Droits et Débats

Santé et protection des données

Un colloque organisé par le Conseil d'État
le 1er décembre 2017

Publications du Conseil d'État chez le même éditeur

Collection « Les rapports du Conseil d'État » (ancienne collection « Études et documents du Conseil d'État », EDCE)

- Le numérique et les droits fondamentaux – étude annuelle 2014, n° 65.
- L'action économique des personnes publiques – étude annuelle 2015, n° 66
- Simplification et qualité du droit – étude annuelle 2016, n° 67.
- Puissance publique et plateformes numériques : accompagner l'« ubérisation » – étude annuelle 2017, n° 68.
- La citoyenneté - Être (un) citoyen aujourd'hui – étude annuelle 2018, n° 69.
- Le sport : quelle politique publique ?, étude annuelle 2019, n° 70.

Collection « Les études du Conseil d'État »

- Le droit d'alerte : signaler, traiter, protéger, 2016.
- Règles applicables aux professionnels de santé en matière d'information et de publicité, 2018.
- La prise en compte du risque dans la décision publique : pour une action publique plus audacieuse, 2018.
- Révision de la loi de bioéthique : quelles options pour demain ?, 2018.
- L'expérimentation des politiques publiques, 2019.

Collection « Droits et Débats »

- Où va l'État ? – Tome 1, n° 14 (2015), et Tome 2, n° 19 (2016).
- Impôt et cotisation : quel financement pour la protection sociale ?, n° 15, 2015.
- La France dans la transformation numérique : quelle protection des droits fondamentaux ?, n° 16, 2016.
- La fiscalité sectorielle, n° 17, 2016.
- L'ordre juridique national en prise avec le droit européen et international : questions de souveraineté ? Le regard croisé du Conseil d'État et de la Cour de cassation, n° 18, 2016.
- L'accord : mode de régulation du social, n° 20, 2016.
- Entretiens sur l'Europe – Tome 1, n° 21 (2017), et Tome 2, n° 26 (2018).
- Droit comparé et territorialité du droit – Tome 1, n° 22, et Tome 2, n° 23, 2017.
- Les entreprises publiques, n° 24, 2017.
- Le droit social et la norme internationale, n° 25, 2018.
- L'ordre public. Regards croisés du Conseil d'État et de la Cour de cassation, n° 27, 2018.
- Les grands investissements publics, n° 28, 2019.
- Santé et protection des données, n° 29, 2019.
- La fiscalité internationale à réinventer ?, n° 30 (à paraître).

Collection « Histoire et Mémoire »

- Faire des choix ? Les fonctionnaires dans l'Europe des dictatures, 1933-1948, 2014.
- Le Conseil d'État et la Grande Guerre, 2017.
- Guide de recherche dans les archives du Conseil d'État, 2019.

Collection « Jurisprudences »

- Jurisprudence du Conseil d'État 2016-2017 (éd. 2018).

Sommaire

Avant-propos

Martine de Boisdeffre
Présidente de la section du rapport et des études

Quelques mois avant l'entrée en vigueur du règlement général sur la protection des données, adopté par le Parlement européen et le Conseil le 27 avril 2016[1], et alors que se préparait la réforme de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, pour l'adapter à la nouvelle réglementation européenne[2], le Conseil d'État a voulu contribuer à la réflexion contemporaine sur l'utilisation et la protection d'une catégorie de données personnelles particulièrement sensibles, les données de santé.

Le Conseil d'État connaît de ce sujet depuis longtemps. Dès la fin des années 1960, dans son rapport annuel de 1969-1970, il s'était interrogé sur « *les conséquences du développement de l'informatique sur les libertés publiques et privées et sur les décisions administratives* » et avait anticipé les risques posés par la constitution de banques de données regroupant des informations personnelles sur les individus[3]. Des recommandations du rapport de Bernard Tricot, conseiller d'État et rapporteur général de la commission informatique et libertés, constituée en 1974, sous la présidence conjointe du vice-président du Conseil d'État, Bernard Chenot, et du premier président de la Cour de cassation, Maurice Aydalot, est issue la loi du 6 janvier 1978 qui a consacré, pour la première fois, un droit à la protection des données personnelles[4].

Dans l'exercice de sa fonction consultative, en donnant un avis sur les projets de décrets autorisant la constitution de traitements de données à caractère personnel[5], comme dans l'exercice de sa fonction contentieuse, en contrôlant la légalité des décisions administratives autorisant ces traitements, le Conseil d'État a veillé au respect de ce droit, corollaire du droit à la protection de la vie privée, en

1 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit règlement général sur la protection des données (RGPD).

2 La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a été modifiée 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 du 6 janvier 1978 et diverses dispositions concernant la protection des données à caractère personnel (voir J.-M. Pastor, « La loi informatique et libertés est réécrite », *in AJDA*, 2018, p. 2468).

3 Rapport cité *in* Conseil d'État, Étude *annuelle 2014, Le numérique et les droits fondamentaux*, Paris, La documentation Française, 2014, p. 71.

4 La loi donnait à toute personne un droit d'opposition, d'information, d'accès et de rectification sur les informations nominatives la concernant qui font l'objet d'un traitement automatisé.

5 L'article 15 de la loi, dans sa version initiale, exigeait un décret pris sur avis conforme du Conseil d'État pour passer outre l'avis défavorable de la commission nationale de l'informatique et des libertés sur la constitution des traitements automatisés de données personnelles pour le compte des personnes publiques et des personnes privées chargées d'une mission de service public. L'article 18 de la loi, dans sa version initiale, prévoyait que l'utilisation du répertoire national d'identification des personnes physiques pour effectuer des traitements nominatifs devait être autorisée par décret en Conseil d'État.

mettant en œuvre un « *triple test de proportionnalité* »[6]. Ainsi, « *l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée que constituent la collecte, la conservation et le traitement, par une autorité publique, d'informations personnelles nominatives, ne peut être légalement autorisée* », juge-t-il dans un arrêt d'assemblée du 26 octobre 2011, *Association pour la promotion de l'image*, « *que si elle répond à des finalités légitimes et que le choix, la collecte et le traitement des données sont effectués de manière adéquate et proportionnée au regard de ces finalités* »[7].

Les questions autour de l'utilisation et de la protection des données personnelles ont été profondément renouvelées par la révolution technologique, en particulier dans le domaine de la santé. Dans l'étude annuelle 2014, *Le numérique et les droits fondamentaux*, le Conseil d'État a constaté que le « *Big Data* »[8], caractérisé à la fois par l'explosion du volume des données personnelles et la multiplication de leurs usages, « *ouvre la voie à de nouvelles méthodes de recherche scientifique* » ainsi qu'à l'amélioration de l'efficacité des politiques publiques[9].

L'analyse de grandes bases de données de santé peut permettre d'identifier les facteurs environnementaux ou génétiques des maladies, de détecter les incidents associés à des médicaments ou encore de constater des anomalies dans la consommation de médicaments ou la réalisation d'actes de soins. Par exemple, c'est une étude effectuée par la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS) sur la base du système national d'information inter-régimes de l'assurance maladie (SNIIRAM)[10] qui a confirmé le lien entre la prise du Médiator et le développement de certaines pathologies cardiaques.

L'accès aux données de santé revêt ainsi un enjeu crucial pour la recherche scientifique, comme pour la conception et la mise en œuvre des politiques de santé publique, la maîtrise des dépenses de santé, la veille épidémiologique et pharmacologique, la prévention et la prise en charge des pathologies. Le partage et l'utilisation des données de santé sont toutefois porteurs de risques, tels que, notamment, la violation de la vie privée et du secret médical, l'atteinte à la réputation, le mésusage des données ou encore la stigmatisation de groupes humains ou de certains comportements. L'ouverture de l'accès aux données de santé doit s'accompagner d'une protection accrue de ces données. La loi du

6 Suivant l'expression de M. Guyomar et de X. Domino dans leur chronique « Le passeport biométrique au contrôle : empreintes et clichés », *in AJDA*, 2012, p. 35.

7 CE, Ass., 26 octobre 2011, n°s 317827, 317952, 318013 et 318051, *Association pour la promotion de l'image et autres*, cl° J. Boucher. Le traitement litigieux était le fichier « TES » qui recueille les données biométriques des passeports. Pour une application de ce contrôle à un traitement automatisé comprenant des données de santé, en l'espèce un fichier constitué par la direction des ressources humaines du ministère de la défense pour la gestion administrative des demandes de pension, voir : CE, 15 octobre 2014, n°s 358876, 358877, 358878, 358879, 359084, 359089 et 359118, *Union nationale du personnel en retraite de la gendarmerie et autres*, cl° Éd. Crépey.

8 Les données massives.

9 Conseil d'État, Étude *annuelle 2014, Le numérique et les droits fondamentaux*, *op. cit.*, p. 48 et suiv. Voir aussi l'annexe 3, « Numérique et santé », p. 361 et suiv.

10 Le SNIIRAM est une base de données qui regroupe l'ensemble des actes de soins de la médecine de ville ayant donné lieu à remboursement par les régimes d'assurance maladie.

26 janvier 2016 de modernisation de notre système de santé[11] a été adoptée pour atteindre et concilier ces différentes exigences.

Dans ce contexte, le Conseil d'Etat a estimé utile de réunir des chercheurs, des juristes et des acteurs du secteur médico-social pour faire un état des lieux des réformes juridiques mises en œuvre pour étendre l'utilisation des données de santé tout en améliorant leur protection.

11 Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

Programme du colloque

9h30 - 10h00 – Séance d'ouverture

Jean-Marc Sauvé, vice-président du Conseil d'État

10h00 - 11h15 – Table ronde n° 1 : La définition des données de santé

Président **:** **Didier Tabuteau**, président adjoint de la section sociale du Conseil d'État

Intervenants **:** **Rémi Decout-Paolini**, rapporteur public à la section du contentieux du Conseil d'État

Irina Vasiliu, chef d'équipe unité protection des données personnelles à la direction générale de la justice et des consommateurs (DG JUST) de la Commission européenne

Jean-Pierre Mignard, avocat au barreau de Paris, membre du Comité national consultatif d'éthique

11h15 - 12h30 – Table ronde n° 2 : La mise en œuvre de la loi santé

Président **:** **Pierre-Louis Bras**, inspecteur général des affaires sociales, président du Conseil d'orientation des retraites (COR)

Intervenants **:** **Mylène Girard**, cheffe de la mission accès aux données de santé, direction de la recherche, des études et de l'évaluation des statistiques (DREES)

Dominique Polton, présidente de l'Institut national des données de santé (INDS)

Thomas Dautieu, directeur adjoint de la conformité à la Commission nationale de l'informatique et des libertés (CNIL)

14h15 - 15h30 – Table ronde n° 3 : L'accès aux données et la protection sanitaire

Président **:** **François Stasse**, conseiller d'État honoraire, administrateur de l'Institut national de la santé et de la recherche médicale (INSERM)

Intervenants **:** **François Bourdillon**, directeur général de l'Agence nationale de la santé publique (ANSP)

Patrick Maddalone, sous-directeur des conditions de travail, de la santé et de la sécurité au travail au ministère du travail

Christian Saout, membre du collège de la Haute Autorité de santé (HAS)

15h30 - 16h45 – Table ronde n° 4 : Le secret médical partagé

Présidente **:** **Pascale Fombeur**, présidente de la 1re chambre de la section du contentieux du Conseil d'État

Intervenants **:** **Anne Laude**, professeure, doyenne de la faculté de droit de l'université Paris-Descartes, co-directrice de l'Institut droit et santé

Agnès Martinel, conseillère à la 2e chambre civile de la Cour de cassation

Jacques Lucas, vice-président du Conseil national de l'ordre des médecins

17h00 - 17h30 – Séance de clôture

Jean-Denis Combrexelle, président de la section sociale du Conseil d'État

Jean-Marc Sauvé
Vice-président du Conseil d'État

Diplômé de l'Institut d'études politiques de Paris (1970) et titulaire d'une maîtrise de sciences économiques (1971), Jean-Marc Sauvé est ancien élève de l'École nationale d'administration (ENA, 1975-1977). Il rejoint le Conseil d'État en 1977 comme auditeur, avant d'exercer des responsabilités à l'extérieur du Conseil d'État, comme conseiller technique au cabinet du garde des sceaux, ministre de la justice (1981-1983), directeur de l'administration générale et de l'équipement au ministère de la justice (1983-1988), directeur des libertés publiques et des affaires juridiques au ministère de l'intérieur (1988-1994), préfet de l'Aisne (1994-1995) et secrétaire général du Gouvernement (1995-2006). Jean-Marc Sauvé est, depuis le 3 octobre 2006, vice-président du Conseil d'État. À ce titre, il préside le Conseil supérieur des juridictions administratives et le Conseil d'administration de l'ENA. Il a également été président du conseil d'administration de l'Académie de France à Rome (Villa Médicis) de 1999 à 2008, membre du conseil d'administration du Musée du Louvre (2002-2008) et président de la commission pour la transparence financière de la vie politique (2006-2013). Il a présidé, de mars 2010 à février 2018, le comité prévu par l'article 255 du traité sur le fonctionnement de l'Union européenne, chargé de donner un avis sur l'aptitude des candidats à l'exercice des fonctions de juge et d'avocat général à la Cour de justice et au Tribunal de l'Union européenne. Il est, depuis le 20 octobre 2017, président de la Cité internationale universitaire de Paris.

Mesdames, Messieurs les présidents[12],
Mesdames, Messieurs,
Mes chers collègues,

« *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* ». Par ces mots, placés en ouverture de la loi du 6 janvier 1978, le législateur, inspiré par le rapport du Président Tricot[13], a sans doute pris quelques libertés avec la normativité de la loi. Mais il a surtout, de manière très claire, porté témoignage à la fois du potentiel de progrès offert par le développement de l'informatique et des risques qu'elle peut faire peser sur les libertés fondamentales et, notamment, le respect de la vie privée.

12 Texte écrit en collaboration avec Sarah Houllier, magistrat administratif, chargée de mission auprès du vice-président du Conseil d'État.
13 Rapport de la Commission informatique et libertés remis en 1975.

Le cœur de l'informatique, ce sont des informations qui font l'objet de traitements automatiques et puissants et de diffusions potentiellement infinies. Parmi ces informations, les données à caractère personnel sont devenues la matière première de l'économie numérique, de l'activité des GAFA[14] et des réseaux sociaux qui s'en nourrissent, afin d'offrir des services d'intermédiation et de mise en relation des usagers.

Bien avant l'essor d'Internet et des plateformes numériques et l'identification des risques qu'ils font courir pour la vie privée, le législateur avait perçu la nécessité d'encadrer le traitement des données personnelles, en particulier par la puissance publique alors perçue comme la source principale de danger. Car ces données peuvent être erronées, collectées et conservées de manière injustifiée ou disproportionnée et, de surcroît, elles sont susceptibles de révéler, sur chaque personne, des habitudes, des préférences ou des opinions. C'est dans ce contexte qu'avait été adoptée la loi du 6 janvier 1978 qui a créé la Commission nationale de l'informatique et des libertés (CNIL)[15].

Au sein des données à caractère personnel, certaines sont encore plus sensibles que d'autres : en particulier celles qui se rapportent à l'état de santé d'une personne, aux traitements médicaux qu'elle suit et aux pathologies dont elle peut être affectée. Ces informations relèvent en effet de l'intime. Elles sont pourtant susceptibles de faire l'objet de traitements ou de communications au même titre que les autres données à caractère personnel, voire même davantage compte tenu de l'intérêt qui s'attache à ce qu'un État puisse posséder une vision claire de l'état de santé de sa population, des risques sanitaires et de l'efficacité des traitements proposés et qu'il puisse aussi mieux maîtriser les dépenses de santé.

Le partage des données de santé est ainsi porteur d'enjeux importants pour le développement d'un système de santé publique efficace et performant. Le président Massot a magistralement éclairé ces enjeux, cette problématique et cette histoire de notre droit dans son article de 2014[16].

Dans ce contexte singulier – sensibilité particulière de ces données et intérêt de leur exploitation et de leur partage –, les données de santé font l'objet d'une protection qui tient compte de leur spécificité, mais dont l'équilibre a été récemment revu pour assurer une conciliation plus adaptée entre le nécessaire respect de la vie privée des personnes physiques et la poursuite d'objectifs légitimes de santé publique.

14 L'acronyme GAFA désigne les quatre entreprises les plus puissantes de l'Internet (*Google*, *Apple*, *Facebook* et *Amazon*), auquel on ajoute parfois *Microsoft* (GAFAM).
15 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
16 J. Massot, « Santé et assurance maladie », *in* A. Debet, J. Massot, N. Metallinos (dir), *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, éd. Lextenso, Paris, 2015.

1. - Compte tenu de leur sensibilité, les données de santé font de longue date l'objet d'une protection qui a toutefois révélé certaines lacunes ou impasses.

1.1. - Ces données revêtent un caractère à la fois sensible et d'intérêt général.

1.1.1. - En raison de leur contenu même, elles touchent à l'essence de la vie privée et de l'intime.

C'est ce qui a très tôt justifié que leur protection soit arrimée à celle de la vie privée. En prenant appui sur l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales – communément appelée Convention européenne des droits de l'homme (Convention EDH) –, la Cour européenne des droits de l'homme (Cour EDH) s'est attachée à définir les contours de cette protection en affirmant à la fois la nécessité de protéger les données personnelles, mais aussi la particularité des données de santé dans ce cadre et l'intérêt de leur conférer une protection renforcée. Sur le plan législatif, la protection des données de santé au titre de la protection de la vie privée est assurée à la fois par le code civil[17], le code de la santé publique[18] et la loi du 6 janvier 1978 révisée[19]. Cette protection a aussi une dimension constitutionnelle, le Conseil constitutionnel ayant reconnu que les données de santé doivent être protégées au titre du respect de la vie privée[20].

La protection des données de santé est également assurée par l'obligation de secret pesant sur les professionnels de santé[21], qui est, pour la Cour EDH, au cœur de la « *confiance des patients dans le corps médical et les services de santé en général* »[22] . Il en résulte une protection particulière de ce secret. Comme les atteintes à la vie privée, les manquements au secret médical sont réprimés par le code pénal[23] et ils peuvent aussi faire l'objet de poursuites disciplinaires[24]. La communication des documents administratifs susceptibles de porter atteinte à la vie privée ou au secret médical est en outre interdite[25].

Par ailleurs, la sensibilité des données de santé tient aussi à ce que leur collecte et leur traitement sont susceptibles d'être conçus ou détournés à des fins

17 Article 9 du code civil : « *Chacun a droit au respect de sa vie privée. (…)* ».
18 Article L. 1110-4 du code de la santé publique.
19 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
20 CC, 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, n° 99-416 DC, consid. 45 : il n'est pas sans intérêt de relever que la première décision constitutionnelle qui range les données de santé au nombre de celles dont la révélation est susceptible de porter atteinte à la vie privée est aussi la première décision qui rattache le respect de la vie privée à l'article 2 de la Déclaration des droits de l'homme et du citoyen. Voir aussi : CC, 21 décembre 1999, *Loi de financement de la sécurité sociale pour 2000*, n° 99-422 DC, consid. 52.
21 Article L. 1110-4 du code de la santé publique.
22 CEDH, 25 février 1997, *Z. c. Finlande*, aff. n° 22009/93, pt. 95.
23 Article 226-13 du code pénal.
24 Voir, notamment : CE, 29 décembre 2000, *M. G.*, n° 211240 et CE, 28 mai 1999, *M. Tordjemann*, n° 189057.
25 Article 6 de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal. Voir notamment : CE, 30 décembre 2015, *Société les laboratoires Servier*, n° 372230 par lequel le Conseil d'État rappelle que lorsque les données à caractère personnel ont aussi le caractère de documents administratifs, elles ne sont communicables aux tiers que s'il est possible d'occulter ou de disjoindre les mentions portant atteinte à la vie privée ou au secret médical.

commerciales ou d'élaboration de profils par et au service d'entreprises privées, notamment celles qui fournissent des services de banque ou d'assurance.

1.1.2. - En dépit de ces risques, le traitement des données de santé présente d'indéniables avantages.

Il concourt, notamment, à la transparence et à l'efficacité du système de santé[26]. La collecte et la diffusion de ces informations permettent, en effet, d'alimenter le débat public sur la santé et, en particulier, de nourrir l'élaboration, la conduite et l'évaluation des politiques publiques de santé[27]. De manière plus significative encore, le traitement des données de santé peut apporter une aide déterminante à la vigilance pharmaco-épidémiologique, améliorer l'efficacité des parcours de soins[28], favoriser la recherche de longue durée sur les protocoles de soins et permettre une veille sanitaire renforcée. L'exploitation des données du système national d'information inter-régimes de l'assurance maladie (SNIIRAM)[29] a, par exemple, permis de mettre au jour les dérives de l'utilisation du Médiator lorsqu'il était prescrit en dehors de l'indication prévue par l'autorisation de mise sur le marché[30]. Les données de santé sont en outre susceptibles de renseigner sur l'évolution des dépenses de santé. La finalité première du SNIIRAM, créé par la loi du 23 décembre 1998[31], était d'ailleurs la maîtrise des dépenses de santé, dans une logique économique prévenant la surconsommation inefficace de médicaments et la multiplication tout aussi vaine des traitements[32].

1.2. - Les risques liés à l'utilisation des données de santé et, dans le même temps, l'intérêt public qui s'attache à leur traitement et leur diffusion ont conduit à créer, pour ces données, un cadre juridique à la fois souple et protecteur, qui s'est toutefois avéré insuffisant.

