IDENTIFICATION DES LIMITES VACCILLANTES DE L'ACCÈS PERMANENT 123

SECTION 1 : L'APPARENCE ARBITRAIRE DU CHOIX DES BÉNÉFICIAIRES DE L'ACCÈS PERMANENT 123

Paragraphe 1 : Le processus méconnu du choix des bénéficiaires 123

Paragraphe 2 : Le manque de maîtrise de l'accès permanent 128

SECTION 2 : L'ARGUMENT FRAGILISÉ DE LA SÉCURITÉ DES DONNÉES EN ACCÈS PERMANENT 132

Paragraphe 1 : L'insuffisance de l'argument sécuritaire 132

Paragraphe 2 : La sécurité au détriment des bénéficiaires 136

CONCLUSION DU CHAPITRE I 141

CHAPITRE II : LE DÉPASSEMENT BIENVENU DES LIMITES À L'ACCÈS PERMANENT 143

SECTION 1 : LA SOUS-EXPLOITATION DOMMAGEABLE DE L'ACCÈS PERMANENT 143

Paragraphe 1 : L'insuffisance d'utilisation de l'accès permanent 144

Paragraphe 2 : L'insuffisance d'évaluation de l'accès permanent 148

SECTION 2 : POUR UNE EXPLOITATION AMÉLIORÉE DE L'ACCÈS PERMANENT 152

Paragraphe 1 : L'amélioration justifiée de l'encadrement de l'accès permanent 152

Paragraphe 2 : Les lacunes de la réforme de l'accès permanent 157

CONCLUSION DU CHAPITRE II 161

CONCLUSION DU TITRE II *163*

CONCLUSION DE LA PARTIE I 165

PARTIE II : LA TRANSPARENCE SÉLECTIVE DES DONNÉES DE SANTÉ AU BÉNÉFICE DES ACTEURS PUBLICS ORDINAIRES ET PRIVÉS À BUT NON LUCRATIF 169

TITRE I : L'ACCÈS SÉLECTIF AUX DONNÉES DE SANTÉ JUSTIFIÉ PAR LA PROTECTION DE LA VIE PRIVÉE *175*

CHAPITRE I : L'ACCÈS SÉLECTIF OUVERT À DES ACTEURS STRICTEMENT CONTRÔLÉS 179

SECTION 1 : L'OUVERTURE DÉLIMITÉE DE L'ACCÈS SÉLECTIF 179

Paragraphe 1 : Les bénéficiaires variés de l'accès sélectif 179

Paragraphe 2 : Le contrôle individuel renforcé de l'accès sélectif 185

SECTION 2 : LA SÉVÉRITÉ DE L'ENCADREMENT DE L'ACCÈS SÉLECTIF 192

Paragraphe 1 : Les garanties préalables à l'accès sélectif 193

A) Les finalités autorisant l'accès sélectif 193

B) Les principes généraux de l'accès sélectif 200

Paragraphe 2 : Les sanctions pesant sur les bénéficiaires de l'accès sélectif 204

CONCLUSION DU CHAPITRE I 209

CHAPITRE II : L'ACCÈS SÉLECTIF SOUMIS À UNE PROCÉDURE PROTECTRICE DE LA VIE PRIVÉE 213

SECTION 1 : LA NATURE CONTRAIGNANTE DE LA PROCÉDURE D'ACCÈS SÉLECTIF 213

Paragraphe 1 : La structure binaire de l'accès sélectif aux données de santé 213

Paragraphe 2 : Le contrôle renforcé de l'accès sélectif aux données de santé 219

SECTION 2 : L'ASSOUPLISSEMENT NÉCESSAIRE DE LA PROCÉDURE D'ACCÈS SÉLECTIF 224

Paragraphe 1 : La rigidité initiale de l'accès sélectif aux données de santé 225

Paragraphe 2 : La nouvelle approche simplifiée de l'accès sélectif 229

A) L'esprit unificateur de la réforme du 26 janvier 2016 229

B) La simplification de la réforme altérée par l'adaptation au droit européen 235

CONCLUSION DU CHAPITRE II 241

CONCLUSION DU TITRE I *243*

TITRE II : L'ACCÈS SÉLECTIF AUX DONNÉES DE SANTÉ EFFECTIF SOUS CONDITIONS *245*

CHAPITRE I : L'ACCÈS SÉLECTIF ENTRAVÉ PAR SES DYSFONCTIONNEMENTS 249

SECTION 1 : L'ACCÈS SÉLECTIF AFFAIBLI PAR SA STRUCTURE 249
Paragraphe 1 : Le constat de l'inadaptation de l'accès sélectif 249
Paragraphe 2 : La dispersion des compétences nuisible à l'accès sélectif 253
SECTION 2 : L'ACCÈS SÉLECTIF DÉCRÉDIBILISÉ PAR SES BLOCAGES INTERNES 258
Paragraphe 1 : La complexité des données issues de l'accès sélectif 258
Paragraphe 2 : Les délais de traitement aléatoires de l'accès sélectif 263
CONCLUSION DU CHAPITRE I 269
CHAPITRE II : L'ACCÈS SÉLECTIF RÉFORME SOUS DE NOUVELLES CONDITIONS 271
SECTION 1 : LE NÉCESSAIRE CHANGEMENT DE PARADIGME DE L'ACCÈS SÉLECTIF 271
Paragraphe 1 : Les solutions de simplification de l'accès sélectif 271
Paragraphe 2 : Les complexités incompressibles de l'accès sélectif 276
SECTION 2 : LA MISE À L'ÉPREUVE CONSTRUCTIVE DE L'ACCÈS SÉLECTIF 280
Paragraphe 1 : Les lacunes du nouvel l'accès sélectif 281
A) Le sentiment d'inachevé du nouvel accès sélectif 281
B) L'incertitude constante du coût du nouvel l'accès sélectif 287
C) La mise en place ralentie des accès simplifiés 292
Paragraphe 2 : L'avenir de l'accès sélectif pavé d'incertitudes 297
A) Les incertitudes durables de l'accès sélectif 298
B) La sécurité contestée de l'accès sélectif 305
CONCLUSION DU CHAPITRE II 309

CONCLUSION DU TITRE II 311

CONCLUSION DE LA PARTIE II 313

PARTIE III : LA TRANSPARENCE TARDIVE DES DONNÉES DE SANTÉ POUR LES ACTEURS PRIVÉS À BUT LUCRATIF 315

TITRE I : L'INTERDICTION INITIALE D'ACCÈS AUX DONNÉES DE SANTÉ POUR LES ACTEURS PRIVÉS À BUT LUCRATIF 317
CHAPITRE I : LA FERMETURE DE L'ACCÈS AUX DONNÉES DE SANTÉ POUR LE RESPECT DE LA VIE PRIVÉE 321
SECTION 1 : LE CHANGEMENT DE PARADAGIME DE L'ACCÈS AUX DONNÉES DE SANTÉ 321
Paragraphe 1 : La flexibilité première de l'accès aux données de santé 321
Paragraphe 2 : L'interdiction expresse d'accéder aux données de santé 325
SECTION 2 : LES RARES EXCEPTIONS À L'INTERDICTION D'ACCÉDER AUX DONNÉES DE SANTÉ 330
Paragraphe 1 : La possibilité de l'accès sélectif par procuration 330
Paragraphe 2 : L'ouverture prudente à de rares acteurs privés 335
CONCLUSION DU CHAPITRE I 341
CHAPITRE II : L'OUVERTURE ATTENDUE DE L'ACCÈS AUX DONNÉES DE SANTÉ DANS LE RESPECT DE LA VIE PRIVÉE 343
SECTION 1 : LES ARGUMENTS EN FAVEUR DE L'ACCÈS AUX DONNÉES DE SANTÉ 343
Paragraphe 1 : Les acteurs institutionnels favorables à l'ouverture au secteur privé à but lucratif 343
Paragraphe 2 : Les prémices jurisprudentiels favorables au secteur privé à but lucratif 348
SECTION 2 : LE REVIREMENT DE LA LOI ET DU JUGE EN FAVEUR DE L'OUVERTURE DES DONNÉES DE SANTÉ 352
Paragraphe 1 : La consécration légale de l'autorisation d'accès aux données de santé 352
Paragraphe 2 : La consécration jurisprudentielle de l'autorisation d'accès aux données de santé 357
CONCLUSION DU CHAPITRE II 363