1.2.1. - La protection des données de santé s'est d'abord inscrite dans le droit commun de la protection des données personnelles, dès lors que la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[33] ne leur réservait aucun sort particulier.

Il a fallu attendre la loi du 4 mars 2002, qui a créé l'article L. 1110-4 du code de la santé publique[34], puis la loi du 6 août 2004[35], qui a transposé la directive européenne

26 Étude annuelle du Conseil d'État, *Numérique et droits fondamentaux*, Annexe 3, éd. La documentation Française, Paris, 2014, p. 367.
27 P.-L. Bras, *Rapport sur la gouvernance et l'utilisation des données de santé*, septembre 2013, p. 43.
28 E. Debiès, « L'ouverture et la réutilisation des données de santé : panorama et enjeux », *in RDSS*, 2016, p. 697.
29 Article L. 161-28-1 du code de la sécurité sociale.
30 Étude annuelle du Conseil d'État, *Numérique et droits fondamentaux, op. cit.*, p. 368.
31 Article 21 de la loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale pour 1999.
32 Étude annuelle du Conseil d'État, *Numérique et droits fondamentaux, op. cit.*, pp. 367-368. L'évaluation des politiques de santé n'est devenue l'un des objectifs de ce système d'information qu'en 2004 (loi n° 2004-806 du 9 août 2004 relative à la politique de santé publique).
33 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
34 Article 3 de la loi n° 2002-203 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.
35 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.

de 1995 sur la protection des données, pour que notre droit national prévoie un cadre juridique spécifiquement adapté aux données de santé. Au premier chef, l'article L. 1110-4 du code de la santé publique protège le « *droit au respect de sa vie privée et du secret des informations la concernant* » pour toute personne prise en charge par un professionnel de santé ou un organisme participant à la prévention et aux soins. Les mesures mises en œuvre pour assurer le respect de ce principe doivent en outre respecter les dispositions de la loi du 6 janvier 1978 qui, depuis la loi du 6 août 2004, protège dans son article 8 les données devant, du fait de leur sensibilité, faire l'objet d'une protection particulière : à savoir, les données relatives à la santé ou la vie sexuelle d'une personne, au même titre que les données permettant de faire « *apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou l'appartenance syndicale* »[36]. En principe, ces données ne peuvent faire l'objet d'aucun traitement[37], l'objectif étant d'éviter les traitements de données sensibles aux fins d'assurer la surveillance des personnes ou de servir des intérêts privés.

Dans quelques hypothèses précisément énoncées, la finalité du traitement peut toutefois justifier son autorisation[38]. C'est le cas lorsque la personne concernée a donné son consentement exprès au traitement, ou que celui-ci est nécessaire à la sauvegarde de la vie humaine, à l'exercice d'un droit en justice, ou à des fins de médecine préventive, de diagnostic ou de gestion des services de santé. Le législateur a aussi prévu d'autoriser le traitement des données nécessaires à la recherche dans le domaine de la santé. En toute hypothèse, le traitement de données de santé doit être accompagné de garanties appropriées pour en garantir la sécurité. Cinq principes gouvernent cette protection : 1) les données doivent être collectées de manière loyale et licite, 2) en vue d'une finalité déterminée et légitime ; 3) les données collectées doivent être pertinentes et adéquates au regard de cette finalité, 4) elles doivent être complètes et exactes et 5) leur conservation doit être prévue pour une durée définie[39]. Le consentement des personnes n'est en revanche pas toujours obligatoire[40].

Au-delà de ces principes, la loi du 6 janvier 1978 rappelle, depuis son adoption, l'interdiction de porter une appréciation sur un comportement humain en se fondant uniquement sur un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé[41].

36 I de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
37 *Ibid*.
38 II de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
39 Article 6 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
40 Le II de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés liste les cas dans lesquels le consentement des personnes n'est pas nécessaire. Ce sont, par exemple, les cas où le traitement est nécessaire à l'exercice d'un droit en justice ou qu'il est justifié par des fins de médecine préventive, de diagnostics médicaux, de l'administration de soins ou de traitements, etc.
41 Article 2 devenu article 10 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

1.2.2. - Ce régime juridique a toutefois éprouvé des difficultés à concilier efficacement le respect de la vie privée et le souhait légitime de pouvoir utiliser ces données pour des motifs d'intérêt général.

Il a été, au fil du temps, confronté à deux faiblesses : l'inadaptation face aux risques du numérique, et la trop grande rigidité de la règle pour atteindre certains objectifs d'intérêt général. D'une part, l'essor du numérique a profondément bouleversé les conditions d'accès aux données de santé et de communication de celles-ci. L'économie numérique repose en effet largement sur des traitements massifs de données personnelles dont les opérateurs économiques se servent pour proposer et vendre des biens et des services. Les mégadonnées ont imposé leurs modes opératoires et leur efficacité. Les données de santé n'échappent pas à ce mouvement[42]. Cette évolution ne va toutefois pas sans risques pour la vie privée des personnes, ni dans l'utilisation de ces données. Bien que ces risques demeurent faibles s'agissant de systèmes pour lesquels de réels traitements d'anonymisation ont été exécutés, l'inclusion de données de santé en apparence anonymes dans un système d'information peut, dans certaines hypothèses, permettre la réidentification des personnes grâce à certaines informations comme le lieu de naissance, la durée et le lieu des consultations de santé[43] Plus encore, les réseaux sociaux font naître une nouvelle appréhension de ces questions. Ils permettent aux malades d'entrer en contact et de partager des informations sur leur état de santé, leur traitement et la progression de leur maladie[44]. Ces réseaux permettent aussi de cartographier les lieux d'occurrence d'une maladie afin de déconseiller les zones à risque en cas d'épidémie[45]. À la main des personnes et non d'administrations ou d'institutions publiques, ils mettent en évidence une profonde évolution sociale qui conduit à une communication plus large, voire à la dissémination sans limite de données susceptibles de renseigner sur l'état de santé au détriment du respect de la vie privée. Dès lors que ces données sont volontairement communiquées par les intéressés, est posée la question de leur consentement aux traitements subséquents susceptibles d'être mis en œuvre. Notre société est ainsi confrontée à un bouleversement supplémentaire induit par le numérique : la détermination du régime juridique des données personnelles et, en particulier, des données de santé et la nécessité d'une approche renouvelée de ces sujets. Ces questions sont d'autant plus sensibles que les traitements se massifient avec les mégadonnées, que les flux transfrontaliers de données se développent, et que les opérateurs sont de moins en moins territoriaux ou nationaux et même européens.

D'autre part, le régime juridique défini dans les années 1990 et 2000 s'est avéré excessivement rigide pour les organismes désireux d'en faire une utilisation à des fins de recherche ou de médecine préventive dans un objectif d'intérêt général. En l'absence d'une doctrine claire, et en présence de mécanismes d'accès jugés trop restrictifs, les données de santé ont été sous-exploitées[46]. Il en résulte des difficultés

42 E. Debiès, « L'ouverture et la réutilisation des données de santé : panorama et enjeux », *préc.*, p. 697.

43 P.-L. Bras, *Rapport sur la gouvernance et l'utilisation des données de santé*, *op. cit.*, p. 26.

44 Étude annuelle du Conseil d'État, *Numérique et droits fondamentaux*, *op. cit.*, p. 371.

45 C'est le cas par exemple de l'application *Germtracker* (Étude annuelle du Conseil d'État, *Numérique et droits fondamentaux, op. cit.*, p. 371).

46 P.-L. Bras, *Rapport sur la gouvernance et l'utilisation des données de santé, op. cit.*, p. 31.

pour atteindre les objectifs d'amélioration du système de soins, d'innovation ou de recherche médicale, dans le respect de la vie privée des personnes et du secret de leurs données de santé.

2. - Le régime juridique de la protection des données de santé a, par conséquent, été refondu pour tenter de répondre à ces exigences contradictoires.

C'est ce que s'est efforcée de faire la loi du 26 janvier 2016 de modernisation de notre système de santé[47]. Car un régime qui ne protège pas assez et qui contraint trop ne répond pas aux objectifs et aux espoirs placés en lui.

2.1. - En premier lieu, le champ de la protection des données de santé devait être révisé et peut-être resserré.

2.1.1. - Compte tenu de la diversité des situations susceptibles d'engendrer des données en lien avec la santé, il est d'abord nécessaire de s'entendre sur le champ des données protégées au sens de la législation nationale et de la règlementation européenne.

L'existence d'une maladie, un traitement médical et un protocole de soins sont, sans doute possible, des données de santé, de même que les caractéristiques physiologiques ou psychiques d'une personne. En est-il de même des données dites de « bien-être » ? Le mouvement du « quantification de soi » (en anglais, « *quantified self* ») interroge en effet le cadre de la protection des données de santé[48]. À l'aide d'applications numériques, chacun peut désormais mesurer et comparer certaines variables de son mode de vie : nutrition, sommeil, activité physique, etc. Cette évolution pose la question de savoir si ces données, telles que le rythme cardiaque mesuré par une montre connectée lors d'une course ou les données nutritionnelles d'une personne, sont des données de santé. Elles ont indéniablement la faculté de renseigner sur certaines caractéristiques physiologiques ou physiques. Elles sont également en mesure, par extrapolation, de renseigner sur l'existence d'un risque cardiovasculaire ou de diabète, par exemple. La situation socio-économique d'une personne peut-elle aussi être qualifiée de donnée de santé ? Ce n'est pas certain. Certaines des données que je viens d'évoquer sont, somme toute, assez indirectement liées à l'état de santé d'une personne. Par conséquent, quel régime faut-il leur appliquer ? Celui, renforcé, des données de santé, ou « seulement » celui des données à caractère personnel ? Une définition large assure une protection renforcée de la vie privée des personnes, mais elle est de nature à créer des obstacles dans l'accès et l'utilisation, y compris à des fins légitimes d'intérêt général, des données de santé. La récente loi du 26 janvier 2016 n'a pas pris position sur ce point. Le règlement européen sur la protection des données de 2016, qui entrera en vigueur en 2018, a en revanche adopté une conception large de ces données qui recouvre, à la fois, les données

47 Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé. Voir aussi ce sur point : CE, 20 mai 2016, *Société Celtipharm*, n° 385305 par lequel le Conseil d'État annule l'arrêté du 19 juillet 2013 relatif à la mise en œuvre du SNIIRAM en tant qu'il interdit aux organismes de recherche, universités et école poursuivant un but lucratif d'accéder aux informations de ce système.

48 Voir, sur ce sujet, le rapport de la CNIL, *Le corps, nouvel objet connecté. Du quantified self à la M-Santé : les nouveaux territoires de la mise en données du monde*, *in* Cahiers IP, Innovation et Prospective, n° 2, mai 2014.

relatives à la santé d'une personne et les données susceptibles de fournir une indication sur un état de santé[49]. Une telle définition avait déjà été retenue par la Cour de justice de l'Union européenne (CJUE) sur le fondement de la directive de 1995 eu égard à la nécessité de donner une portée utile à cette directive[50].

2.1.2. - La conciliation des exigences de vie privée et d'intérêt général au sens large suppose en outre de s'interroger sur le champ du secret médical.

Ce dernier demeure une règle déontologique et pénale forte, mais sa portée s'est amenuisée à mesure que le champ des dérogations possibles s'est élargi. La loi du 26 janvier 2016 a, par exemple, étendu les possibilités de communication aux hypothèses de diagnostic d'une maladie infectieuse transmissible[51] ou à la nécessité de se défendre en justice. Le secret médical peut en outre être partagé entre un nombre plus important de professionnels grâce au dossier médical partagé (DMP), qui devient un outil de coopération entre professionnels de santé avec pour objectif de mieux coordonner les soins et d'éviter les examens redondants.

La nouveauté introduite par la loi du 26 janvier 2016 est de permettre ce partage entre les professionnels de santé, mais aussi avec tous les professionnels qui participent à la prise en charge du patient, y compris les professionnels du secteur social et médico-social[52]. En contrepartie, le code de la santé publique prévoit que « *tous les professionnels intervenant dans le système de santé* » sont soumis au secret[53]. En revanche, à l'égard des personnes privées, le secret médical reste absolu, notamment à l'égard de l'employeur, du banquier ou de l'assureur. Par conséquent, sans qu'il ne puisse être fait le constat d'un effacement du secret médical, les hypothèses de dévoilement ou de partage, voire de dilution de ce secret se font plus nombreuses.

2.2. - En second lieu, les modalités de mise en œuvre de l'accès, de la collecte, et du traitement des données de santé ont été précisées.

2.2.1. - L'article 193 de la loi du 26 janvier 2016 redéfinit complètement la politique d'accès aux données de santé au profit d'une ouverture renforcée.

D'un point de vue formel, cette réforme s'est traduite par le regroupement de l'ensemble des bases de données de santé en un seul ensemble, le système national des données de santé (SNDS), composé notamment du système national

49 Considérant 35 et article 4§15 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Cela inclut aussi bien les données collectées au moment de l'inscription en vue de bénéficier d'un soin, que les informations obtenues à l'issue d'une analyse, d'un examen ou d'un test médical et les informations concernant un traitement clinique ou l'état physiologique d'une personne.

50 CJCE, 6 novembre 2003, *Lindqvist*, aff. C-101/01, pt. 49.

51 Article D. 3113-7 du code de la santé publique.

52 II et III de l'article L. 1110-4 du code de la santé publique.

53 I de l'article L. 1110-4 du code de la santé publique.

d'information inter-régimes de l'assurance maladie (SNIIRAM)[54]. Un institut national des données de santé (INDS) est créé pour centraliser les demandes d'autorisation d'accès aux données et émettre des avis sur le caractère d'intérêt public d'une recherche[55]. En outre, la loi du 26 janvier 2016 ouvre plus largement l'accès aux données de santé en distinguant entre celles qui sont complètement anonymes et celles qui peuvent permettre l'identification ou la réidentification des personnes. Les premières sont mises à la disposition du public avec pour objectif de permettre à tous de les utiliser, y compris les organismes à but lucratif. L'intérêt de cette approche est de favoriser l'innovation, mais aussi la transparence et le débat en matière de santé publique[56].

En revanche, les données comportant un risque de réidentification sont uniquement ouvertes aux personnes qui justifient d'un motif d'intérêt public et à condition qu'elles respectent la vie privée des intéressés. En ce qui concerne les données véritablement anonymes, le Conseil d'État a, par exemple, jugé que l'amélioration de la connaissance relative à la consommation des produits de santé était un objectif légitime justifiant le traitement des données issues des feuilles de soins anonymisées[57].

En outre, la loi demande aux assureurs et aux industriels en produits de santé d'apporter des garanties supplémentaires pour éviter que l'utilisation des données ne conduise à une sélection du risque pour les premiers et à un ciblage commercial pour les seconds[58]. Ils doivent ainsi soit justifier que la méthode de traitement retenue ne permettra aucune forme d'identification ou de profilage, soit recourir à un intermédiaire agréé pour accéder à la base de données[59]. Le règlement européen de 2016 confirme cette approche en insistant sur la nécessité de prévenir la communication des informations recueillies à des tiers non-médicaux ou qui ne sont pas impliqués dans la poursuite d'un objectif d'intérêt général[60].

54 Article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé qui crée un article L. 1461-1 du code de la santé publique. L'objectif est notamment de permettre l'information sur la santé, la définition et l'évaluation des politiques de santé, la connaissance des dépenses dans ce domaine, l'information des professionnels, la surveillance sanitaire et la recherche dans le domaine de la santé.

55 Article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé qui crée un article L. 1462-1 du code de la santé publique.

56 Cette évolution s'inscrit dans le droit-fil de la jurisprudence de la Commission d'accès aux documents administratifs (CADA) qui avait estimé que les données anonymes demandées par l'association *Initiative Transparence Santé* dans le sillage de l'affaire du Médiator pouvaient lui être transmises, dès lors qu'elles sont anonymes et ne peuvent donc porter atteinte au secret médical ou à la vie privée des personnes (Avis CADA, 21 novembre 2013, n° 2013/4348, p. 2).

57 CE, 26 mai 2014, *Société IMS Health*, n° 354903.

58 E. Debiès, « L'ouverture et la réutilisation des données de santé : panorama et enjeux », *préc.*, p. 697.

59 Article L. 1461-3-I du code de la santé publique créé par l'article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé publique.

60 Considérant 53 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Enfin, la loi du 26 janvier 2016 prévoit des obligations renforcées pour le traitement et la conservation des données de santé sur support numérique et leur transmission par voie électronique, afin de garantir leur qualité et leur confidentialité[61].

2.2.2. - La recherche d'un meilleur équilibre entre le respect de la vie privée des personnes et une plus grande ouverture de l'accès aux données de santé repose sur une régulation confiée, en particulier, à la Commission nationale de l'informatique et des libertés (CNIL) et, ultimement, au juge.

La CNIL joue depuis l'origine un rôle central dans la protection des données de santé. Bien avant que la loi de 1978 ne consacre leur caractère particulier, elle s'est attachée à contrôler les conditions d'utilisation de certains fichiers existants au moment de son entrée en vigueur. Elle a ainsi émis, dès 1981, un emblématique avis défavorable à l'utilisation du fichier « GAMIN » qui prévoyait le traitement automatisé des certificats de santé des jeunes enfants, compte tenu des risques de « profilage » des enfants devant en priorité être suivis par les services de la protection maternelle et infantile (PMI)[62]. S'agissant de la prise en charge du SIDA, la CNIL s'est aussi attachée, avec une extrême attention, à encadrer rigoureusement les conditions du traitement des données de santé aux fins de recherche[63]. Ce faisant, elle s'est inscrite dans le droit-fil de la jurisprudence de la Cour EDH[64]. En outre, dans le cadre de la loi du 26 janvier 2016, la CNIL s'assure que les procédures de traitement à des fins de recherche protègent la confidentialité des données et que celles-ci ne seront conservées que pour une durée limitée nécessaire au traitement[65]. Cette approche, fondée sur un mécanisme d'autorisation allégé, devrait permettre de faciliter la recherche dans le domaine de la santé en s'appuyant notamment sur les bases de données existantes.

Dans un second temps, le juge est appelé à vérifier que les garanties mises en œuvre sont adaptées et suffisantes, dans une logique de contrôle de proportionnalité[66]. Il s'assure aussi du respect du secret médical et du respect de la vie privée lors de l'instruction des affaires dont il est saisi. Ainsi, le juge administratif peut demander au requérant, à qui le secret médical n'est pas opposable, de produire son dossier médical ou, le cas échéant, à l'administration de le communiquer au requérant. Il n'appartient en revanche qu'au requérant de décider s'il entend porter son

61 Article L. 1110-4-1 du code de la santé publique : « *Afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, les professionnels de santé, les établissements et services de santé, les hébergeurs de données de santé à caractère personnel et tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social utilisent, pour leur traitement, leur conservation sur support informatique et leur transmission par voie électronique, des systèmes d'information conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24. Ces référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés* ».

62 Délibération n° 81-74 du 16 juin 1981 portant décision et avis relatifs à un traitement d'informations nominatives concernant le traitement automatisé des certificats de santé dans les services de la protection maternelle et infantile (annexe 10 au rapport d'activité de la CNIL pour 1980-1981).

63 J. Massot, "Santé et assurance maladie", *préc.*, p. 1002.

64 CEDH, 25 février 1997, *Z. c. Finlande*, aff. n° 22009/93, pt. 96.

65 Article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé qui modifie l'article 54 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

66 Voir sur ce point : CE, 18 novembre 1992, *LICRA*, n° 115367.

dossier à la connaissance du tribunal[67]. Plus largement, le juge administratif s'est récemment engagé dans un dialogue intense avec la CJUE en lui transmettant huit questions préjudicielles sur l'interprétation des dispositions de la directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[68].

Conclusion

La protection des données de santé est une problématique ancienne que l'essor d'Internet et des réseaux sociaux a, comme dans bien d'autres domaines, contribué à renouveler. Le régime de protection se trouve en effet déstabilisé et fragilisé par la multiplication des divulgations et transmissions, plus ou moins volontaires, de données, l'ampleur des traitements dont elles font l'objet, l'explosion des mégadonnées, et l'a-territorialité des opérateurs concernés. Le règlement européen de protection des données personnelles (RGPD) offre une première réponse aux questions soulevées, mais d'autres sont toujours en suspens dans le domaine de la santé mais aussi plus largement s'agissant de toutes les données personnelles.

Le projet de réforme de la loi du 6 janvier 1978 devrait permettre de clarifier certains aspects des questions pendantes. Il est toutefois clair que les évolutions technologiques et sociales, comme la montée en puissance des intérêts généraux ou privés autour de l'accès aux données médicales, créent une situation particulièrement instable et appellent des réglages fins qui relèvent, dans leur principe, du législateur et, pour leur mise en œuvre, de l'autorité de régulation et du juge.

Le présent colloque permettra déjà d'éclairer l'étendue et les limites de la protection qui doit être accordée aux données de santé, ainsi que l'équilibre atteint et désirable entre une stricte protection de la vie privée et une ouverture plus large dans l'intérêt de la recherche et de la santé publique : quelle doit être la juste articulation entre l'une et l'autre ?