CONCLUSION DU TITRE I 365

TITRE II : L'AUTORISATION PROGRESSIVE D'ACCÈS AUX DONNÉES DE SANTÉ POUR LES ACTEURS PRIVÉS À BUT LUCRATIF 367
CHAPITRE I : L'ACCÈS AUX DONNÉES DE SANTÉ REFUSÉ SANS MOTIF CONCRET 369
SECTION 1 : L'INTROUVABLE JUSTIFICATION DU REFUS D'AUTORISATION D'ACCÈS 369
Paragraphe 1 : Le caractère arbitraire du refus d'autorisation d'accès 369

Paragraphe 2 : L'argument sécuritaire discutable du refus d'autorisation d'accès 375
SECTION 2 : LES RISQUES POTENTIELS INSUFFISANTS DE L'AUTORISATION D'ACCÈS 379
Paragraphe 1 : La nouveauté des données ouvertes, argument irrecevable du refus d'autorisation d'accès 379
Paragraphe 2 : L'inconnue des données massives, argument fragile du refus d'autorisation d'accès 384
CONCLUSION DU CHAPITRE I 389
CHAPITRE II : L'ACCÈS AUX DONNÉES DE SANTÉ AUTORISÉ DANS UN CONTEXTE FAVORABLE 391
SECTION 1 : LES ARGUMENTS PROPICES À L'AUTORISATION D'ACCÈS 391
Paragraphe 1 : L'autorisation d'accès favorisée par les incohérences de l'interdiction 391
Paragraphe 2 : L'autorisation d'accès favorisée par des contre-arguments convaincants 395
SECTION 2 : LES GARANTIES BIENVENUES MAIS INCOMPLÈTES DE L'AUTORISATION D'ACCÈS 399
Paragraphe 1 : L'autorisation d'accès fonctionnelle mais imparfaite 400
A) L'accès sélectif classique opérationnel 400
B) Les accès simplifiés encore en phase de développement 404
Paragraphe 2 : L'autorisation d'accès confortée par le Règlement européen relatif à la protection des données 409
CONCLUSION DU CHAPITRE II 415
CONCLUSION DU TITRE II *417*

CONCLUSION DE LA PARTIE III 419

CONCLUSION GÉNÉRALE 423

BIBLIOGRAPHIE 429

[Ouvrages] *429*

[Ouvrages collectifs] *432*

[Thèses] *433*

[Rapports et Avis] *433*

[Articles] *436*

[Autres] *449*

[Décisions de justice et délibérations] *450*

[Textes normatifs] *454*

[Sites internet] *462*

INDEX 465

ANNEXES 471

ANNEXE 1 : Arrêté du 11 avril 2002 relatif à la mise en œuvre du système national d'information inter-régimes de l'assurance maladie *472*

ANNEXE 2 : Arrêté du 20 juin 2005 relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie *476*

ANNEXE 3 : Arrêté du 19 juillet 2013 relatif à la mise en œuvre du Système national d'information interrégimes de l'assurance maladie *479*

ANNEXE 4 : Décret n° 2016-1871 relatif au traitement de données à caractère personnel dénommé « système national des données de santé » *483*

ANNEXE 5 : Conseil d'Etat, 1ère - 6e chambres réunies, 20 mai 2016, n° 385305, recueil Lebon, Celtipharm *490*