Avant de céder la place à la première table ronde, je souhaite remercier l'ensemble des intervenants et, en particulier, les présidents des quatre tables rondes qui nous font l'honneur de leur participation : M. Didier Tabuteau, président-adjoint de la section sociale du Conseil d'État ; M. Pierre-Louis Bras, président du Conseil d'orientation des retraites ; M. François Stasse, conseiller d'État honoraire et administrateur de l'Institut national de la santé et de la recherche médicale (INSERM) et Mme Pascale Fombeur, présidente de la 1re chambre de la section du contentieux du Conseil d'État. Je remercie également le président Jean-Denis Combrexelle, président de la section sociale du Conseil d'État, qui présentera les conclusions de cette journée.

67 CE, avis, 6 avril 2007, *Douwens Prat*, n° 293238.
68 CE, Ass., 24 février 2017, *Mme Chupin et autres*, n° 391000.

Je vous souhaite de fructueux débats. Je ne suis pas sûr qu'à la fin du colloque auront été réglés les immenses problèmes qui se posent à nous, mais ils auront été davantage éclairés, évalués et pondérés. Je suis sûr, par conséquent, que leur maturation et leur résolution auront progressé.

C'est en tout cas le vœu que je forme au seuil de cette 7e édition des *Entretiens du Conseil d'État en droit social*, coproduits une nouvelle fois, et je les en remercie, par la section sociale et la section du rapport et des études du Conseil d'État.

La définition des données de santé

Le droit français ne fournit pas de définition des données de santé. L'enjeu est pourtant important dans la mesure où ces données, considérées comme sensibles au sens de la loi « informatique et libertés » du 6 janvier 1978[69], sont soumises, lorsqu'elles revêtent un caractère personnel, à un régime protecteur encadrant leur collecte et leur traitement.

La jurisprudence, notamment européenne, ainsi que les autorités administratives directement concernées retiennent une conception large des données de santé, comme englobant toute donnée relative à la santé d'une personne ou même seulement susceptible de donner une indication sur son état de santé. Cette approche extensive, qui tranche avec l'acception plus restrictive des données de santé privilégiée dans d'autres pays comme les États-Unis, a été consacrée par le règlement du Parlement européen et du Conseil du 27 avril 2016[70] qui entrera en vigueur en mai 2018.

Une telle définition présente sans doute le risque de soumettre certaines données relatives à la santé à un régime juridique inadapté, car restreignant leur accès de manière exagérée ; reste que cette approche unitaire et simplifiée de la donnée de santé, qui tient compte de la situation sanitaire globale de la personne, favorise une protection renforcée de la vie privée des intéressés.

Sommaire

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

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

Biographie des intervenants

Les fonctions mentionnées sont celles exercées à la date de la conférence

Modérateur

Didier Tabuteau
Président adjoint de la section sociale du Conseil d'État

Conseiller d'État, Didier Tabuteau est également responsable de la chaire Santé à l'Institut d'études politiques de Paris, professeur associé et codirecteur de l'Institut droit et santé à l'université Paris-Descartes (INSERM UMRS 1145), rédacteur en chef de la revue *Les tribunes de la santé* et codirecteur de la rédaction du *Journal du droit de la santé et de l'assurance maladie*. Il a été deux fois directeur du cabinet du ministre de la santé (1992-1993 et 2001-2002) et à deux reprises directeur adjoint du cabinet du ministre des affaires sociales (1988-1991 et 1997-2000). Il a dirigé l'Agence du médicament de 1993 à 1997. En 2000, il a été chargé de la préparation du projet de loi relatif aux droits des malades et à la qualité du système de santé. Il est ancien élève de l'École Polytechnique et de l'École nationale d'administration (ENA), docteur en droit et titulaire de l'habilitation à diriger des recherches. Il a publié ou coordonné différents ouvrages parmi lesquels *Droit de la santé* (avec A. Laude et B. Mathieu, PUF, 3e éd. 2012), *Traité de santé publique* (avec G. Brücker et F. Bourdillon, Flammarion, 2e éd. 2007), *Traité d'économie et de gestion de la santé* (avec P.-L. Bras et G. de Pouvourville, Sciences Po-Éd. de santé, 2009), *La judiciarisation de la santé* (avec A. Laude et J. Pariente, Éd. de santé, 2012), deux Que-sais-je ? (PUF) - *La santé publique*, avec A. Morelle (2010) et *Les assurances maladie* avec P.-L. Bras (2012) et *Démocratie sanitaire, Les nouveaux défis de la politique de santé* (éd. Odile Jacob, 2013).

Intervenants

Rémi Decout-Paolini
Rapporteur public à la section du contentieux du Conseil d'État

Rémi Decout-Paolini a commencé sa carrière au ministère de l'intérieur, avant d'effectuer sa mobilité au Conseil d'État, puis d'exercer les fonctions de conseiller juridique, chargé des libertés publiques, au cabinet du Premier ministre. Nommé maître des requêtes au Conseil d'État en 2011, il est rapporteur à la section du contentieux et à la section de l'intérieur avant d'exercer, depuis 2015, les fonctions de rapporteur public au sein de la 1re chambre de la section du contentieux. Rémi Decout-Paolini est également membre de la section du rapport et des études et professeur associé en droit à l'université de Lille.

Irina Vasiliu
Chef d'équipe unité protection des données personnelles à la direction générale de la justice et des consommateurs (DG JUST) de la Commission européenne

Irina Vasiliu est le chef d'équipe pour le Règlement général sur la protection des données (RGPD) dans le cadre de l'unité protection des données au sein de la direction générale justice et consommateurs de la Commission européenne. Elle a été l'un des principaux négociateurs du paquet protection des données (un règlement général et une directive pour les données personnelles traitées à des fins répressives) dans le Conseil et le Parlement européen. Auparavant, Irina Vasiliu a travaillé comme administrateur au sein du secrétariat de la commission libertés civiles du Parlement européen.

Jean-Pierre Mignard
Avocat au barreau de Paris, membre du Comité national consultatif d'éthique

Jean-Pierre Mignard est avocat au barreau de Paris, docteur en droit pénal de l'université Panthéon-Sorbonne (thèse sur la cybercriminalité) et maître de conférences à l'Institut d'études politiques de Paris (droit pénal des affaires, droit de la communication et des données numériques). Il est notamment spécialiste des questions de droit pénal des personnes et des affaires. Son domaine d'intervention s'étend également au droit de la presse et de la communication et des données numériques, ainsi qu'au droit européen des droits de l'homme. Il est intervenu dans des dossiers tels que le naufrage de l'Erika, l'affaire des écoutes de l'Élysée, les procès Mediapart contre l'entourage de Liliane Bettencourt. Il fut l'avocat des familles des parties civiles dans les affaires dites « de Clichy-sous-Bois » et « de Villiers-le-Bel ». Il a également siégé dans des jurys d'arbitrage. Il a assisté des États africains dans de nombreux litiges territoriaux auprès de la Cour internationale de justice (CIJ) à La Haye. Il est aujourd'hui associé-gérant de la société d'avocats Lysias Partners. Il est membre du Comité consultatif national d'éthique.

Actes – La définition des données de santé

Didier Tabuteau
Président adjoint de la section sociale du Conseil d'État,
modérateur de la table ronde

Nous avons la lourde tâche, dans cette première table ronde, d'essayer de fixer un cadre tout en abordant un certain nombre de notions dont le vice-président nous a montré à la fois la complexité, l'actualité et l'immensité. Cela sera d'autant moins simple que nos échanges s'inscrivent dans un format limité dans le temps. Nous allons pourtant essayer de poser ces problématiques de départ, afin que les trois tables rondes suivantes puissent s'appuyer sur ce qui aura été rappelé, défini et affiné au cours de cette première séance.

Pour ce faire, j'ai le plaisir et l'honneur d'accueillir à mes côtés trois intervenants qui connaissent particulièrement bien notre sujet : Mme Irina Vasiliu, chef d'équipe Règlement général sur la protection des données personnelles à la direction générale de la justice et des consommateurs de la Commission européenne, qui a beaucoup œuvré pour l'élaboration de la règlementation européenne ; maître Jean-Pierre Mignard, avocat au barreau de Paris, membre du Comité national consultatif d'éthique, spécialiste des questions de droit pénal des personnes et des affaires, qui a accepté de nous livrer son regard sur les questions de protection des données, dans un cadre à la fois européen et états-unien, pour que la comparaison puisse être la plus ouverte possible sur les enjeux internationaux de ces questions ; et enfin M. Decout-Paolini, rapporteur public à la section du contentieux du Conseil d'État et professeur associé à l'université de Lille, qui ouvrira cette table ronde par une analyse de la problématique des données de santé dans la jurisprudence, notamment du Conseil constitutionnel et du Conseil d'État.

Dans la séance d'ouverture à ce colloque, le vice-président a rappelé le cadre juridique dans lequel nous nous situons, et sa remarquable évolution depuis quelques décennies, jusqu'à la définition à la fois très précise et très large donnée par les textes européens. Cette question chemine ainsi en parallèle des politiques de santé, des règles applicables au secret médical , mais également des transformations de la société. Il a été rappelé l'impact que peut avoir l'essor d'Internet et des réseaux sociaux sur l'usage et les enjeux de la multiplication des données de santé.

Cela se traduit par une protection juridique fortement renforcée au fil du temps, à travers les législations, mais aussi les décisions de la Cour de justice de l'Union européenne (CJUE), de la Cour européenne des droits de l'homme (Cour EDH), du Conseil constitutionnel et du Conseil d'État. Mais l'élément essentiel qui, aujourd'hui, est au cœur du débat sur les données de santé, leur définition, leur champ d'application, leurs limites et leur traitement juridique et social,

tient à leur nature très évolutive en fonction des connaissances médicales et épidémiologiques, et pas seulement au développement des outils techniques qui permettent d'y accéder.

Et ce champ des données de santé concerne, non seulement, les données médicales, les données génétiques et biologiques, les données médico-administratives (hospitalisations, arrêts de travail, incapacités, etc.) – c'est-à-dire toutes les données naturellement présentes dans le champ du système de santé –, mais aussi des données beaucoup plus indifférenciées : les recherches d'information sur la santé, la consultation des sites médicaux, la commande de produits de santé, etc., qui sont des éléments indirectement révélateurs de préoccupations de santé – voire de problèmes de santé – et qui peuvent même apparaître comme des informations susceptibles de renseigner sur les déterminants de la santé. Cela signe une évolution majeure, le passage de données strictement médicales à des données sur les déterminants de la santé (activité professionnelle, lieu de vie, niveau socio-économique, pratiques sportives, etc.). Et ces données multiformes, le droit peine à les déterminer pour les placer sous un régime juridique de protection, adapté aux enjeux de leur utilisation. Le mouvement du « quantification de soi » (en anglais, « *quantified self* ») évoqué dans le discours d'ouverture est donc au cœur de cette problématique.

J'ajouterai un point supplémentaire. Ces données, très indirectes et pouvant paraître anodines, peuvent avoir, lorsqu'elles sont regroupées par un opérateur, une signification très précise pour la santé, au point de retenir l'attention d'acteurs économiques ou sociaux. Par exemple, il y a cinquante ans, la connaissance du nombre d'heures d'exposition au soleil d'une personne ne présentait aucun intérêt sur le plan sanitaire, tandis qu'aujourd'hui ces informations peuvent intéresser des assureurs ou des acteurs qui cherchent à établir des profils types.

L'enjeu qui est actuellement posé pour le droit des données de santé, et qui nous oblige à arbitrer constamment entre liberté d'utilisation et secret médical, c'est bien sûr la protection au regard de la surveillance, notamment des autorités publiques qui pourraient être tentées de faire un usage contestable de ces données, mais aussi au regard de la *négligence*, c'est-à-dire de l'appropriation de ces données, de leur utilisation, par des acteurs de la société civile plus ou moins bien intentionnés.

Si l'on ajoute à cela la dilution du secret médical que provoque une série de phénomènes, que ce soit l'expansion du champ de la santé, le développement du « tourisme médical », les logiques de vigilance sanitaire, les transferts massifs de données, etc., on mesure qu'autour de ces questions la problématique juridique est profondément renouvelée. C'est donc à la réflexion sur ce renouvellement que sont invités nos trois intervenants.

Je vais, dans un premier temps, donner la parole à M. Decout-Paolini, puis Mme Vasiliu présentera la problématique du règlement européen et, enfin, M. Mignard nous livrera ses réflexions sur cette question.

La parole est à M. Decout-Paolini.

Les données de santé ont l'apparence de l'évidence pour les personnes qui les recueillent comme pour celles qui les exploitent ou, éventuellement, les détournent.

Certains membres du public ont peut-être lu le dernier roman policier de Fred Vargas, *Quand sort la recluse*[71]. Rappelons, sans dévoiler l'énigme, que lorsque le célèbre commissaire Adamsberg est intrigué par la mort de plusieurs personnes à la suite de morsures de l'araignée *Loxosceles reclusa*, qu'on appelle usuellement la recluse, normalement inoffensive, c'est assez logiquement qu'il essaye d'obtenir, même s'il le fait frauduleusement (ce qui soulève un problème de secret médical et de protection des traitements informatiques) les comptes rendus des médecins sur ces cas de « loxoscélisme foudroyant, jamais répertorié » – pour une description savoureuse de ces comptes rendus, je renvoie les lecteurs à la page 205 du roman.

Ces informations relèvent à l'évidence de données relatives à la santé des patients, et c'est ainsi qu'elles sont présentées par le commissaire Adamsberg à son équipe. Et pourtant on constate assez curieusement, lorsqu'on examine dans le détail les questions relatives aux données de santé que, si ces dernières font bien l'objet d'un régime de protection, elles ne sont curieusement pas clairement définies, ou ne l'étaient pas clairement jusqu'à l'intervention de l'article 4 du règlement général sur la protection des données (RGPD)[72].

Je souhaiterais juste illustrer dans ces propos introductifs ce paradoxe – certes relatif, n'exagérons pas tout de même – entre la protection renforcée dont bénéficient les données de santé et l'incertitude ou le flou qui s'attache aux franges de la notion, compte tenu notamment de l'évolution de ces données et de l'évolution des techniques.

Comme le président Massot l'avait relevé dans son étude de référence « Santé et assurance maladie »[73], qui nourrit notre présentation, la loi « informatique et libertés » de 1978[74] ne mentionnait pas, curieusement, dans sa version initiale,

71 F. Vargas, *Quand sort la recluse*, éd. Flammarion, Paris, 2017.

72 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ; règlement également appelé « règlement général sur la protection des données (RGPD) ». S'agissant de l'article 4, celui-ci définit les « *données à caractère personnel* » comme « *toute information se rapportant à une personne physique identifiée ou identifiable* », sachant qu'une « personne physique identifiable » est celle « *qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* » (RGPD, article 4) ; notons que les données qui ont fait l'objet d'une « pseudonymisation » « *et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable* » (RGPD, article 4, raison 26).

73 J. Massot, « Santé et assurance maladie », *in* A. Debet, J. Massot, N. Metallinos (dir), *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, éd. Lextenso, Paris, 2015.

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

les données de santé parmi les données sensibles dont le traitement était proscrit sauf accord des intéressés.

Mais c'est assez rapidement, en réalité, que la Commission nationale de l'informatique et des libertés (CNIL) a estimé que ces données devaient faire l'objet d'une protection particulière, notamment en regard du secret médical, et elle a été confortée dans cette approche par la convention du Conseil de l'Europe du 28 janvier 1981[75] dont l'article 6 mentionne les données à caractère personnel relatives à la santé parmi celles qui ne peuvent pas être traitées sans garanties particulières.

On notera que c'est avec la transposition de la directive de 1995[76], par la loi de 2004[77], que les données de santé figurent explicitement dans la loi de 1978[78] qui en encadre le traitement.

Ces données font l'objet, à l'instar des autres données mentionnées à l'article 8 de la loi de 1978, comme les données « *qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes* », d'une protection particulière – ou renforcée – en raison de leur sensibilité.

Cette sensibilité est évidente, car la santé touche à l'intimité de la personne – on rejoint ici la notion de vie privée. Elle peut être aussi un facteur de discrimination pour, par exemple, l'accès à certains droits ou à certaines prestations comme le montrent les débats relatifs à l'accès aux prêts bancaires des personnes guéries de maladies cancéreuses, ou les examens médicaux exigés avant la souscription d'un emprunt.

En quoi consiste cette protection renforcée ? Le I de l'article 8 de la loi du 6 janvier 1978 interdit la collecte ou le traitement de ces données, mais des exceptions sont prévues par le II – et admises dès lors qu'elles sont entourées de garanties.

L'exception tient, pour « *certaines catégories de données* », à l'exigence même de la finalité du traitement – dès lors donc que la finalité est regardée comme acceptable (toutes les finalités ne le sont pas !) –, et que le recueil des données en cause répond à des exigences de nécessité et de proportionnalité. Deux alinéas concernent le domaine de la santé : le 6° et le 8°.

Le 6° du II mentionne ainsi « *les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre*

75 Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

76 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ; abrogée le 24 mai 2018 par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD).

77 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.

78 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dernière modification par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles).

d'une profession de santé, ou par une autre personne à laquelle s'impose, en raison de ses fonctions, l'obligation de secret professionnel prévue par l'article 226-13 du code pénal » ; le 8° mentionne « *les traitements nécessaires à la recherche, aux études et évaluations* [ces deux items ont été ajoutés par la loi n° 2016-41 du 26 janvier 2016] *dans le domaine de la santé selon les modalités prévues au chapitre IX* ».

La protection qui est assurée par la loi du 6 janvier 1978, et qui se traduit par l'application de règles et de formalités particulières aux traitements concernés, est la protection de référence à laquelle renvoient les articles du code de la santé publique.

On notera que l'on relève dans ledit code cinquante-cinq articles de renvoi à la loi du 6 janvier 1978 – et encore ces renvois ne concernent-ils que des dispositions dans lesquelles le numéro de la loi apparaît, ce qui n'est pas toujours le cas comme on le voit avec l'article L. 1413-6 relatif à la transmission à l'agence nationale de santé publique (ANSP) d'informations ou de données de santé.

La protection qui est assurée par la loi du 6 janvier 1978 en matière de données de santé répond bien sûr à des exigences supérieures, constitutionnelles et conventionnelles.

Le juge constitutionnel range les données de santé au nombre de celles dont la révélation porte atteinte à la vie privée et doit être entourée de garanties. C'est l'apport essentiel de la décision du 23 juillet 1999 sur la loi portant création d'une couverture maladie universelle (CMU)[79] et qui a élevé, pour la première fois, au rang de principe constitutionnel, découlant de la Déclaration des droits de l'homme et du citoyen de 1789, le respect de la vie privée.

La jurisprudence du Conseil constitutionnel a ensuite été précisée sur ce point par la décision du 21 décembre 1999 sur la loi de financement de la sécurité sociale pour 2000[80], et le Conseil y indique que la liberté proclamée par l'article 2 implique le droit au respect de la vie privée ; et ce droit requiert que soit observée une particulière vigilance dans la transmission des informations nominatives à caractère médical entre les médecins prescripteurs et les organismes de sécurité sociale. Cette jurisprudence a été réaffirmée dans les décisions ultérieures, en particulier la décision du 12 août 2004[81].

Et si, en réalité, la jurisprudence du Conseil constitutionnel n'est pas des plus fournies en la matière, c'est que plusieurs lois, qui ont institué les systèmes de collecte d'informations à des fins sanitaires, n'ont pas été soumises à son contrôle ; et lorsque le Conseil constitutionnel a été saisi il n'a pas soulevé de motifs d'inconstitutionnalité – je vous renvoie en ce sens à la loi « HPST » du 21 juillet

79 CC, décision n° 99-416 DC du 23 juillet 1999, *loi portant création d'une couverture maladie universelle*.
80 CC, décision n° 99-422 DC du 21 décembre 1999, *loi de financement de la sécurité sociale pour 2000*.
81 CC, décision n° 2004-504 DC du 12 août 2004, *loi relative à l'assurance maladie, dite « Douste-Blazy »*.

2009[82] (CC, décision n° 2009-584 DC du 16 juillet 2009) réformant les systèmes d'information de la veille sanitaire et de la toxicovigilance (article 106), et à la loi du 26 janvier 2016[83] (CC, décision n° 2015-727 DC du 21 janvier 2016) organisant la mise à disposition des données de santé (article 193) et réformant à nouveau la toxicovigilance (article 171).

C'est également au titre du respect de la vie privée, garantie à l'article 8 de la Convention EDH, que la Cour EDH a eu l'occasion de se prononcer sur les données de santé. Au début, la Cour a été amenée à le faire à l'occasion d'affaires qui ne traitaient que de la seule divulgation des données de santé, s'agissant en particulier du champ resserré de la divulgation du secret médical, comme par exemple en 1997 dans l'affaire *Z contre Finlande*[84], dans laquelle la Cour EDH indique que le respect du caractère confidentiel des « informations » sur la santé constitue un principe essentiel soulignant qu'« *il est capital, non seulement pour protéger la vie privée des malades, mais également pour préserver leur confiance dans le corps médical et les services de santé en général* »[85]. L'affaire était particulière, et la Cour EDH a jugé au cas d'espèce que seule la divulgation de l'identité et de l'état de santé de la requérante avaient posé un problème. En 2008, dans une autre affaire, *I. contre Finlande*[86], la Cour constate une violation, cette fois de l'article 8 de la Convention EDH, parce que le dossier médical d'une infirmière, soignée contre le sida dans un hôpital, n'avait pas été mis à l'abri du regard de ses collègues. Notons que plusieurs arrêts concernent également la question de l'utilisation – notamment dans les procédures de divorce – des données de santé du conjoint[87].

Il est important de relever ici que la Cour EDH est de plus en plus saisie de litiges portant, non pas sur la divulgation des données, mais sur la manière dont ces données sont maintenant collectées. À cet égard, un arrêt *Worwa contre Pologne* de 2003[88] juge que la répétition, à bref délais, d'expertises médicales sur l'état mental d'un prévenu est contraire au droit au respect de la vie privée.

Notons que l'on trouve une bonne synthèse de la position de la Cour EDH en matière de protection des données dans son arrêt de Grande chambre du 4 décembre 2008, *S. et Marper contre Royaume-Uni*[89], où elle indique que le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 de la Convention EDH, mais que pour l'appréciation sur une éventuelle violation celle-ci doit tenir compte du contexte particulier dans lequel les informations sont recueillies et conservées, de la manière dont elles sont utilisées et traitées, et des résultats qui peuvent en être tirés. On retrouve là des principes qui sont aussi mis en œuvre par la jurisprudence de l'Union européenne[90].

82 Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.
83 Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.
84 CEDH, 25 février 1997, *Z c. Finlande*, n° 22009/93.
85 *Ibid*., point 95.
86 CEDH, 17 juillet 2008, *I. c. Finlande*, n° 20511/03.
87 Voir par exemple : CEDH, 10 octobre 2006, *L.L. c. France*, n° 7508/02.
88 CEDH, 27 novembre 2003, *Worwa c. Pologne*, n° 26624/94.
89 CEDH, Gde ch., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, n°s 30562/04 et 30566/047.
90 CJCE, 20 mai 2003, *Rechnungshof (C-465/00) c. Österreichischer Rundfunk et autres* et *Christa Neukomm (C-138/01) et Joseph Lauermann (C-139/01) c. Österreichischer Rundfunk*.

On en arrive alors au paradoxe suivant, qui consiste à assurer un niveau élevé de protection des données, mais dans un champ qui, en réalité, n'est pas établi avec certitude. La notion de « données » apparaît en effet comme une notion au contour incertain.

Ce qui frappe, d'abord, c'est le caractère fluctuant des terminologies dans les textes comme dans les décisions qui traitent de cette question : « *données de santé à caractère personnel* » (article L. 1111-8 du code de la santé publique relatif aux principes généraux en matière d'information des usagers du système de santé) ; « *données relatives à la santé* » (article 8 de la loi n° 78-17 du 6 janvier 1978), formulation que l'on retrouve habituellement dans les délibérations de la CNIL, mais explicitée sous la forme « *données relatives à la santé des personnes concernées* »[91]. On trouve aussi des rédactions déployées et plus englobantes : « *informations et données issues de l'observation et de la surveillance de la santé des populations* » (article L. 1413-6 du code de la santé publique relatif à la mise à disposition de ces informations et données par l'Agence nationale de santé publique) ; ou « *données médicales* » dans les tables de la jurisprudence du Conseil constitutionnel[92].

Il n'y a sans doute pas d'indétermination de la notion de *données*, mais un certain flou.

Pas d'indétermination, car l'on constate que les « données de santé » se composent d'un noyau dur comprenant, notamment, des données relatives aux examens et aux diagnostics médicaux, aux antécédents médicaux, au parcours de soin du patient, et de façon générale à tous les éléments relatifs à la prise en charge médicale. Et les actes comme les délibérations de la CNIL éclairent usuellement cette notion de données de santé – comme par exemple la délibération citée précédemment du 13 juillet 2017[93] où la catégorie relative aux données de santé est explicitée par trois sous-catégories extrêmement précises.

Il existe, cependant, un certain flou sur les franges de la notion, qui se comprend sans doute au regard de l'évolution des nouvelles technologies et de la survenance d'enjeux liés, par exemple, aux objets connectés – au nombre desquels certains dispositifs médicaux. On trouve une illustration de cette incertitude dans le besoin exprimé par les pouvoirs publics de lancer, en 2015, une réflexion sur les usages souhaités des données massives dans le domaine de la santé[94] : l'une des premières interrogations portait précisément sur la « délimitation des données de santé », afin de délimiter leur champ dans le contexte actuel[95].

91 CNIL, délibération n° 2017-215 du 13 juillet 2017 portant adoption d'une norme destinée à simplifier l'obligation de déclaration des traitements de données à caractère personnel ayant pour finalité le dépistage organisé du cancer du sein, du cancer colorectal et du cancer du col de l'utérus mis en œuvre par les structures de gestion conventionnées (…), article 3.

92 CC, décision n° 2011-640 DC du 4 août 2011, *loi modifiant certaines dispositions 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*.

93 CNIL, délibération n° 2017-215 du 13 juillet 2017, *préc.*, article 3.

94 Voir la déclaration de la ministre des affaires sociales, de la santé et des droits des femmes, sur les aspects juridiques et éthiques du « *big data* » en santé et les usages des données de santé, Paris, 10 septembre 2015.

95 Voir *Big Data en santé. Quels usages ? Quelles solutions ?*, résultat des travaux du groupe de réflexion sur les données massives en santé, ministère des affaires sociales et de la santé, 4 juillet 2016.

Le juge administratif a été amené à clarifier de son côté certains aspects de la notion de « données de santé ».

Le juge administratif a notamment tranché une question, née de la rédaction utilisée pour le I. de l'article 8 de la loi n° 78-17 du 6 janvier 1978, considérant qu'il fallait prendre en compte la notion relative à la santé comme une donnée qui révèle, même indirectement, l'état de santé d'une personne.

Dans une décision de 2010 relative à un fichier de l'éducation nationale[96], le juge administratif a indiqué que doit être regardée comme une donnée personnelle relative à la santé la mention d'une classe d'intégration scolaire (CLIS) ; dans une autre décision, également de 2010[97], le juge a précisé que « *la mention d'un code de référence des établissements de soins, si elle permet de savoir que l'élève a été souffrant, ne fournit par elle-même aucune information sur la nature, la durée, ou la gravité de l'affection de l'élève* »[98]. Enfin, dans une affaire de 2014[99], le Conseil d'État a précisé que « *la mention du taux d'incapacité permanente ou du taux d'invalidité du conjoint ou partenaire et des personnes à la charge de l'agent n'est pas une donnée relative à la santé au sens des dispositions précitées de l'article 8 de la loi du 6 janvier 1978* »[100] ; et l'on voit bien que cette jurisprudence, au regard notamment de ce qu'indique le règlement général sur la protection des données, pourrait éventuellement évoluer.

Nous avons, en effet, dans la jurisprudence de la Cour de justice de l'Union européenne, une acception de la notion de « données relatives à la santé » apparemment plus large que celle donnée par la jurisprudence du Conseil d'État, comme le montre notamment l'affaire *Lindqvist*[101] qui indique que cette notion comprend « *des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne* »[102].

L'on retrouve également cette notion plus large dans la position qui a été exprimée par le groupe de travail des CNIL européennes (G29)[103], notamment dans un courrier de 2015[104] en réponse à une demande de la Commission européenne[105].

96 CE, ssr, 19 juillet 2010, n° 317182.
97 CE, ssr, 19 juillet 2010, n° 334014.
98 *Ibid*., considérant 10.
99 CE, ssr, 28 mars 2014, *SIRHEN*, n° 361042.
100 *Ibid*., considérant 15.
101 CJCE, 6 novembre 2003, *Bodil Lindqvist*, aff. C-101/01.
102 *Ibid*., point 50 : « *il convient de donner à l'expression « données relatives à la santé » employée à son article 8, paragraphe 1* [de la directive 95/46]*, une interprétation large de sorte qu'elle comprenne des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne* ».
103 Le 25 mai 2018, le G29 a disparu pour laisser place au Comité européen de protection des données, créé par l'article 68 du RGPD.
104 Voir lettre du 5 février 2015 de l'Article 29 Data Protection Working Party à Paul Timmers [05/02/2015 Letter from the ART 29 WP to the European Commission, DG CONNECT on mHealth]. Voir également : Press release European Commission : *mHealth in Europe : Preparing the ground* – consultation results published, 12 January 2015 (site Internet : https://ec.europa.eu/digital-agenda/en/news/mhealth-europe-preparing-ground-consultation-results-published-today).
105 Cette demande intervient à la suite de plusieurs travaux de la Commission européenne relatifs à la « santé mobile ». Voir *Livre Vert sur la santé mobile*, 10 avril 2014, COM (2014) 219 final ; ainsi que le document de travail des services de la Commission sur le cadre juridique existant de l'Union européenne applicable aux applications « mode de vie et bien-être ».

Ce qui montre bien que l'on est toujours avec cet enjeu constant et renouvelé, de définition et de délimitation de la notion même de données, aux franges de cette donnée. Et le G29 a considéré que des données telles que l'obésité, la tension, les prédispositions génétiques, ou encore la consommation excessive d'alcool ou l'usage de drogues sont des données relatives à la santé car elles permettent, au vu des connaissances scientifiques, d'établir des facteurs de risque dans le développement de nombreuses maladies. Et l'on voit bien ici comment la notion de *données massives* va renforcer encore cette appréciation relativement large.

Ce qui nous conduit donc tout naturellement à la définition à laquelle s'est essayé le règlement général sur la protection des données (RGPD) de 2016 au regard de son considérant 35[106] et de son article 4 (Définitions).

Didier Tabuteau
Président adjoint de la section sociale du Conseil d'État,
modérateur de la table ronde

Merci pour cette présentation synthétique d'un champ jurisprudentiel très large. Je donne la parole à Mme Vasiliu pour évoquer la question du règlement européen.

Irina Vasiliu
Chef d'équipe unité protection des données personnelles à la direction générale de la justice et des consommateurs (DG JUST) de la Commission européenne

Merci M. le président. Je vous propose une intervention en deux parties. La première partie sera consacrée à la substance du règlement général sur la protection des données (RGPD)[107], tandis que la seconde partie sera dévolue à l'explication du travail de la Commission européenne depuis l'adoption de ce règlement en 2016 jusqu'à ce jour, voire au-delà puisque ce travail n'est pas achevé.

Pour ce faire, je vais partir des mots du vice-président Sauvé qui rappelait combien l'instabilité créée par ces évolutions technologiques et sociales « *appelle des réglages fins* **»** – justement, le règlement général sur la protection des données prévoit de tels réglages.

106 « *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* [du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers] *au bénéfice de cette personne physique ; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques ; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro* », RGPD, cons. 35.

107 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, *préc*.

Ce règlement adresse en effet plusieurs objectifs essentiels en même temps : il offre une protection élevée des données personnelles, il assure une liberté (encadrée) aux opérateurs, il donne plus de sécurité juridique, il sauvegarde l'intérêt public et, enfin, il assure une libre circulation des données dans l'Union européenne.

Du fait de son caractère général, le RGPD donne ainsi des règles à la fois au secteur public et au secteur privé, dans une diversité de domaines qui vont du secteur de la santé au secteur financier et se prolongent avec le traitement des données au sein des organismes de ces secteurs (écoles, entreprises, etc.).

Ce règlement est aussi une expression de « proportionnalité ». Si l'on prend l'exemple du traitement des données à grande échelle, celui-ci doit avoir une justification, une légalité et une finalité précises à la hauteur de l'intrusion encourue dans les droits des personnes concernées.

Par ailleurs, le RGPD a été mis en place pour un certain nombre de raisons supplémentaires : nécessité de gérer la fragmentation des approches observées dans l'Union européenne durant les vingt années d'application de la directive 95/46/CE, de faire face à la mondialisation, d'offrir davantage de sécurité juridique aux opérateurs et, surtout, de renforcer les droits des utilisateurs.

En ce sens, le RGPD est plus une évolution qu'une révolution. En effet, si l'on analyse les concepts clés qui président à ces évolutions (par exemple, données à caractère personnel, responsable du traitement, sous-traitant, etc.)[108], ceux-ci demeurent les mêmes ainsi que les principes qui les sous-tendent (finalité, proportionnalité, traitement ultérieur incompatible).

Ce qui est important, ici, c'est que ces concepts sont clarifiés. Dans la directive 95/46/CE, il existait huit définitions contre vingt-six dans le RGPD. Parmi ces définitions, certaines sont particulièrement importantes.

Le concept de « données à caractère personnel ».

Ce concept va bien au-delà des données de santé. L'approche de la directive 95/46/CE ainsi que celle du RGPD est de concevoir une définition suffisamment large, évolutive et, surtout, en lien avec la réalité pour bien prendre en compte le fait que les données à caractère personnel sont des données qui identifient directement ou indirectement une personne par tout moyen (numéro d'identification, élément de géolocalisation, etc.). Car il faut être conscient qu'aujourd'hui de plus en plus de données sont ou deviennent des données personnelles.

Bien sûr – et c'est là l'aspect « raisonnable » du RGPD –, pour identifier directement ou indirectement une personne, on doit garder à l'esprit que cela nécessite de la part des responsables du traitement des moyens technologiques parfois importants ou de fortes ressources pour identifier la personne derrière une adresse IP[109].

Quel est le champ où le droit de la protection des données ne s'applique pas ?

108 Voir RGPD, article 4 (Définitions).

109 L'adresse IP (« *Internet protocol* ») est l'identifiant de l'ordinateur connecté à Internet, ou à un réseau local.

Le droit ne s'applique pas au moment où cette donnée est ou devient anonyme.

Ce qui est important pour le « responsable du traitement » des données c'est de faire preuve, dans son travail, des vérifications ou des contrôles nécessaires (« *due diligence* ») pour que ledit traitement ne porte pas préjudices à des tiers, mais également d'analyser ce traitement en se projetant à moyen terme, afin de se demander si une donnée aujourd'hui anonyme le restera dans les années à venir.

Le concept de « pseudonymisation » – la donnée reste toujours une donnée personnelle, mais le traitement met de côté certaines informations de manière à ce que l'on ne puisse pas identifier la personne sans des informations supplémentaires – est certes réversible, mais à condition de disposer de moyens techniques.

Les trois nouvelles définitions du RGPD.

Ces trois nouvelles définitions sont bâties par la jurisprudence de la Cour de justice de l'Union européenne (CJUE) et de la Cour EDH, ainsi que par le travail essentiel des autorités européennes de protection des données réunies au sein du groupe de l'article 29 (G29).

Les données de santé sont définies comme des données relatives à la santé physique ou mentale d'une personne, y compris la prestation de services de soins de santé. Sont également concernés par cette définition les objets connectés. Dans ce contexte, il convient de s'interroger sur les conséquences de ces nouveaux outils sur les individus. Notons également qu'en 2015 le G29 avait précisé que toute information bonne ou mauvaise sur l'état de santé d'une personne devait être qualifiée de « donnée de santé personnelle »[110].

Par-delà le concept, déjà ancien, de données de santé, il doit être noté que le RGPD introduit les concepts de « *données génétiques* » (considérant 34) et de « *données biométriques* » (considérant 51). Toutes ces données sont des données dites « sensibles » dont il est interdit, par principe, de faire usage. Cependant, il existe dans le RGPD un nombre important de dispositions qui en permettent le traitement en toute licéité, loyauté et transparence. Par exemple, les données de santé peuvent être traitées avec le consentement explicite d'une personne.

Ce qui est essentiel ici, et ce dont on manque peut-être dans certains de nos États membres, c'est le fait que ce consentement est un *acte positif clair*. Trop souvent en effet le silence vaut consentement. À partir du 25 mai 2018, le RGPD ne permet(tra) plus ce genre de situation.

On notera que non seulement le consentement explicite d'un individu peut permettre le traitement des données de santé, mais encore que la loi peut également le faire : loi en matière de santé, mais aussi en matière d'emploi, de sécurité sociale, etc. L'essentiel étant que soit prévue dans la loi une mention claire par le législateur européen ou national du motif d'intérêt général permettant le traitement des données de santé.

110 Voir les travaux du G29 sur https://ec.europa.eu/newsroom/article29/news-overview.cfm

Bien sûr, dans toutes ces situations, des garanties appropriées doivent exister dans les lois faisant état de ces traitements spécifiques des données.

Autre nouveauté du RGPD : la clarification que les données sensibles, y compris celles de santé, peuvent être traitées pour de l'archivage dans l'intérêt public ou à des fins de recherche scientifique sur la base d'une loi nationale ou européenne qui prévoit aussi les garanties appropriées. Cela est important, car de telles considérations ouvrent un nouveau champ en matière de traitement des données de santé dans le domaine de la recherche.

Avant de préciser le sujet des règles de recherche, je voudrais évoquer un autre élément qui est explicité dans le RGPD.

Les États membres peuvent maintenir ou introduire plusieurs conditions, ou restrictions au traitement des données de santé, des données génétiques ou des données biométriques. Concrètement, nous avons à ce jour deux États membres qui ont indiqué à la Commission vouloir interdire le traitement des données génétiques à des fins d'assurance.

Dans l'exercice de cette liberté, l'État membre doit veiller à ne pas entraver la libre circulation des données dans l'Union européenne ; d'autant que la recherche et le traitement des données sont de plus en plus transfrontaliers.

D'autre part, je souhaiterais préciser certains éléments au sujet des règles spécifiques en matière de recherche, car aujourd'hui les données de santé sont très utiles et utilisées dans le domaine de la recherche.

Le RGPD contient un régime favorable pour les traitements d'archivage ayant un intérêt public et pour les traitements ayant trait à la recherche scientifique. Il s'agit d'un traitement ultérieur, présumé compatible par le législateur, qui ne fonctionne que sur la même base légale que le traitement initial (contrat, « balance d'intérêt », intérêts vitaux d'une personne). Par ailleurs, les données personnelles traitées à des fins d'archivage ayant un intérêt public et de recherche scientifique peuvent être conservées pour une durée plus longue.

Que signifie un « consentement large » en matière de recherche sur les données de santé ?

Si je prends l'exemple des maladies génétiques rares, un chercheur, au début de sa recherche, ne peut pas identifier exactement les différents types de maladies rares qu'il est en train de chercher. De ce fait, le législateur, tout en encadrant cette permission, permet, quand il s'agit de recherche, que ce consentement soit donné pour des domaines de recherche et non pas pour une seule finalité. Enfin, ce consentement doit bien évidemment être conforme à toutes les règles du RGPD ainsi qu'aux règles éthiques.

Quelques mots sur les droits des personnes et les obligations des responsables du traitement.

En matière de *droits*, tous les droits applicables aux personnes (droit à l'information, etc.) doivent être également appliqués en matière de données de santé. Par ailleurs, les personnes dont les données de santé sont utilisées peuvent voir leurs droits restreints par le législateur national ou européen pour des raisons d'intérêt public.

Au niveau des *obligations* des responsables du traitement, on passe d'un système de notification – d'autorisation de la CNIL – à un système de *responsabilité du traitement* où il y aura, entre autres, un délégué à la protection des données pour le traitement des données de santé à grande échelle. Ce faisant, il y aura besoin d'études d'impact qui seront faites pour le traitement des données de santé à grande échelle, ainsi que de mesures de sécurité qui devront être imposées. Tout traitement avec ses mesures afférentes doit être calibré en fonction du risque qu'il pose pour les droits et les libertés des personnes.

In fine, les pouvoirs de la CNIL et de toutes nos autorités sont harmonisés ; quant aux amendes, celles-ci peuvent atteindre 4 % du chiffre d'affaires des entreprises.

En conclusion, on notera, s'agissant du travail de la Commission, que celui-ci est engagé, depuis ces deux dernières années, sur trois niveaux :

- au niveau des États membres : quand un règlement entre en application, comme par exemple le règlement européen sur la protection des données personnelles, il s'agit de voir quelle loi nationale modifier ou abroger. Le travail des États membres est donc de faire cette analyse ;

- au niveau du groupe 29 (G29) qui élabore des lignes directrices sur des concepts clés du règlement (profilage, consentement, etc.) ;

- au niveau des entrepreneurs et de la société civile pour comprendre quels sont aussi ces « réglages fins » que l'on doit encore apporter sur le terrain.

Didier Tabuteau
Président adjoint de la section sociale du Conseil d'État,
modérateur de la table ronde

Merci Mme Vasiliu pour cette prouesse d'avoir présenté en si peu de temps un règlement si difficile à lire. Je donne maintenant la parole à maître Mignard pour qu'il nous livre ses réflexions sur ce règlement général sur la protection des données (RGPD) et le mette en perspective avec d'autres législations, notamment avec le « bouclier de confidentialité » (en anglais, « *privacy shield* »)[111] qui, tant aux États-Unis qu'en Europe, suscite bien des débats.

111 Accord commercial négocié entre les États-Unis et l'Union européenne et destiné à assurer la protection des données personnelles à l'échelle mondiale. Cet accord est entré en vigueur en 2016. Il a été élaboré pour remplacer la décision *Safe Harbor* 2000/520/EC invalidée par la Cour de justice de l'Union européenne le 6 octobre 2015.

Jean-Pierre Mignard
Avocat au barreau de Paris, membre du Comité national consultatif d'éthique

Merci M. le président. Je viens surtout vous dire où nous en sommes au Comité consultatif national d'éthique (CCNE)[112] sur cette question des données de santé au regard, bien sûr, de la notion d'éthique.

Je ne vais pas revenir sur le RGPD[113] qui a été admirablement présenté par les intervenants précédents qui sont rentrés avec hardiesse et méthode dans ses méandres. Et je dois dire que la première impression que nous avons eue au CCNE, où *a priori* nous ne faisons pas du droit, mais où l'éthique côtoie sans cesse le droit, c'est d'admirer une construction humaine qui peut, quoique s'apparentant parfois sur le plan linguistique à la finesse d'un complexe pétrochimique, réussir à offrir un repère de droit inestimable aux populations des vingt-sept États de l'Union européenne.