ANNEXE 6 : Schémas du circuit des demandes d'accès au SNDS *494*
Schéma publié par le SNDS de 2016 à 2018 494
Schéma publié par le SNDS en 2019 495

ANNEXE 7 : Schémas des procédures d'accès simplifiées au SNDS *496*
Schéma publié par le SNDS de 2016 à 2018 496
Schéma publié par le SNDS en 2019 497

TABLE DES MATIÈRES 499

Résumé en Français

Les données numérisées font aujourd'hui partie de notre quotidien. Parmi elles, les données de santé à caractère personnel représentent une frange particulièrement sensible à traiter et à partager car elles recèlent des renseignements relatifs à la vie privée des personnes. Elles font donc l'objet d'une protection spécifique par principe. Mais elles sont, dans le même temps, hautement convoitées du fait du potentiel qu'elles représentent pour l'amélioration de l'ensemble du système de santé. En France, deux grandes bases de données historiques, le SNIIRAM et le PMSI, sont dédiées à la récolte et au traitement des données de santé. Bien que ces bases ne contiennent aucune information directement identifiante, elles ont longtemps été verrouillées et accessibles à des conditions très strictes, parfois peu intelligibles, au nom du respect de la vie privée des individus. L'accès difficile à ces bases représente cependant une perte de connaissance avérée et des moyens juridiques et techniques existent pour assurer la sécurité des données et le droit au respect de la vie privée des individus. C'est notamment pour cette raison que les modalités d'accès aux données de santé à caractère personnel contenues dans ces bases ont été entièrement réformées et continuent de l'être. Pour bien comprendre le cheminement qui a conduit à l'ouverture récente des bases de données médico-administratives, cette étude s'attache à connaître le fonctionnement des accès à ces données depuis leur création jusqu'à nos jours. Au regard des typologies d'accès qui existent, cela demande de se positionner selon trois angles : celui des acteurs publics privilégiés qui bénéficient d'un accès permanent ; celui des acteurs publics ordinaires et des acteurs privés à but non lucratif qui peuvent accéder à certaines données en se pliant à un régime d'autorisation préalable ; celui des acteurs privés à but lucratif qui ont d'abord été mis à l'écart de l'accès aux données de santé avant d'y être finalement admis. L'évolution de l'accès à ces données sensibles est, encore aujourd'hui, au cœur de l'actualité à travers une réforme supplémentaire de la gouvernance des bases de données médico-administratives et de leur contenu. Ce nouveau projet entend faire cohabiter la protection du droit au respect de la vie privée avec l'accès le plus ouvert possible au plus grand nombre de données de santé.

Abstract in English

Digitized data is an integral part of our daily lives. Among them, personal health data represent a particularly sensitive group which must be processed and shared with care because they contain information relating to the private lives of individuals. They are therefore subject to special protection as a matter of principle. But at the same time, they are highly coveted because of their potential to improve the entire healthcare system. In France, two major historical databases, SNIIRAM and PMSI, are dedicated to the collection and processing of health data. Although these databases do not contain any personally identifying information, they have long been accessible only under very strict conditions, sometimes difficult to understand, in the name of respect for the privacy of individuals. However, difficult access to these databases represents a proven loss of knowledge, and legal and technical means exist to ensure data security and the right to privacy of individuals. It is for this reason in particular that the procedures for accessing the personal health data contained in these databases have been completely reformed and continue to be reformed. To fully understand the process that led to the recent opening of medico-administrative databases, this study focuses on how access to these data has worked from their creation to the present day. With regard to the types of access that exist, this requires positioning oneself from three angles: that of privileged public actors who benefit from permanent access; that of ordinary public actors and private non-profit actors who can access certain data by complying with a prior authorization regime; and that of private for-profit actors who were first excluded from access to health data before finally being admitted. The evolution of access to this sensitive data is still a headlining topic due to a further reform of the governance of medico-administrative databases and their content. This new project aims to ensure that the protection of the right to privacy is combined with the widest possible access to as much health data as possible.