Nous avons, en France, une excellente loi en matière de santé[114], dont la définition en termes de données me semble parfaite – ce qui montre l'avance du législateur français dans ce domaine. L'article L. 1461-2 de cette loi précise en effet que les données de santé « *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* ». Ceci, afin que les potentialités des données soient utilisées au mieux dans l'intérêt de la collectivité. Nous avons donc là un texte bien équilibré, que nous pourrions sans crainte, sur ce point précis, qualifier de « modèle ».

Cette loi aurait pu nous suffire, mais nous ne sommes pas limités par nos frontières. C'est pourquoi nous sommes amenés à travailler dorénavant dans le cadre d'un règlement européen (le RGPD) qui constitue à lui seul une véritable entreprise d'harmonisation, même si celle-ci est parfois déconcertante par son architecture exubérante.

Je suis même convaincu – et je le dis à l'attention de ceux qui s'imaginent que par rapport aux géants du numérique nous serions bien faibles – que ce règlement européen, si l'on veut bien le concevoir, dote l'Union européenne d'une d'influence considérable sur le reste du monde.

Certes, nous n'avons pas d'industrie comparable aux GAFAM dans le domaine du numérique, mais nous avons, à travers l'extraordinaire bassin d'internautes que représentent les utilisateurs européens des vingt-sept États membres et la richesse des données produites par ces mêmes internautes, une puissance considérable

112 Le Comité consultatif national d'éthique (CCNE) est une institution indépendante fondée en 1983 qui « *a pour mission de donner des avis sur les problèmes éthiques et les questions de société soulevés par les progrès de la connaissance dans les domaines de la biologie, de la médecine et de la santé* » (loi n° 2004-800 du 6 août 2004 relative à la bioéthique).

113 Le règlement général sur la protection des données (RGPD) est entré en vigueur dans les États de l'Union européenne le 25 mai 2018.

114 Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

sur l'organisation du marché, qui peut influencer voire diriger, en matière de collecte et de traitement des données, les choix des grandes sociétés américaines du numérique. L'Europe est donc présente dans le monde et dans la « civilisation des données » par cette architecture règlementaire, qui s'efforce de donner et de faire partager une définition générique de la santé, et qui semble être parvenue à franchir la première étape.

Nous avons, dans la loi française, décrit un processus par l'usage des statistiques et des agrégations de données, et, dans le RGPD, instauré des normes qui entendent fixer un périmètre à tous les États membres de l'Union européenne afin que les législateurs nationaux puissent adapter et harmoniser leurs législations et ainsi promouvoir les quatre libertés garanties par le marché unique (libre circulation des biens, des capitaux, des services et des personnes) avec la protection des personnes, c'est-à-dire puissent concilier droits fondamentaux et dignité humaine. Il faut donc établir ici un équilibre entre ces deux aspects majeurs et antagoniques s'ils ne sont pas harmonisés, à savoir la *liberté* et la *protection*, qui caractérisent les sociétés démocratiques de l'Union européenne.

Si les législations nationales existent et sont (parfois) très sophistiquées, elles devront s'harmoniser. C'est pourquoi le *consentement* de l'internaute, fournisseur de données à tout traitement, est le pilier du RGPD. Il s'agit de la portée considérable, presque téléologique, de ce règlement. Encore faut-il que ce consentement soit, selon la règle classique du droit civil, « *libre et éclairé* ». Libre, on peut supposer qu'il le sera, mais sera-t-il éclairé ? Que vaudrait en effet un consentement qui ne serait pas éclairé ? Et que vaudrait une volonté qui ne serait pas autonome au point qu'elle exercerait un pouvoir tout d'apparence dans un monde qu'elle ne connaîtrait pas ?

Le groupe de travail *Éthique et données massives* du CCNE au cours de la rédaction de son rapport au comité plénier[115] se pose les questions suivantes : comment peut-on être éclairé, notamment en matière de données de santé ? Comment peut-on savoir ce que l'on vous prend, et l'usage que l'on s'apprête à en faire ? Nous sommes, dans ce domaine, dans un cadre différent qui n'est plus le cadre déductif auquel nous étions habitués, mais un cadre inductif. Nous ne sommes plus seulement confrontés aux bases de données antérieures, sorte de « silos » ou de « lacs » composés de données massives enregistrées dans un cadre bien défini, mais à des données *tellement* massives, prises tous azimuts, que les entreprises les prélèvent indistinctement pour les « travailler » afin d'en tirer un maximum de profit, à l'instar du chercheur d'or tamisant la boue de la rivière pour récolter ses pépites.

Quelles sont ou seront ces données ? Qui sera le « chercheur d'or » ? De quel or s'agira-t-il ? Et en fera-t-il de l'or ou du vil métal en rupture avec nos principes de droit ?

115 Le travail au sein du CCNE se répartit entre le comité plénier, la section technique et les groupes de travail. Les séances des deux premières instances ne sont pas publiques.

Dans un vieux pays de droit comme la France nous sommes toujours un peu inquiets, car nous souhaitons apprécier en quoi un progrès peut choquer ou attenter à l'équilibre du droit. Le CCNE a beaucoup travaillé sur ces questions avec de nombreux praticiens et chercheurs. Que permettent les données massives ?

Dans un contexte de création de très grandes banques de données, par exemple sur la recherche génomique, les conséquences sont considérables et surtout utiles : création d'indicateurs et de bio-marqueurs en matière de diagnostics, amélioration de l'efficacité des traitements, prédiction des facteurs de risques (par exemple, les corrélations cliniques, les données génomiques ou comment prévenir à partir du génome l'émergence de certaines maladies), aide à la décision – nous sentons bien sur ce point l'existence de progrès majeurs en termes de cancérologie et d'interprétation d'imagerie –, étude des maladies rares, développement des médicaments en matière de recherche pharmacologique (nouveaux médicaments, pharmacovigilance), etc. Tout ceci présente un intérêt épidémiologique évident et offre une qualité de prise en charge et d'impact des traitements. Voilà ce que nous pouvons espérer des données de santé qui, d'ailleurs, produisent déjà ce type de résultats.

Les données de santé et leur traitement apparaissent ainsi comme des biens majeurs. Il convient alors de partir du progrès – et non pas de l'inquiétude –, et voir où celui-ci pourrait nous entraîner s'il n'était pas constamment rivé à nos principes de droit et à l'intérêt général, c'est-à-dire aux finalité du traitement des données.

C'est pourquoi le CCNE, en réponse à une saisine effectuée par la ministre de la santé et des affaires sociales en date du 25 janvier 2017, mène une réflexion en cours sur les questions éthiques qui peuvent se poser pour les chercheurs, la médecine, les producteurs et les utilisateurs de données[116].

D'abord, il s'agit de reconnaître que les données sont liées à des personnes et que le risque existe de leur nuire, même si certaines données sont catégorisées comme « publiques » – le domaine public n'étant pas, en soi, un label de protection *erga omnes* et pour toujours. Ensuite, il faut prendre conscience de l'importance de la notion de *traçabilité* des données. La définition de la notion de vie privée peut être différente pour le chercheur et pour la personne dont on traite les données – par exemple, dans le domaine génétique. Il est également nécessaire d'engager une réflexion de ce qui sera fait en aval avec les résultats de la recherche, et notamment la possible réutilisation nuisible des résultats – ce que nous constatons parfois en matière de génétique ou de discrimination. En outre, le chercheur peut travailler en collaboration avec des partenaires internationaux – et là nous sortons de l'Union européenne – dont les principes éthiques peuvent être différemment définis, avec des standards moins exigeants, et donc se heurter à une sorte de « moins disant éthique ».

Dans ce contexte, l'algorithme est au cœur du système, et les chercheurs et les mathématiciens en sont les principaux acteurs. Or si les chercheurs, les scientifiques, les médecins et les mathématiciens sont acteurs, trouveront-ils dans le RGPD et

116 Comité consultatif national d'éthique, *Données massives et santé : une nouvelle approche des enjeux éthiques*, avis 130, rendu public le 29 mai 2019.

dans les lois nationales des réponses à leurs questions ? Indéniablement, oui. Trouveront-ils toutes les réponses qu'un chercheur peut se poser au fur et à mesure que ses recherches avancent ? Sans doute pas. D'où l'importance du rôle du CCNE qui, bien sûr, ne va pas interdire au chercheur d'interrompre ses recherches – il n'en a pas la compétence –, mais va l'aider à en dissiper les incertitudes et à mieux en maitriser les finalités. Parce que souvent les chercheurs devront, comme les mathématiciens, de manière collégiale, se doter d'un cadre éthique pour échanger, élucider leurs recherches et ce qu'il est possible ou non de faire, là où peut-être des violations du droit des données personnelles pourraient se produire en raison des mailles trop larges du filet de la loi ou du règlement.

Le RGPD reste un texte plein d'intelligence, pour peu que l'on consente à dépasser son côté « obscur ». Ainsi, outre le périmètre institutionnel auquel nous sommes attachés ou habitués, il va falloir accepter de voyager à l'intérieur de cette « cathédrale », avec des procédures de compréhension du texte qui relèvent plutôt de la *Common Law* – ce qui transparaît notamment à travers les mots utilisés : « certifications », « codes de conduite », « normes éthiques » y compris celles des responsables du traitement, « autorités de contrôle » dont la CNIL, puis une sorte de sommet régulier des autorités de contrôle, puis ensuite un « comité européen de la protection des données » spécialement dédié à examiner les avis des autorités de contrôle, et même *in fine* tout en haut de cette pyramide la Commission européenne. Cela explique l'usage du mot « cathédrale », à la différence près que cet empilement baroque ressemble plus à la *Sagrada familia*[117] de Barcelone qu'à Notre-Dame de Paris. Mais le baroque figure parmi les plus grands courants artistiques, les plus impressionnants aussi…

On est donc là en présence d'un système ingénieux, mais qui ne pourra vivre que si les acteurs (chercheurs, scientifiques, médecins, mathématiciens) lui ajoutent un usage éthique. Cela est tout à fait essentiel, car les mailles d'un filet législatif ou règlementaire, fût-il de la meilleure confection, sont toujours trop larges. Et il faudra d'ailleurs que le législateur européen et les législateurs nationaux sachent vivre avec l'apprentissage éthique du texte, car le RGPD n'a pas uniquement pour fonction de permettre la libre circulation des données et leur utilisation afin qu'elles puissent produire tout ce qu'elles peuvent pour améliorer notre santé. Il va aussi falloir qu'un système de protection des données des personnes soit mis en place et qu'il soit suffisamment clair pour être effectif.

Ce règlement est ambitieux, car avec un tel bassin d'internautes en Europe les données collectées vont forcément voyager, notamment *via* l'opérateur de traitement, puis son sous-traitant, ainsi que d'autres sous-traitants à des niveaux inférieurs. Ce qui signifie que des données seront dispersées aux quatre coins du monde. Il faut donc trouver une solution pour régler les litiges susceptibles de se poser – et ils seront nombreux – entre fournisseurs de données, entre responsables de traitement et sous-traitants, notamment sur la protection des données de santé qui constitue l'un des dispositifs majeurs du règlement.

117 Célèbre basilique conçue par l'architecte espagnol Antoni Gaudi (1852-1926).

Dans ce contexte, et selon la personne saisie, ce méta-régulateur peut très bien être un juge péruvien, thaïlandais ou californien. Mais en vertu de quel droit devra-t-il statuer ? Le droit qui s'appliquera sera le droit du lieu du litige. À moins qu'avec ce système d'autres États ne trouvent des formes d'harmonisation. Les États-Unis s'y sont essayés, mais cela n'a été adopté que par quelques États fédérés, les plus proactifs dans la problématique des droits de la personne. De sorte qu'il est à craindre que nous n'ayons pas de système d'harmonisation – nous l'avons bien vu avec l'écroulement du « *Safe Harbour* » après les révélations de M. Snowden, ainsi qu'avec le « *Privacy Shield* » aujourd'hui déjà obsolète au regard du contenu du RGPD.

Le règlement a toutefois prévu une protection particulière et majeure des données primaires dans le domaine de la santé, précisément afin de soustraire leur collecte et leur traitement à l'inconnu du consentement. Ainsi, l'article 9 (*Traitement portant sur des catégories particulières de données à caractère personnel*) interdit le traitement des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques ou religieuses, philosophiques ou les appartenances syndicales, le traitement des données génétiques ou biométriques, ou encore la santé et l'orientation sexuelle de toute personne physique.

Ces dispositions limitatives souffrent cependant des exceptions aux articles 2 (*Champ d'application matériel*) et 3 (*Champ d'application territorial*), ainsi qu'au travers de l'article 9, précité, lorsque les données sont traitées à des fins de médecine préventive ou du travail, de diagnostics médicaux, de gestion des systèmes et des services de soins de santé ou de protection sociale sur la base des droits de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé. On retrouve également de telles exceptions si le traitement s'avère nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, en cas de menaces transfrontalières graves pesant sur la santé, ou dans le but de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments.

Ces exceptions relèvent à la fois de l'autorisation règlementaire et de la loi de tout État membre, qui se doit de garantir les mesures aptes à la sauvegarde des droits et des libertés de la personne concernée, notamment le secret professionnel. L'éthique du professionnel devient alors essentielle ; les données de santé échappant ainsi à la pure liberté du consentement. *Bien public* et *bien personnel intime*, donc bien doublement précieux, les données de santé obéissent à un régime d'exception – qui peut encore être limité ou se voir ajouter des conditions supplémentaires – d'autant plus strict qu'il déroge lui-même à un régime d'interdiction plus général. Les données de santé sont, en quelque sorte, amarrées à un port d'attache et ne peuvent pas prendre le large sans contrôle ni vérification de navigation, le tout sécurisé et garanti.

Nous allons donc bien avoir un droit européen, des normes européennes et une culture européenne de la santé qui pourrait, pour reprendre le mot de Mme Delmas-Marty, « polliniser » le monde. On peut à ce stade évoquer une « puissance douce » ou un pouvoir d'attraction, car nul doute que le juge péruvien,

thaïlandais ou californien sera sensible à cette définition des droits de la personne en matière de santé et, à son tour, pourra agir puisque les actions en recours collectif sont prévues et que le RGPD y incite.

Nous sommes aujourd'hui à un carrefour civilisationnel où nos responsabilités, en tant que juristes, politiciens, chercheurs, scientifiques ou mathématiciens européens, sont d'autant plus grandes que notre responsabilité vis-à-vis du reste du monde est importante, et que nous savons que nous sommes à la fois attendus et entendus par nombre de personnes, par des ONG spécialisées dans le domaine de la santé, des associations de patients et des laboratoires, qui tenteront de s'appuyer sur ce que nous faisons pour faire évoluer leur législation dans le sens que nous leur indiquons. Ceci, cependant, à la condition que nous ne nous arrêtions jamais et que nous sachions rester humbles, car, pour reprendre les mots de Goethe, certes, la théorie est grise – ce qui correspond assez bien au RGPD –, mais l'arbre de la vie est éternellement vert[118].

118 Johann Wolfgang von Goethe (1749-1832), dans le *Faust I* (1808) fait dire à Méphistophélès : « *Mon bon ami, toute théorie est grise, mais vert et florissant est l'arbre de la vie* » (« *Grau, theurer Freund, ist alle Theorie, Und grün des Lebens goldner Baum* »), ou « *Mon bon ami, toute théorie est sèche, et l'arbre précieux de la vie est fleuri* » (*Faust*, éd. Dondey-Dupré père et fils, Paris, 1828, trad. G. de Nerval).

Échanges avec la salle

Question à l'attention de Mme Vasiliu

Vous avez insisté sur l'importance du consentement dans le RGPD. Pourtant l'article 8 dudit règlement[119] *accorde un traitement particulier aux enfants et ne dit rien sur la question des personnes vulnérables, souvent très mal représentées dans le secteur médico-social. Faut-il y voir une volonté de faire intervenir le législateur français sur ces aspects particuliers ?*

Mme Irina Vasiliu

Pour les personnes vulnérables dont le consentement n'est pas éclairé, on pourrait considérer que c'est le consentement plutôt que la loi qui est la base pour un traitement des données personnelles de santé. L'on pourrait également considérer qu'il est plus opportun de se fonder sur les intérêts vitaux de ces personnes si elles ne sont pas en mesure de donner un consentement éclairé. C'est plutôt cette réflexion-là qui a été privilégiée dans la directive de 1995, puis dans le RGPD.

Ce qui est important, dans le règlement actuel, c'est tout ce qui concerne le droit d'information et l'obligation de transparence de la part des responsables du traitement. Ceux-ci sont en effet obligés d'informer les personnes de façon adaptée, qu'il s'agisse d'un enfant, d'une personne vulnérable, ou d'un adulte faisant une demande de crédit. Il s'agit, avec cette obligation, de ne plus présenter à ces personnes des dossiers comportant des dizaines de pages peu ou pas lues, voire incompréhensibles.

Dans ce contexte, il reste à voir comment le marché va s'adapter à cette nouvelle approche, et comment ces informations vont vraiment être utiles, notamment pour les opérateurs qui devront être plus attentifs à ce qu'ils font.

119 RGPD, article 8 (Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information) : « *1. Lorsque l'article 6, paragraphe 1, point a), s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans. / 2. Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles. / 3. Le paragraphe 1 ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant* ».

Question à l'attention de M. Mignard

Je souhaiterais que maître Mignard nous précise sa pensée sur la question des données massives. Quels sont les garde-fous éthiques en la matière ? Car tout est possible à travers ces données qui, sans être a priori des données de santé, vont se révéler extrêmement intrusives dans la vie des personnes par leur utilisation et leur exploitation massives.

Jean-Pierre Mignard

C'est un fait que l'utilisation massive des données se révèle très intrusive dans la vie des personnes, d'autant que nous sommes rivés à un système juridique qui individualise les droits – les droits de la personne, notion capitale qui, sous l'influence notamment de René Cassin, va éclore à partir de 1945 au cœur de la mise en place de nos systèmes de démocratie libérale et humaniste. Il faut donc être très vigilant avec la collecte des données massives, d'autant que ces données permettent également des travaux sur les groupes et non plus seulement sur les personnes – la notion de groupe touchant à des aspects plus globaux (quartier d'habitation, lieu de vacances, préférence sexuelle, origine ethnique, etc.).

Le risque est donc que les géants de l'Internet[120] *collectent – sans forcément qu'on leur prête de mauvaises intentions – tellement d'informations que, si nous ne sommes pas vigilants, les grandes compagnies d'assurance ne seront plus demain Alliance ou Axa, mais Google et Amazon. C'est là un souci majeur, car la collecte massive des données, a priori sans finalité, peut tout permettre si nous n'y prenons pas garde. Et dans ce contexte, la barrière entre ce qui est permis et ce qui est défendu, entre le licite et l'illicite, entre le respect de nos valeurs et ce qui n'y répondrait pas, est le traitement, et même le cadre du traitement avec la responsabilité de l'opérateur du traitement. On voit là que la question des groupes est tout à fait essentielle. Par exemple, une compagnie d'assurance pourra être intéressée par connaître les informations particulières de tel ou tel quartier d'habitation (taux de mortalité des jeunes, nombre d'accidents ou de comportements à risques liés notamment à l'usage de stupéfiants, etc.) pour adapter sa politique d'assurance. Et l'aspect le plus inquiétant est que l'utilisation de toutes ces données massives nous fait entrer dans le règne de la statistique pure. C'est pourquoi il me semble indispensable que les mathématiciens deviennent également nos gardiens.*

Irina Vasiliu

Je rejoins maître Mignard pour dire que l'approche de l'Union européenne en matière de protection des données, à travers notamment le RGPD, est un modèle, voire un standard, qui peut être exporté dans d'autres pays grâce à une législation à la fois protectrice et garante des libertés individuelles.

120 Également connus sous l'acronyme GAFAM (*Google*, *Apple*, *Facebook*, *Amazon* et *Microsoft*).

Il est également important de réfléchir à ce qu'un traitement implique. On ne peut pas en effet collecter des informations sans afficher clairement le but recherché, ou sans se justifier, et en se cachant derrière des procédures techniques qu'il serait trop compliqué d'expliquer aux non spécialistes.

Il faut donc à la fois acter le pouvoir donné à l'individu, mais aussi protéger ceux qui traitent de façon légale et légitime les données.

Par contre, je suis en désaccord avec maître Mignard lorsqu'il prétend que le « bouclier de protection des données » (en anglais, « Privacy Shield ») serait obsolète. En effet, l'effort de la Commission a été de le rendre compatible avec le RGPD, voire de renforcer certains aspects dudit règlement dans le « bouclier de protection des données » en imposant un bilan annuel. C'est la raison pour laquelle le traitement des données personnelles au sein de l'Union européenne bénéficie d'une protection élevée : qu'il s'agisse, avec les mêmes règles, de transférer ces données d'un pays à l'autre de l'Union, ou vers un pays tiers – auquel cas s'ajoutent des conditions protectrices supplémentaires. Il s'agit là selon moi d'un bon équilibre.

Didier Tabuteau
Président adjoint de la section sociale du Conseil d'État,
modérateur de la table ronde

Merci pour ces échanges riches et fructueux. Dans cette évolution de l'approche des données personnelles de santé, il me semble que l'émergence de la notion de « groupe », soulignée par maître Mignard, sera peut-être aux données massives au XXI^{e} siècle ce que l'émergence de la notion de « population » a été à l'hygiène publique au XIX^{e} siècle. C'est donc là une transformation radicale qui nous interroge et qui risque de nous interroger encore longtemps.

Je remercie encore nos trois intervenants pour leurs exposés passionnants, ainsi que le public pour son écoute attentive et sa participation à cette séance.

La mise en œuvre de la loi santé

La loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé a mis en place un nouveau cadre pour la mise à disposition des données de santé. L'objectif affiché est de créer les conditions d'un accès ouvert aux données de santé, tout en garantissant la protection des données de santé à caractère personnel.

Pour ce faire, la loi a réformé tant les procédures d'accès aux données de santé que les institutions dédiées à leur mise à disposition, créant l'Institut national des données de santé (INDS), chargé de piloter, en lien étroit avec la Commission nationale de l'informatique et des libertés (CNIL), la mise à disposition des données de santé dont les bases ont été consolidées au sein du système national des données de santé (SNDS). Près de deux ans après l'adoption de cette loi, il convient de s'interroger sur la mise en œuvre de ces nouveaux dispositifs.

Sommaire

Biographie des intervenants

Les fonctions mentionnées sont celles exercées à la date de la conférence

Modérateur

Pierre-Louis Bras
Inspecteur général des affaires sociales, président du Conseil d'orientation des retraites (COR)

Pierre-Louis Bras est ancien élève de l'École des hautes études commerciales de Paris (HEC) et de l'École nationale d'administration (ENA). Il a exercé des fonctions de direction dans le secteur bancaire et mutualiste. Il a également été responsable des questions de sécurité sociale aux cabinets de Claude Évin (1988-1991), de Martine Aubry (1997-2000) et de Jérôme Cahuzac (2012-2013). Il a été nommé à la direction de la sécurité sociale (DSS) de 2000 à 2002. Pierre-Louis Bras a, par la suite, occupé la fonction de secrétaire général des ministères sociaux de 2013 à 2014. Il est inspecteur général des affaires sociales depuis 2003, président du Conseil d'orientation des retraites (COR) depuis 2015, professeur associé à l'université Paris-Descartes et associé aux travaux de la chaire santé de l'Institut d'études politiques de Paris.

Intervenants

Mylène Girard
Cheffe de la mission accès aux données de santé, direction de la recherche, des études et de l'évaluation des statistiques (DREES)

Mylène Girard est cheffe de la mission d'accès aux données de santé à la direction de la recherche, des études, de l'évaluation et des statistiques (DREES) au sein du ministère des solidarités et de la santé depuis mai 2016. La DREES est notamment chargée du pilotage des orientations stratégiques du système national des données de santé (SNDS). Auparavant, Mylène Girard a travaillé douze ans dans la sphère des allocations familiales dans des fonctions locales, régionales et nationales du réseau. Elle a notamment été adjointe à la direction de l'évaluation et de la stratégie à la Caisse nationale des allocations familiales (CNAF), puis a exercé la fonction de rapporteur extérieur à la cinquième chambre de la Cour des comptes, d'octobre 2012 à mai 2016.

Dominique Polton
Présidente de l'Institut national des données de santé (INDS)

Dominique Polton est présidente de l'Institut national des données de santé (INDS). Économiste et statisticienne de formation, elle a été conseillère du directeur général de la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) de 2014 à 2016, après avoir dirigé pendant huit ans la direction de la stratégie, des études et des statistiques de cette même institution. Elle a auparavant dirigé l'institut de recherche et de documentation en économie de la santé (IRDES). Elle préside le conseil scientifique de l'École des hautes études de santé publique et la Commission des comptes de la santé. Ses principales publications portent sur les politiques de régulation et les analyses comparatives des systèmes de santé.

Thomas Dautieu
Directeur adjoint de la conformité à la Commission nationale de l'informatique et des libertés (CNIL)

Titulaire d'un diplôme d'études approfondies (DEA) de droit public et diplômé de l'Institut d'études politiques de Lille, Thomas Dautieu est directeur adjoint de la conformité à la Commission nationale de l'informatique et des libertés (CNIL), en charge plus spécifiquement des secteurs économiques et de la santé. Il a commencé sa carrière à la CNIL en se consacrant aux problématiques liées aux communications électroniques, pour ensuite devenir responsable du service des contrôles. Il est également l'auteur d'articles juridiques traitant de la protection des données et des autorités administratives indépendantes, et est chargé d'enseignement à l'université Panthéon-Assas. Précédemment, Thomas Dautieu était en poste au Conseil supérieur de l'audiovisuel (CSA) en tant que directeur adjoint des programmes.

Actes – La mise en œuvre de la loi santé

Pierre-Louis Bras
Inspecteur général des affaires sociales,
président du Conseil d'orientation des retraites (COR),
modérateur de la table ronde

La deuxième table ronde de ce colloque porte sur la mise en œuvre de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, dite loi « santé ». Dans la continuité de la table ronde n° 1 qui traitait de façon générale des données de santé, nous allons évoquer ici les données de santé constituées par les pouvoirs publics, c'est-à-dire les données médico-administratives dont traite principalement la loi « santé » de 2016.

Pour évoquer ce sujet, j'ai le plaisir de recevoir trois des principaux acteurs de la mise en œuvre de cette loi : Mme Girard, cheffe de la mission accès aux données de santé à la direction de la recherche, des études et de l'évaluation des statistiques du ministère de la santé ; Mme Polton, présidente de l'Institut national des données de santé (INDS), qui a connu ce type de données en participant au développement du système d'information en santé à la Caisse nationale d'assurance maladie (CNAM) ; et M. Dautieu, directeur adjoint de la conformité à la Commission nationale de l'informatique et des libertés (CNIL). J'ajoute que j'ai eu également à connaître ce dossier en rédigeant un rapport en amont de la loi « santé » de 2016, qui a été l'un des éléments de préparation du texte final.

Pour commencer cette séance que j'ai le privilège de présider, je souhaiterais présenter quelques éléments pour cerner la question dont nous allons débattre.

Nous parlons d'un système de données de santé qui, historiquement, s'est constitué autour de deux piliers principaux : le système national d'information inter-régimes de l'Assurance maladie (SNIIRAM) qui recueille toutes les informations portées sur les feuilles de remboursement de soins de médecine de ville ; et le programme de médicalisation des systèmes d'information (PMSI) ayant pour objet de décrire l'activité hospitalière qui, depuis le début des années 2000, sert à tarifer et à payer les hôpitaux.

Ces deux systèmes avaient été développés pour des finalités particulières : envoyer des informations aux professionnels de santé ; contrôler, évaluer et aider à la maitrise des dépenses de santé côté SNIIRAM ; et connaître l'activité hospitalière et tarifée côté PMSI.

Ces deux systèmes ont été connectés entre eux et ont pu converger, en 2009-2010, créant ainsi une base de données administrative permettant de décrire de façon assez complète l'ensemble du parcours de soins du patient français. Nous sommes donc là en présence d'un système informationnel très riche, qui stocke

énormément de données, qu'il s'agisse de médecine de ville (actes médicaux, médicaments délivrés, analyses biologiques réalisées, etc.) ou de médecine hospitalière (diagnostics principaux, diagnostics secondaires, actes médicaux hospitaliers, médicaments consommés, etc.).

Certes ce système comporte quelques lacunes. On ne dispose pas, par exemple, de résultats de biologie ou de données environnementales sur la personne (obésité, tabagisme, alcool). Malgré cela, l'intérêt de cette base de données est réel comme l'a prouvé, de manière très concrète, l'affaire dite « du Médiator ». C'est en effet grâce à cet outil informatique que l'on a pu confirmer l'hypothèse, formulée par la pneumologue Irène Frachon[121], selon laquelle la consommation du Médiator entraînait des problèmes pour les valves cardiaques.

Ce système d'information se révèle donc d'un très grand intérêt public, grâce aux nombreux bénéfices qu'il permet de réaliser : bénéfices sanitaires en termes de pharmacovigilance et de conception des politiques publiques ; bénéfices économiques dès lors que cela permet de travailler sur l'organisation de notre système de soins et sur la pertinence des actes ; bénéfices économiques aussi pour l'industrie pharmaceutique puisqu'elle peut activer des recherches en utilisant cette base qui lui évite de constituer des échantillons. Pour l'activité pharmaceutique, comme pour chacun d'entre nous, cela peut donc constituer un apport majeur, par exemple, en matière de pharmacovigilance – comme dans l'affaire du Médiator –, et aussi générer un bénéfice démocratique parce que ces données peuvent contribuer au débat public sur notre système de santé.

Pour autant, ce système d'information restait sous-utilisé. Et de nombreux chercheurs soulignaient les obstacles qu'ils devaient franchir pour accéder aux données. Ainsi, lorsque les réflexions sur la réforme de notre système de santé ont débuté, la volonté de mettre en place un système de *données ouvertes* (en anglais, « *open data* ») s'est fait entendre ; l'idée étant qu'il s'agissait de données publiques à mettre à la disposition du public. À l'époque, une association appelée *Libérer les données de santé* a même été créée contre les « technocrates » – surtout ceux travaillant à la CNAM – accusés de vouloir garder le pouvoir en refusant l'accès à ces données de santé.

Puis, il est apparu que les principes des données ouvertes ne trouvaient pas à s'appliquer à ces informations, car, bien qu'anonymisées – c'est-à-dire sans le nom ou le NIR[122] – et cryptées, elles ouvraient des possibilités de réidentification si l'on avait accès à la complétude des données (par exemple, dans la base des données anonymisées figure la date d'entrée à l'hôpital, or si l'on connait cette date et qu'il n'y a eu qu'une seule entrée ce jour-là dans l'hôpital en question, il est facile de retrouver la personne et d'avoir accès à toutes ses données de santé y compris celles sur ses parcours de soins). Dans ce cadre, des réidentifications opportunistes sont également possibles à travers quelqu'un qui, ayant accès aux données, pourra consulter le parcours de soins de son collègue, d'un membre de sa famille ou d'une personnalité par curiosité.

121 Le docteur Irène Frachon est le premier médecin à avoir établi un lien direct entre la mort de nombreux patients et la prise du Mediator.

122 Le numéro d'inscription au répertoire (NIR) est le numéro de sécurité sociale.

Tout cela rendait le système juridique d'accès aux données de santé extrêmement compliqué, et faisait peser sur les chercheurs voulant y accéder des obstacles quasiment infranchissables. Alors même que certaines données réidentifiantes étaient, quant à elles, en matière hospitalière, largement diffusées à travers le PMSI (par exemple, sous forme de Cédérom dont on avait ensuite plus aucune traçabilité).

La loi « santé » a donc souhaité, dans un premier temps, faciliter l'accès aux données de santé – le risque étant que cet accès maîtrisé soit perçu comme une loi d'enfermement.

Les principes de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

Le principe de base de la loi « santé » est qu'elle donne une nouvelle dénomination à tous les systèmes d'information de santé, regroupés sous la dénomination de système national des données de santé (SNDS) pour montrer son caractère unifié et sa vocation à aider à l'information, à la veille, à l'étude et à la recherche.

La loi « santé » place ce système sous l'autorité stratégique de l'État, par opposition à ce qui existait auparavant, à savoir que le système d'information appartenait à celui qui l'avait construit et transmettait les informations (sécurité sociale, professionnel de santé, etc.) ; l'État n'étant alors qu'un tiers parmi d'autres.

Ainsi placé sous l'autorité stratégique de l'État, ce nouveau système d'information a pour mission d'offrir à tous les utilisateurs un accès aux données de santé, aux fins de renseignements et de statistiques. Pour cela, un organisme *ad hoc* a été créé en 2017 : l'Institut national des données de santé (INDS) qui regroupe l'ensemble des parties prenantes qui ont intérêt ou vocation à accéder aux données de santé. Cet institut, qui succède à l'Institut des données de santé (IDS) créé en 2007, est actuellement présidé par Mme Dominique Polton qui nous fait l'honneur de sa présence à cette séance.

La loi « santé » a donc permis de reconstruire une gouvernance autour du système d'information de santé et de poser des principes de bases, à savoir que pour tous les accès il y a des exigences de secret professionnel, de traçabilité et de préservation des données.

Il ne s'agit pas ici de céder à la mode des données ouvertes, mais d'offrir, à partir de ces informations, un accès à des données qui ne sont pas réidentifiantes. C'est ainsi que l'on traite des données agrégées et des données « floutées » qui ne permettent pas la réidentification. Ensuite, dès lors que ces données sont constituées, elles doivent être rendues publiques – et l'on renvoie ici à l'initiative des pouvoirs publics et à la vigilance de l'INDS pour promouvoir cette diffusion publique de données.

Pour ce qui concerne les données réidentifiantes, deux systèmes existent : des accès permanents, octroyés aux organismes qui ont besoin pour leurs fonctions d'accéder à ces données – par exemple, les agences sanitaires –, et des accès ponctuels,

processus que le législateur a voulu le plus simple possible en passant devant un comité d'expertise[123], puis devant la Commission nationale de l'informatique et des libertés (CNIL), afin d'offrir une possibilité d'accès aux données dans un cadre préservé[124].

Après ces quelques mots d'introduction pour tracer sommairement l'historique et la position de la loi « santé », je donne la parole à Mme Girard qui va nous exposer la mise en œuvre de cette loi.

Mylène Girard

Cheffe de la mission accès aux données de santé, direction de la recherche, des études et de l'évaluation des statistiques (DREES)

Merci M. le président. Je vous propose d'évoquer le cadre juridique du système national des données de santé (SNDS) pour vous donner un aperçu de son architecture. Le SNDS est évoqué à l'article 193 de la loi « santé »[125] et s'est traduit par deux décrets d'application du 26 décembre 2016[126] et un ensemble d'arrêtés[127].

Le contenu du SNDS

Les données du SNDS sont issues des principales sources médico-administratives qui transitent par les caisses primaires d'assurance maladie (CPAM) et par les hôpitaux – *via* l'Agence technique de l'information sur l'hospitalisation (ATIH)[128] –, auxquels nous sommes en train de chaîner les causes médicales de décès – *via* l'Institut national de la santé et de la recherche médicale (Inserm).

La première version du système national de données de santé (SNDS) a été ouverte en avril 2017. Il regroupe et met à disposition, pour des finalités précises, des données individuelles de santé dites « pseudonymisées ». Ce chaînage de plusieurs bases de données regroupe trois éléments : le système national d'information inter-régimes de l'assurance maladie (SNIIRAM)[129] ; les données des hôpitaux et autres établissements de santé (programme de médicalisation des systèmes d'information ou PMSI)[130] ; et les données statistiques relatives aux causes médicales de décès (BCMD)[131].

123 Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (CEREES) créé par la loi du 26 janvier 2016.
124 Dispositif de l'article 193 de la loi du 26 janvier 2016 de modernisation de notre système de santé.
125 Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.
126 Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé » ; et décret n° 2016-1872 du 26 décembre 2016 modifiant le décret n° 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978.
127 Voir par exemple, 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 ».
128 L'agence technique de l'information sur l'hospitalisation est un établissement public administratif créé par le décret n° 2000-1282 du 26 décembre 2000.
129 Le SNIIRAM regroupe les données patients (démographiques, géographiques, certains diagnostics, marqueurs de précarité) et tous les contacts avec le système de santé de ville (actes, prescriptions, médicaments, etc.).
130 Résumé de tous les séjours hospitaliers, et diagnostics principaux et associés et actes principaux codés.
131 Causes de décès codées (classification internationale des maladies).

Ces trois bases de données offrent une vision complète du parcours de soins. On y retrouve en effet une masse d'informations très précises sur le parcours de soins de soixante-sept millions de personnes, qui plus est sur un historique de dix ans et sans perdus de vue. C'est un ensemble d'informations très intéressantes et attendues par les chercheurs. En revanche, ces bases ne contiennent ni données cliniques ou para-cliniques, ni informations sur les antécédents ou les facteurs de risque des patients.

Le SNDS intègrera, lorsqu'elles seront constituées, deux bases de données supplémentaires :

- les données médico-sociales des maisons départementales pour les personnes handicapées, régies par les dispositions relatives au handicap, placées sous la responsabilité de la Caisse nationale de solidarité pour l'autonomie (CNSA). Ces données ne remonteront probablement pas avant 2019 dans la mesure où la CNSA est en train de mener un important chantier d'harmonisation des systèmes d'information des maisons départementales des personnes handicapées, afin de disposer de données homogènes qui pourront s'agréger de façon satisfaisante ;

- un échantillon représentatif des données de remboursement par bénéficiaires transmis par les mutuelles. Ce cinquième flux, très attendu, permettra de mener des études intégrant la partie complémentaire des dépenses. Il ne sera probablement pas dans le SNDS avant 2019.

Il doit être noté que le SNDS est gérée de façon opérationnelle par la Caisse nationale d'assurance maladie (CNAM), qui est le responsable de traitement, avec un pilotage des orientations stratégiques par l'État. Les données de tous les citoyens y sont déversées, ce qui représente chaque année un milliard deux cent millions de feuilles de soins et onze millions de séjours hospitaliers, et occupe un espace de stockage de quatre cent cinquante téraoctets[132] gérés par la CNAM.

La mise à disposition des données du SNDS peut se faire au travers d'extractions à façon, de travail sur des échantillons généralistes au 1/100e de la population, ou au travers de données agrégées. À la rédaction des textes d'application du SNDS, une attention très particulière a été portée à la question de la sécurité des données, sachant que le risque de réidentification est toujours possible lorsque l'on sait manipuler les données.

L'accès aux données s'effectue dans des conditions qui en assurent la confidentialité et l'intégrité, ainsi que la traçabilité des accès et des autres traitements. Un « référentiel de sécurité » est porté par un arrêté en date du 22 mars 2017[133]. Il pose les grands principes suivants : pseudonymisation, traçabilité des entrées et des sorties de données et des traitements réalisés à l'intérieur de l'espace sécurisé géré par la CNAM, impossibilité de sortir des données si elles ne sont pas anonymes, accord d'habilitations sur des périodes précises en lien avec des projets et les agents missionnés pour ce projet.

132 Unité de mesure d'importantes quantités d'informations numériques. Un téraoctet (1 To) est égal à 1 024 gigaoctets (1 024 Go).

133 Arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au système national des données de santé.

Une très grande attention est également portée à la sensibilisation des utilisateurs : la CNAM et tous les utilisateurs publics et privés appelés à manipuler ces données ont l'obligation de sensibiliser les utilisateurs au maniement de ces informations. Ils s'engagent formellement et personnellement à ne pas poursuivre une finalité de réidentification, au risque sinon d'encourir des sanctions pénales.

L'accès aux données ne présentant pas de risque de réidentification

Les jeux de données qui ne présentent aucun risque de réidentification des personnes, même indirect, sont accessibles en données ouvertes, c'est-à-dire accessibles à tous, y compris au grand public. Il existe de nombreuses informations présentées en données ouvertes sur les sites Internet, notamment ceux de la CNAM et de l'Agence technique de l'information sur l'hospitalisation (ATIH). Dans ce contexte, l'idée est d'orienter les utilisateurs vers les données dont ils ont besoin de façon à faciliter l'utilisation des informations déjà mises en lignes.

L'accès aux données comportant un risque de réidentification

Pour mener des études, recherches et évaluations, deux modalités d'accès existent :

- Un accès permanent est accordé à des organismes qui disposent d'une mission de service public – c'est un critère porté par la loi « santé » de 2016 dont l'un des décrets mentionne les vingt-cinq catégories d'organismes ou de services disposant de cet accès. Cependant, disposer d'un accès permanent ne signifie pas avoir accès à tout. C'est ainsi qu'il y a eu un important travail préalable à la parution du texte pour lister les usages et les besoins de ces catégories d'organismes, de façon à ne leur permettre l'accès qu'aux données dont ils ont besoin. Par exemple, le décret « SNDS » du 26 décembre 2016[134] précise bien que telle catégorie d'organisme a accès à telle catégorie de données. Tout le monde n'a donc pas accès à l'exhaustivité des données, et certains organismes n'ont accès qu'à des données agrégées.

Ce travail extrêmement précis est une condition de crédibilité du système. En effet, derrière ces accès permanents, il y a entre deux et trois mille utilisateurs potentiels, ce qui multiplie d'autant les risques de mésusage. Parmi ces utilisateurs, on compte notamment les agences sanitaires, les agences régionales de santé, les directions des ministères, les observatoires régionaux de santé, etc.

- Le second type d'accès concerne l'accès sur projet. Il est ouvert à tous les acteurs publics et privés, ainsi qu'aux acteurs qui ont un accès permanent (par exemple, un acteur qui aurait un accès permanent pour une catégorie de données agrégées et qui, pour un projet ponctuel précis, aurait besoin de davantage de données). S'applique alors la procédure classique constituée de trois étapes. Ce mécanisme de confiance, instauré sur tout le dispositif, a parfois été perçu comme un alourdissement, notamment au début de la mise en place du SNDS. En réalité, le travail d'examen produit lors des étapes préalables à l'examen des projets par la CNIL lui permettent de statuer plus vite.

134 Décret du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».

Les obligations à respecter

Les organismes ayant un accès permanent doivent désigner des correspondants « informatique et libertés » (CIL), devenus « délégués à la protection des données » (DPO) avec l'entrée en vigueur du Règlement général sur la protection des données (RGPD)[135]. Ces mêmes organismes doivent tenir le registre de ce qu'ils font avec le SNDS (liste des traitements et des personnes habilitées), sensibiliser les agents, établir un bilan d'utilisation des données, et déposer un dossier *via* la procédure classique lorsqu'ils veulent faire un appariement – un accès permanent à une catégorie de données ne signifiant pas que l'on puisse faire un assemblage avec d'autres données sans passer par la procédure classique.

Une précision importante à noter est que, pour tous les acteurs publics ou privés, le dépôt d'un dossier reste subordonné à un critère d'*intérêt public*.

Enfin, il doit être rappelé que le législateur a prévu l'interdiction de certaines finalités : interdiction par les industriels d'utiliser les données du SNDS pour faire la promotion commerciale des produits de santé, et pour les assureurs de tenter d'exclure certaines personnes des garanties des contrats d'assurances ou de modifier la tarification selon les profils individuels.

L'obligation de transparence

La dernière obligation d'importance est le corollaire de tout ce qui vient d'être rappelé, et concerne la transparence. Il existe en effet une nécessité de dire ce que l'on fait avec les données de santé, d'indiquer qui les manipule et, au final, ce que l'on en a fait. Et si l'on a mené une étude, une recherche, ou une évaluation, le résultat doit être publié.

C'est un enjeu fort, notamment vis-à-vis des industriels et des assureurs, qui doit être concilié avec le respect du secret commercial.

Dominique Polton

Présidente de l'Institut national des données de santé (INDS)

Effectivement, à partir de ce premier cadre, le système s'est mis en place relativement rapidement. L'Institut national des données de santé (INDS) qui a succédé à l'Institut des données de santé (IDS) a été créé en avril 2017 – il ne faudrait pas croire qu'avant cette période il n'y avait pas d'accès, même si ce dernier était complexe notamment en raison d'un empilement de dispositifs –, et la procédure d'accès dans le nouveau système a été opérationnelle à partir de la fin du mois d'août 2017.

Il y a eu un petit temps mort – que l'on aurait souhaité plus court –, qui a fait que durant quelques mois il n'y avait pas vraiment de réceptacle pour les dossiers. Mais on avait pris soin, pendant le mois précédant l'ouverture, de mettre à disposition

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

toute la documentation nécessaire et de se mettre en situation de réceptionner les dossiers dès l'ouverture, pour que les demandeurs puissent préparer leur dossier. Cette demande de dossier, faite auprès de l'Institut national des données de santé (INDS) – porte d'entrée unique pour l'accès au système national des données de santé (SNDS) et, plus globalement, à toutes les bases de données déjà constituées –, est aujourd'hui totalement dématérialisée. D'emblée, on a conçu un système doté d'une plateforme informatique sur laquelle les demandeurs renseignent, ou déposent un certain nombre de pièces et d'éléments. Il n'y a pas d'échange papier.

La procédure a été ouverte le 28 août 2017. Elle passe par une première étape auprès de l'INDS qui aide le demandeur ayant déposé son dossier. L'INDS vérifie que le dossier est complet et le transmet dans un délai très encadré de sept jours au Comité d'expertise pour les recherches, évaluations et études (CEREES). Ce dernier examine le dossier et dispose d'un mois pour rendre son avis sur la méthodologie, l'adéquation du projet aux données demandées et aux finalités (et éventuellement la qualité scientifique du dossier). Sans réponse au bout d'un mois, l'avis est réputé favorable. Le dossier est alors transmis à la Commission nationale de l'informatique et des libertés (CNIL) qui se prononce dans un délai de deux mois (qui peut être prolongé dans les conditions prévues par la loi), et qui autorise ou non le traitement. L'absence de réponse de la CNIL ne vaut pas autorisation.

La loi a aussi confié à l'INDS la responsabilité d'évaluer, sur saisine du ministère, ou de la CNIL, ou à sa propre initiative, si les études, recherches et évaluations pour lesquelles les données sont sollicitées présentent un caractère d'*intérêt public*.

Je reviendrai sur cette question de l'intérêt public, car c'est une notion qui est aujourd'hui peu définie. Pour aider l'INDS à élaborer une doctrine, un comité spécifique a été constitué auprès du conseil d'administration de l'INDS.

Depuis la mise en place de la nouvelle procédure d'accès, le 28 août 2017, cent vingt demandes d'accès aux données ont été déposées, dont une quarantaine pour les données du SNDS : deux tiers sont orientés vers la recherche publique (centres hospitaliers universitaires, Institut national de la santé et de la recherche médicale, centres de lutte contre le cancer, etc.), et un tiers émane des industriels ou des bureaux d'études qui travaillent pour ces derniers.

Le Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (CEREES), qui examine le dossier à la suite de l'INDS, fait un travail approfondi et valide favorablement 60 % des dossiers qui lui sont déférés – avec parfois des recommandations. Cela ne signifie pas que 40 % des dossiers sont rejetés, ceux-ci pouvant revenir modifiés auprès du CEREES pour être de nouveau examinés. On le voit, l'examen est attentif, et il est nécessaire que les protocoles soient suffisamment précis pour que l'on comprenne bien ce que les intéressés veulent faire, que la liste des informations souhaitées soit clairement établie. Dans ce contexte, il n'est pas rare que les dossiers soient vus deux fois par le CEREES.

Notons enfin que la procédure est relativement rapide, le CEREES se réunissant tous les mois pour examiner entre vingt et vingt-cinq dossiers. On peut donc affirmer que cette procédure dématérialisée fonctionne bien et respecte les délais contraints qui sont les siens.

Comme je le rappelais précédemment, le rôle de l'INDS est d'être le point d'entrée dans cette procédure dématérialisée, opérationnelle depuis la fin du mois d'août 2017. Mais l'INDS a aussi, avant que les demandeurs ne déposent leurs dossiers, un rôle de conseil et d'accompagnement. En effet, l'INDS reçoit de nombreuses demandes de renseignement, notamment sur la manière de procéder ou sur les conditions d'accès aux données, et aide les demandeurs à formaliser leurs dossiers pour qu'*in fine* ceux-ci arrivent à la CNIL dans les meilleures conditions, et que celle-ci puisse disposer d'informations précises, nécessaires pour statuer. Tout ce parcours-là facilite l'ensemble du dispositif.

L'INDS réalise également un travail avec les différentes familles d'utilisateurs pour leur permettre d'accéder aux données de santé comportant un risque de réidentification, soit de façon permanente, soit en fonction de projets précis. Mais un certain nombre d'utilisateurs permanents souhaiteraient pouvoir disposer d'accès « intermédiaires ». Cela serait possible, par exemple, en ayant une autorisation unique – une décision unique de la CNIL –, afin d'avoir accès à des jeux de données précis de manière récurrente. Dans ce contexte, le rôle de l'INDS est d'accompagner les utilisateurs pour les aider à exprimer leurs besoins, afin de trouver des solutions dans le dispositif actuel. Il peut s'agir notamment de *procédures d'accès facilités* qui sont les méthodologies de référence, les décisions uniques, ou des procédures que la CNIL pourrait homologuer pour que, par exemple, dans certains cas précis et bien délimités, l'on n'ait pas forcément besoin de passer par l'ensemble du circuit INDS-CEREES-CNIL. Tout cela est en construction ; l'objectif étant d'ouvrir les données au maximum d'utilisations et de multiplier les usages.

Il existe, au sein de l'INDS, un comité d'expertise sur l'intérêt public qui examine certains dossiers et essaye de définir progressivement, à travers ces cas individuels, une doctrine pour définir plus précisément ce qui relève ou non de l'intérêt public. L'intérêt public n'est pas forcément antinomique avec l'intérêt commercial, sinon on n'ouvrirait pas les bases de données aux acteurs privés qui ont nécessairement des intérêts privés. La question est : au-delà de l'intérêt commercial, cette étude ou recherche présente-t-elle *aussi* un intérêt public suffisant ? C'est ce travail d'analyse que réalise, en fonction des demandes, le comité d'expertise qui a dû évaluer depuis ses débuts six dossiers.

Enfin, le groupement d'intérêt public que constitue l'INDS possède une gouvernance où sont représentés tous les producteurs et toutes les familles d'utilisateurs : usagers, régulateurs publics (État, assurance maladie, agences), professionnels et établissements de santé, organismes d'assurance complémentaire, industriels et bureaux d'études, ainsi que la recherche et l'enseignement. Cette gouvernance a pour but de favoriser le dialogue entre les producteurs et les utilisateurs et de développer la confiance et la volonté d'utiliser au maximum les données dans de

bonnes conditions et selon les besoins propres à chacun. Il s'agit également, à travers ce dialogue, de faire progresser le SNDS, qui en est aujourd'hui à sa version première – et pour lequel on attend, dans quelques années, une version enrichie.

Si nous avons été visionnaires pour créer cet outil, nous devons constamment l'améliorer pour rester parmi les pays les plus avancés en la matière, car d'autres pays sont engagés dans des démarches identiques et assez ambitieuses. Dans ce contexte, l'INDS peut être un contributeur important, car il regroupe autour de lui beaucoup d'intelligence collective provenant de tous les acteurs, et peut ainsi mieux répondre aux besoins nouveaux et faire progresser l'ensemble du système.

Mylène Girard

Cheffe de la mission accès aux données de santé, direction de la recherche, des études et de l'évaluation des statistiques (DREES)

S'agissant des perspectives d'évolution, maintenant que les briques du dispositif sont en place, nous sommes mobilisés pour renforcer l'accompagnement des utilisateurs. Le système fonctionnant très bien, nous nous devons en effet de répondre aux attentes croissantes des utilisateurs dont certains étaient très sceptiques au début. Notons qu'en novembre 2017, la CNIL a libéré les premières autorisations d'accès aux données qui étaient à l'examen du CEREES au mois de septembre. Ainsi, sur les premiers dossiers, le délai intégral depuis le dépôt à l'INDS jusqu'à l'autorisation de la CNIL se monte-t-il à deux mois et demi. Nous sommes donc très satisfaits de voir que les délais de mise à disposition des données sont tenus – d'autant qu'il s'agissait d'une attente forte de la part des acteurs publics et privés.

Dans les autres perspectives d'évolution, il y a la mise en place de procédures simplifiées. Comme l'a rappelé Mme Polton, nous disposons d'un système de décision unique qu'il faut pouvoir adapter – ce qui avait été mis en place dans les dispositions antérieures, avec des autorisations notamment d'utilisation du PMSI. C'est pourquoi nous sommes actuellement en train de travailler à une mise à disposition simplifiée pour accéder à l'échantillon généraliste des bénéficiaires – échantillon du SNDS à 1/100e. L'idée étant de classer les catégories de dossiers, comme par exemple les dossiers quasi-règlementaires ou ceux commandés par la puissance publique, afin d'éviter de passer systématiquement par les trois étapes INDS, CEREES et CNIL. Ce dispositif est actuellement à l'examen du CEREES, avant de faire l'objet d'un examen par la CNIL pour homologation.

Enfin, l'idée est également de développer les méthodologies de référence qui sont un outil particulièrement important, qui va dans le sens de la responsabilisation des acteurs et de l'entrée en vigueur du règlement général sur la protection des données (RGPD). Cet outil permettra de responsabiliser les responsables de traitement qui se conforment à une méthodologie de référence et se déclarent en conformité sur un formulaire CNIL. Nous avons donc tout un travail lancé par l'INDS de recensement des besoins qui est très attendu des différentes communautés d'acteurs.

In fine, l'idée est de démultiplier l'usage de ces données dans un cadre extrêmement respectueux de la vie privée des citoyens.

Pour terminer, je souhaiterais rappeler que les partenaires privés avec lesquels nous travaillons, notamment les industriels, insistent sur le caractère déterminant du point de vue de l'attractivité de la réussite de ce projet, ainsi que sur les avantages d'une ouverture des données avec, à la clé, une meilleure connaissance de notre système de soins au bénéfice du citoyen[136]. Et pour davantage d'informations, je vous encourage à visiter les sites Internet du SNDS et de l'INDS.

Pierre-Louis Bras
Inspecteur général des affaires sociales,
président du Conseil d'orientation des retraites (COR),
modérateur de la table ronde

Merci beaucoup. Je donne maintenant la parole à M. Dautieu.

Thomas Dautieu
Directeur adjoint de la conformité à la Commission nationale de l'informatique et des libertés (CNIL)

Je remercie le Conseil d'État pour son invitation qui permet à la Commission nationale de l'informatique et des libertés (CNIL) de donner son point de vue sur la mise en œuvre de la loi « santé » de 2016. Beaucoup de choses ont été dites sur ce sujet, aussi vais-je essayer de faire le lien entre les différents éléments évoqués.

1. - L'article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé

Pour ce qui concerne la CNIL, l'article 193 de la loi « santé » modifie la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés en fusionnant les deux chapitres IX et X, qui s'appliquaient aux procédures de recherche dans le domaine de la santé, pour ne plus avoir qu'un seul chapitre IX (une seule procédure) pour toutes les données de santé. Notons également qu'actuellement la loi « informatique et libertés » de 1978 est en cours de révision, notamment pour intégrer le règlement général sur la protection des données (RGPD).

Dans ce contexte, la CNIL doit contribuer à mettre en œuvre une procédure dématérialisée récente d'accès aux données de santé avec, en regard de cet objectif, une loi « informatique et libertés » en cours de révision sous l'influence des dispositions relatives aux données de santé mais aussi du RGPD.

Dans un premier temps, je vous propose de replacer la question de l'accès aux données de santé dans le cadre porté par le RGPD, puis, dans un second temps, d'analyser le rôle de la CNIL dans ce cadre juridique.

136 Voir : rapport du Conseil national de l'industrie, comité stratégique de filière (CSF) des industries et technologies de santé, *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*, 29 mars 2017, éd. ministère des affaires sociales et de la santé.

Au-delà de l'aspect purement juridique, il me semble important que le cadre français, en termes de recherche dans les données de santé, s'inscrive dans la philosophie portée par le RGPD.

Quelles sont les idées fortes portées par le RGPD, dont certaines nous intéressent directement ? Elles sont, selon moi, au nombre de trois.

1.1. - Mettre l'individu au centre de la régulation

Le RGPD renforce considérablement le rôle de l'individu dans le traitement de ses données en lui offrant notamment une information améliorée, plus importante et plus lisible, avec bien sûr tous les droits classiques qui s'y rattachent (droits d'accès, de rectification ou d'opposition), mais également de nouveaux droits portés par le RGPD comme, par exemple, le « droit à la portabilité » – qui n'a pas vocation à s'appliquer de façon première dans le domaine de la santé, mais mérite toutefois d'être souligné.

Et puis, au titre de l'amélioration des droits des personnes, il y a aussi le rôle du « consentement » qui devient un élément central du traitement de ces données.

1.2. - Crédibiliser les CNIL européennes

La crédibilisation des autorités de régulation porte sur deux niveaux. Le premier, qui ne nous concerne pas directement, est un mécanisme de coopération entre les CNIL européennes destiné à donner des réponses uniques en cas de traitements transfrontaliers. Il s'agissait de répondre à une critique récurrente envers les CNIL européennes qui pouvaient, sur certaines questions, avoir des positions divergentes. Le RGPD crée un mécanisme de coopération qui *in fine* permet de crédibiliser la réponse qui sera apportée par la CNIL en charge du dossier.

Le second niveau concerne le renforcement des pouvoirs de sanction des CNIL européennes, avec notamment des pouvoirs en matière d'amendes administratives qui peuvent s'élever jusqu'à plusieurs dizaines de millions d'euros – un montant inconnu de la CNIL française.

1.3. - Responsabiliser les garants des traitements

L'idée portée par le RGPD est de sortir de cette logique de formalité administrative préalable. En effet, pour trop de personnes encore, respecter la loi « informatique et libertés » signifie faire une déclaration ou une demande d'autorisation à la CNIL pour, une fois l'accord obtenu, ne plus se soucier de rien. Force est de constater que cela ne correspond plus aux exigences informatiques actuelles, notamment en termes de sécurité ou d'analyse de l'anonymisation des données.

C'est pourquoi la philosophie portée par le RGPD est d'alléger considérablement, voire de supprimer, toutes ces formalités administratives pour responsabiliser la personne qui met en œuvre le traitement, à travers un certain nombre d'outils proposés ou imposés : délégué à la protection des données, études d'impact, registres, etc.

Les données de santé

Concernant les données de santé, le RGPD s'inscrit dans le droit fil de la directive (abrogée) de 1995 et de la loi « informatique et libertés » de 1978, avec un principe d'interdiction et des exceptions pour permettre le traitement des données de santé.

Parmi ces exceptions, l'article 89 du RGPD permet le traitement des données de santé à des fins de recherche, sous réserve de « *mesures techniques et organisationnelles* ». Dans ce contexte, il est donc possible de traiter des données de santé à des fins de recherche, à condition d'avoir mis en place de telles mesures. Notons qu'au titre des mesures techniques, le RGPD promeut notamment le principe de pseudonymisation.

Le RGPD fixe donc des principes et permet aux différentes lois nationales d'apporter des exigences complémentaires, y compris des limitations, pour renforcer les conditions de traitement des données de santé.

Sur ce point, c'est tout l'objet de la loi « informatique et libertés » qui est actuellement en cours de réécriture ; projet sur lequel la CNIL a rendu son avis fin novembre 2017[137].

Par ailleurs, il me semble nécessaire de faire deux remarques sur les marges de manœuvre qui sont permises aux États membres.

1) Il ne faudrait pas qu'en matière de traitement de santé, on arrive à une sorte de grand écart juridique avec, pour l'ensemble des traitements, des formalités administratives qui seraient réduites à zéro pour le droit commun des traitements et, pour les traitements des données de santé, le maintien de régimes administratifs extrêmement lourds. Il faut donc que tout cela soit en cohérence, pour que les chercheurs n'aient pas l'impression qu'une suspicion pèse sur leurs travaux auxquels on imposerait des formalités administratives trop contraignantes.

2) Enfin, il faut également que le système juridique français soit compétitif. Il ne faudrait pas, en effet, qu'au niveau de l'Union européenne, les contraintes imposées aux chercheurs français pousse ce type de recherche à se développer dans d'autres pays.

C'est là tout l'objet de la révision de la loi « informatique et liberté » de 1978, et notamment de son chapitre IX.

Bien sûr, mon propos n'est pas de plaider pour un abaissement de la protection des personnes, mais de trouver un juste équilibre entre les contraintes que le législateur national a fait ou va faire dans le cadre de la révision de la loi de 1978, et le principe de *responsabilisation* des acteurs porté par le RGPD.

Notons que ce principe de responsabilisation est déjà à l'œuvre dans le droit français, comme, par exemple, au niveau du mécanisme des accès permanents qui

137 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 (demande d'avis n° 17023753).

n'a pas de mécanisme d'autorisation administrative préalable, mais seulement un certain nombre d'obligations pesant sur les organismes qui en bénéficient et à qui il incombe de le mettre en œuvre en interne. Dans un autre domaine, comme par exemple l'hébergement des données de santé, on s'aperçoit que la loi « santé » de 2016 a fait le choix de passer d'un principe d'agrément par le ministère à un principe de certification pour, également, alléger les contraintes administratives *a priori* pour responsabiliser les acteurs concernés.

2. - Le rôle de la CNIL

Le rôle de la CNIL est important à double titre. D'une part, elle est garante de la protection des données – c'est même son rôle essentiel. C'est pourquoi elle examine les dossiers qui lui sont soumis avec grande attention, notamment sur les aspects relatifs à la sécurité informatique, aux durées de conservation des données, ou à l'information des personnes. D'autre part, la CNIL est soucieuse de mettre en place une régulation agile plutôt que stricte, c'est-à-dire qu'elle est soucieuse de ne pas imposer des règles trop contraignantes, notamment dans le cadre de l'accès aux données de santé.

Dans ce contexte, la loi permet de faciliter les demandes d'autorisation faites par les demandeurs avec des outils spécifiques, des décisions uniques – qui permettent aux demandeurs de ne pas refaire les mêmes demandes lorsque la finalité est identique –, des accès à des échantillons, et des méthodologies de référence. Il s'agit d'outils proposés par le législateur, dont la CNIL a signifié, dès 2016, qu'elle entendait les utiliser pleinement de façon à faciliter l'accès aux données dans cette même logique de responsabilisation, puisque ces textes, notamment les méthodologies de référence, prévoient un certain nombre d'obligations qui doivent être respectées par le demandeur, à charge pour la CNIL de contrôler le respect de ces obligations. Ces outils s'établissent en coordination avec l'Institut national des données de santé (INDS), le ministère et, de façon générale, l'ensemble des acteurs. Notons que la CNIL a lancé le 30 novembre 2017, et pour trois mois, une consultation publique sur la réécriture des méthodologies de référence auprès de plus d'une trentaine d'acteurs.

Cette régulation agile concerne également l'évaluation des dossiers au cas par cas. Ainsi, par exemple, la loi impose une information individuelle des personnes dont les données sont traitées dans le cadre de projets de recherche ; mais la loi permet aussi à la CNIL de ne pas imposer cette information individuelle lorsqu'il est impossible de retrouver les personnes. Avec cette adaptation, les services de la CNIL développent une lecture pertinente des dossiers pour mieux répondre aux besoins du demandeur.

On rappellera aussi un autre aspect essentiel dans le cadre de la régulation de la CNIL : la rapidité d'instruction des données dans les délais imposés par la loi.

Enfin, il faut souligner que pour être crédible une régulation doit pouvoir s'appuyer sur des outils répressifs offerts par la loi et le règlement. Dans ce contexte, les procédures simplifiées apparaissent comme une forme de responsabilisation dans le domaine de la santé. De sorte que le régulateur est amené à changer l'orientation

de son action pour ne plus la concentrer sur l'examen des dossiers de formalités préalables, mais pour la réorienter en partie sur la réalisation d'audits sur place – la CNIL ayant un pouvoir de contrôle sur place –, car il n'y a que sur site que l'on peut réellement apprécier la façon dont les mesures décrites dans les dossiers sont mises en œuvre – par exemple en matière de sécurité.

Pour l'avenir, il y a donc une réorientation de l'activité de la CNIL vers l'allègement des formalités et le renforcement des contrôles *a posteriori*. Cette approche avait d'ailleurs été préconisée par la Cour des comptes dans son rapport de mars 2016 concernant les données personnelles gérées par l'assurance maladie[138].

S'il y avait un seul mot à retenir, ce serait celui de « confiance ». Il est important que nos concitoyens aient confiance dans l'utilisation de leurs données de santé. Sans cette confiance, on perçoit que le mécanisme ainsi décrit pourrait facilement se gripper. C'est pourquoi le dispositif législatif actuel ou à venir devrait permettre à la CNIL de préserver ce climat de confiance au bénéfice de nos concitoyens.

Pierre-Louis Bras
Inspecteur général des affaires sociales,
président du Conseil d'orientation des retraites (COR),
modérateur de la table ronde

Je me réjouis de constater que les idées des uns et des autres convergent vers les mêmes objectifs. Mais ce n'est pas parce qu'une certaine harmonie règne parmi les intervenants qu'elle est partagée par tous. Le moment est donc venu de laisser la parole au public.

138 Cour des comptes, *Les données personnelles de santé gérées par l'assurance maladie - Une utilisation à développer, une sécurité à renforcer*, communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale, mars 2016.

Échanges avec la salle

Question du public

Il existe aujourd'hui, disponible sur le marché, la possibilité de « tatouer » les images médicales, voire les données personnelles. Cela permet de les suivre, mais aussi d'en annuler l'utilisation si l'intéressé change d'avis. Cette notion de tatouage est un concept nouveau qui, techniquement, est opérationnel, mais vis-à-vis duquel le droit est muet. A-t-on prévu une approche juridique de ce type de concept ?

Thomas Dautieu

Ce que vous décrivez renvoie à un concept du règlement européen, qui est le principe du respect de la vie privée dès la conception (en anglais, « privacy by design ») ; c'est-à-dire que le responsable du traitement doit, dès la conception du programme informatique, mettre en place des dispositifs qui visent à garantir un niveau maximal de protection des données. Aussi, un responsable de traitement mettant à disposition de tiers et dans un cadre légal, par exemple, des données de santé, et qui anticiperait l'exercice d'un droit d'opposition, ou ferait appel à un dispositif technique pour éviter des mésusages, comme par exemple celui du « tatouage », s'inscrit parfaitement dans la philosophie prônée par le RGPD.

Pierre-Louis Bras

Allons plus loin à travers un exemple concret. Gravement malade, vous êtes hospitalisé. À la sortie de l'hôpital vos données de santé sont transférées dans le système national des données de santé (SNDS). À ce moment-là, force est de constater que les patients ont d'autres soucis que de consentir ou pas à l'utilisation de leurs données de santé ; en outre comme il faut bien que le SNDS fonctionne, les informations lui sont transmises d'office. Bien sûr la loi a prévu un pouvoir d'opposition ; de sorte qu'un patient pourrait, après une hospitalisation, demander à ce que celles-ci soit retirées du SNDS. Mais si une telle demande était faite sur une large échelle, elle enlèverait une grande partie de l'intérêt du dispositif informatique qui repose sur son exhaustivité. Dans ce contexte, existe-t-il un risque que ce pouvoir d'opposition, qui semble toutefois plus théorique que pratique, menace le dispositif construit pour le SNDS ?

Thomas Dautieu

Je ne le pense pas, même si dans l'état actuel de la règlementation le patient a en effet un droit d'opposition au SNDS. Notons que l'approche est différente

dans le RGPD et dans la loi « informatique et libertés » de 1978. Dans cette dernière, chacun peut s'opposer à l'utilisation de ses données personnelles pour motif légitime – autrement dit, il faut dire pourquoi l'on souhaite s'opposer à un traitement. Le RGPD, quant à lui, renforce le droit des personnes en « inversant la charge de la preuve » par rapport à la loi de 1978, en considérant que l'on a un droit d'opposition et que c'est au responsable de traitement de dire pourquoi il ne peut pas y faire droit.

Question du public

Dans le domaine des études en vie réelle, il est souvent nécessaire d'enrichir le SNDS avec des données médicales issues d'autres bases de données ; mais comme le NIR a longtemps été quasiment interdit de collecte dans les bases de données on est souvent obligé d'utiliser des méthodes probabilistes, ce qui n'est pas l'idéal. Dans ce contexte, est-ce que lorsque des académies voudront constituer des bases de données médicales dans une pathologie et demanderont à la CNIL l'autorisation de collecter le numéro d'inscription au répertoire national d'identification des personnes physiques (dit « NIR » ou numéro de sécurité sociale), obtiendront-elles cette autorisation ?

Thomas Dautieu

C'est vrai que la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé et les textes pris pour son application permettent maintenant de traiter le NIR. Sur le principe, la CNIL admet dorénavant que le NIR puisse être utilisé pour faire des appariements avec les données qui sont dans le SNDS, mais elle pourra imposer de recourir à un tiers qui, lui, fera la liaison entre les données que vous mettez en œuvre et le NIR pour permettre d'aller faire les requête dans le SNDS.

Dominique Polton

L'avenir du SNDS consiste effectivement dans ce déploiement d'appariements entre les données, notamment cliniques, issues des dossiers médicaux ou des registres et cohortes, et les données administratives qui certes sont pauvres en données cliniques mais ont cette caractéristique fondamentale de pouvoir suivre des patients sur de très longues périodes et à un coût très faible.

Pierre-Louis Bras

Avant la loi de 2016, pour faire ces appariements il fallait un décret en Conseil d'État. Or préparer un décret en Conseil d'État n'était pas la priorité des services du ministère de la santé.

Question du public

Au sujet de l'accès à la base de données du système national inter-régimes d'assurance maladie (SNIIRAM) par les laboratoires pharmaceutiques, il y a l'hypothèse où les pouvoirs publics s'opposent à la consultation des données par les industriels, soit au moment de l'inscription au remboursement, soit au moment de la fixation du prix par le Comité économique des produits de santé (CEPS)[139]*. Comment résoudre cette difficulté ?*

Dominique Polton

Parmi les finalités auxquelles les industriels ont droit – hors l'interdiction de promouvoir leurs produits auprès des professionnels ou des établissements de santé –, il y a en premier lieu celle qui consiste à répondre aux demandes des autorités sanitaires, par exemple de la Haute Autorité de santé (HAS) quand elle demande des études post-inscription dont une partie peut être faite sur les données médico-administratives ou les dossiers du CEPS. Par ailleurs, et sans qu'il y ait forcément de demande explicite, il y a aussi des éléments dont l'industriel a besoin pour préparer son dossier d'inscription. Tout ceci fait partie des finalités licites pour lesquelles les dossiers sont déposés et entrent ensuite dans un processus d'examen et d'acceptation comme les autres, c'est-à-dire avec un jugement sur l'adéquation entre les données demandées, la finalité et la qualité scientifique du dossier, avec à la fin l'autorisation qui leur est accordée.

Question à M. Dautieu

Comment voyez-vous l'effectivité du « droit à la portabilité », qui est un droit nouveau décrit à l'article 20 du RGPD et dont la mise en œuvre risque d'être difficile en regard des besoins d'interopérabilité des systèmes d'information ?

Thomas Dautieu

Ce droit est en effet nouveau et a des conséquences techniques importantes. Notons qu'il a fait l'objet d'une analyse de la part du G29[140] *qui, régulièrement, publie des opinions et des lignes directrices relatives à l'application des textes européens relatifs à la protection des données. Parmi celles-ci, le G29 a adopté des lignes directrices sur la portabilité*[141] *; il s'agit d'un document auquel on peut se référer pour une meilleure compréhension et/ou analyse du RGPD.*

139 Le Comité économique des produits de santé (CEPS) est un organisme interministériel principalement chargé par la loi de fixer le prix des médicaments remboursables par les régimes obligatoires d'assurance-maladie.

140 Le G29 est le nom du groupe de travail qui réunit l'ensemble des « CNIL européennes ». Avec l'entrée en application du règlement général sur la protection des données (RGPD), le 25 mai 2018, le G29 est remplacé par le Comité européen de la protection des données (CEPD) prévu aux articles 68 à 76 dudit règlement.

141 Groupe de travail « article 29 » sur la protection des données, *Lignes directrices relatives au droit à la portabilité des données*, 13 décembre 2016, version révisée et adoptée le 5 avril 2017 (WP 242 rev. 01).

Mais, sans entrer dans les détails juridiques, cette portabilité n'est toutefois pas un droit absolu. C'est un droit limité, notamment sur un certain nombre de bases légales, de sorte que tout le monde ne peut pas s'en prévaloir : un patient, par exemple, n'a pas un droit à la portabilité des données détenues par un établissement de santé.

En revanche, pour ce qui concerne les applications de bien-être, ce droit fonctionne. Ainsi, par exemple, le client d'une application qui enregistre ses données de santé depuis des années (nombre de pas, activité physique, heures de sommeil, etc.) et qui, à un moment donné, se sent captif de cette application et souhaite en utiliser une autre, par exemple plus respectueuse de ses données, peut faire jouer ce droit à la portabilité et récupérer ses informations. Théoriquement c'est donc possible. Ensuite, il faudra vérifier concrètement comment cela se matérialise au niveau des outils informatiques. En tout cas, ce sera une obligation pour les responsables des traitements que de permettre techniquement la récupération de ses données.

Pierre-Louis Bras
Inspecteur général des affaires sociales,
président du Conseil d'orientation des retraites (COR),
modérateur de la table ronde

Je remercie nos trois intervenants pour la richesse de leurs discours qui nous ont permis de mieux comprendre la nouvelle règlementation sur l'accès aux données de santé, et le public pour son écoute attentive et sa participation au débat, et clôture la séance.

L'accès aux données et la protection sanitaire

La loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé entend optimiser des voies d'accès aux données de santé, auparavant considérées comme inutilement restrictives et insuffisamment protectrices de la vie privée. À cette fin, la loi introduit une distinction entre les procédures d'accès aux données de santé selon qu'elles peuvent, ou non, donner lieu à l'identification des personnes auxquelles elles se rapportent.

L'accès aux données anonymisées est désormais libre et gratuit, même si une telle mise à disposition implique le plus souvent un travail préalable de traitement potentiellement long et contraignant pour les détenteurs de ces données. S'agissant des données de santé à caractère personnel, la loi entend ouvrir plus largement leur accès à des fins de recherches ou d'études répondant à un « *motif d'intérêt public* », notamment en simplifiant les procédures d'autorisation par la CNIL et en reconnaissant aux entreprises ou organismes à but lucratif, sous certaines conditions, un droit d'accéder aux données contenues dans le SNDS. Des garde-fous sont érigés, afin de protéger les personnes contre le mésusage qui pourrait être fait des données personnelles de santé dont l'effectivité, eu égard à l'importance des enjeux en cause, mérite d'être examinée.

Sommaire

Biographie des intervenants

Les fonctions mentionnées sont celles exercées à la date de la conférence

Modérateur

François Stasse
Conseiller d'État honoraire, administrateur de l'Institut national de la santé et de la recherche médicale (INSERM)

Docteur en économie, diplômé de l'Institut d'études politiques de Paris, François Stasse entre au Conseil d'État en 1984. Il est par la suite directeur général de l'Assistance publique - Hôpitaux de Paris (1989-1993), directeur général de la Bibliothèque nationale de France (1998-2001), et président de l'Agence nationale de recherche sur le sida (2005-2011). Au sein du Conseil d'État, il est rapporteur général de la section du rapport et des études de 1996 à 1998, puis président adjoint de la section sociale de 2007 à 2017. François Stasse est membre du conseil d'administration de l'INSERM depuis 2016, et membre honoraire du Conseil d'État depuis 2017.

Intervenants

François Bourdillon
Directeur général de Santé publique France

Médecin de santé publique, passé par les plus grandes instances de la discipline (Haut Conseil de la santé publique, Observatoire français des drogues et des toxicomanies, Conseil national du sida, Société française de santé publique, Institut national de veille sanitaire (InVS), et ancien vice-président de Médecins sans frontières), François Bourdillon a été chargé par la ministre de la santé de la préfiguration de Santé publique France, fusion de l'InVS, de l'Institut national de prévention et d'éducation pour la santé (INPES), l'Établissement de préparation et de réponse aux urgences (EPRUS) et d'Addictions drogues alcool info service (ADALIS). François Bourdillon est directeur général de Santé publique France, l'Agence nationale de santé publique, depuis juin 2016.

Patrick Maddalone
Sous-directeur des conditions de travail, de la santé et de la sécurité sociale au ministère du travail

Patrick Maddalone est diplômé de l'Institut universitaire de technologie (IUT) de Marseille Luminy (1990) et de l'Institut national du travail de l'emploi et de la formation professionnelle (INTEFP, formation d'inspecteur du travail, 1994). Après un premier poste de contrôleur du travail à la direction départementale du travail, de l'emploi et de la formation professionnelle d'Annecy, de 1985 à 1988, il effectue la première partie de sa carrière à l'Inspection générale du travail des

transports. D'abord affecté à Lyon comme contrôleur du travail, de 1990 à 1992, Patrick Maddalone est nommé inspecteur du travail à Bourg-en-Bresse en 1994, après sa formation à l'INTEFP, jusqu'en 1997, puis à Paris jusqu'en 2001. Il rejoint alors l'Inspection générale du travail des transports comme chargé de mission puis, en 2006, est nommé secrétaire général adjoint. En mai 2007, il est nommé directeur régional du travail des transports du Centre, avant de revenir à Paris huit mois plus tard comme conseiller technique chargé du dialogue social au ministère de l'écologie, de l'énergie, du développement durable et de l'aménagement du territoire, pendant deux ans. En 2009, il rejoint la direction régionale des entreprises de la concurrence, de la consommation, du travail et de l'emploi de la région Provence-Alpes-Côte-d'Azur (Direccte Paca) comme directeur régional adjoint, responsable du pôle entreprises, emploi et économie, et, en 2012, est nommé commissaire au redressement productif. Patrick Maddalone poursuit ensuite sa carrière à la direction générale du travail à partir de septembre 2016, en tant que sous-directeur des conditions de travail, de la santé et de la sécurité au travail.

Christian Saout
Membre du collège de la Haute autorité de santé (HAS)

Premier conseiller des tribunaux administratifs et des cours administratives d'appel, Christian Saout est volontaire depuis 1993 au sein de AIDES, association française de lutte contre le VIH/Sida et hépatites virales, dont il a été président de 1998 à 2007. Il a été membre des conseils d'administration de l'Institut national de prévention et d'éducation pour la santé (INPES) de 2002 à 2007 et de l'Institut national de la santé et de la recherche médicale (INSERM) de 2009 à 2013, membre du Conseil national du Sida de 2003 à 2007 et président de la Conférence nationale de santé de 2006 à 2010. Christian Saout est, de 2004 à 2009 et depuis 2014, membre du conseil de la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS), et membre du Haut Conseil pour l'avenir de l'assurance maladie (HCAAM) depuis 2004. Il est, par ailleurs, secrétaire général délégué depuis 2012 du Collectif inter-associatif sur la santé (CISS), dont il a été vice-président de 2004 à 2007 et président de 2007 à 2012. Christian Saout est co-auteur du rapport « Pour une politique nationale d'éducation thérapeutique du patient » (2008) et du « Rapport complémentaire sur les actions d'accompagnement des patients » (2010) réalisé à la demande de Roselyne Bachelot, ministre de la santé. Il est également corapporteur de la mission « 2011, année des patients et de leurs droits », auteur du rapport « Cap Santé » en vue des projets d'accompagnement à l'autonomie en santé (2016) à la demande de Marisol Touraine. Il est enfin personnalité associée au Conseil économique, social et environnemental (CESE).

Actes – L'accès aux données et la protection sanitaire

François Stasse
Conseiller d'État honoraire, administrateur de l'Institut national de la santé et de la recherche médicale (INSERM),
modérateur de la table ronde

J'ai l'honneur d'accueillir pour cette séance trois praticiens, trois responsables institutionnels ou associatifs, ayant entre leurs mains ce nouvel outil qui est la loi « santé » de 2016[142] et qui vont nous dire si celle-ci est utile, efficace ou si elle présente des insuffisances – si tant est que nous disposions déjà d'un recul suffisant pour dresser ce premier bilan.

En lien avec les deux premières tables rondes, je rappelle brièvement de quoi nous parlons à travers les données massives médicales françaises que la loi de 2016 nomme le « système national des données de santé » (SNDS). Il s'agit de la réunion de plusieurs outils qui existent depuis longtemps, ainsi que l'a notamment rappelé M. Bras, à savoir le système national d'information inter-régimes de l'assurance maladie (SNIIRAM)[143] géré par la Caisse nationale de l'assurance maladie (CNAM) qui rassemble toutes les feuilles de soin établies par les médecins de ville, le programme de médicalisation des systèmes d'information (PMSI)[144] qui retrace les séjours effectués par les patients à l'hôpital ainsi que les fiches réalisées par les médecins qui établissent les causes médicales des décès. Et l'on peut espérer que, dans un temps ultérieur, ce système rassemblera aussi les données du secteur médico-social, notamment les données concernant les personnes âgées accueillies dans les EHPAD[145] ainsi que les données de l'assurance maladie complémentaire.

Ce système a été qualifié, notamment par M. Bras, de « *système médico-administratif le plus important du monde* ». Cela peut surprendre en France, pays de taille moyenne de soixante-six millions d'habitants, mais cela s'explique très bien pour des raisons à la fois historiques et médicales. Les raisons historiques concernent la tradition jacobine centralisatrice française qui s'est traduite, sur le plan médical et de la santé, par l'unicité de notre système d'assurance maladie. Cette tradition a donc créé un système unique, centralisé, qui a rassemblé une base de données exceptionnellement unique et homogène, d'excellente facture et de grande ampleur qui s'ajoute à la bonne qualité du système de santé français.

142 Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *préc*.
143 Base de données pseudonymisées de consommations de soins ne contenant pas les noms, prénoms, adresses et numéros de Sécurité sociale des assurés, et dont l'accès est réservé à des utilisateurs individuellement habilités pour des finalités d'études dans le cadre de missions de service public ou de recherche en santé.
144 Base de données hospitalières.
145 Établissement d'hébergement pour personnes âgées dépendantes (maison de retraite).

Ce point est essentiel au moment où la révolution technologique a mis à disposition de cette base de données des outils d'une efficacité technique, d'une rapidité et d'une puissance de calcul exceptionnels par rapport à ceux qu'avaient connus les générations précédentes.

Pendant longtemps, ce qui a prévalu, à la fois pour des raisons de sociologie administrative et pour des raisons juridiques de protection du secret médical, est une certaine frilosité dans l'utilisation de ces données ; et c'est ce qui a évolué de manière spectaculaire avec la loi « santé » de 2016. Pour résumer d'un mot l'état d'esprit de ce changement, je citerai l'un de nos plus grands médecins qui a été, pendant de nombreuses années, président du Comité national d'éthique, le professeur Didier Sicard. Il a résumé ainsi le dilemme de nos prédécesseurs : « *il n'y a pas de risque zéro du point de vue de la divulgation du secret médical, mais les risques pour la santé publique d'une non utilisation des données de santé sont bien plus importants* ».

Autrement dit, le bénéfice que nous pouvons potentiellement tirer d'une utilisation intelligente et sous contrôle de ces énormes bases de données, à l'aide de ces très puissants moteurs de recherche dont nous disposons aujourd'hui, est extraordinaire par rapport aux risques qui, bien que non nuls, restent toutefois limités. D'où la réforme de la loi du 26 janvier 2016 qui, sur le plan institutionnel, a confié l'organisation et le traitement du système à la Caisse nationale d'assurance maladie (Cnam) et a créé par ailleurs un groupement d'intérêt public (GIP) : l'Institut national des données de santé (INDS) – dont la directrice Mme Polton est intervenue précédemment – qui veille à la qualité des données et aux conditions générales de leur utilisation – sachant bien sûr que les conditions individuelles sont sous le contrôle et l'autorisation de la Commission nationale de l'informatique et des libertés (CNIL).

Sur le plan de l'accès à ces données – sujet de cette table ronde –, la loi institue une distinction cardinale entre les données sans risque d'identification ou de réidentification qui sont d'accès libre et gratuit, et les données identifiantes ou sous risque important de réidentification parmi lesquelles la loi identifie deux régimes : un régime d'accès permanent qui devient possible pour une liste limitée de services de l'État définis par décret en Conseil d'État avec les garanties habituelles (personnes habilitées, secret professionnel, traçabilité des interventions), et un régime d'accès ponctuel à des fins de recherche, d'étude et d'évaluation répondant à un intérêt public avec des garanties supplémentaires si la demande émane de l'industrie ou du secteur de la banque et de l'assurance ; l'accès dans ce cas là est autorisé par la CNIL après avis d'un comité d'experts indépendants.

Tel est le cadre dont les trois intervenants qui m'entourent sont les utilisateurs. Cadre qui n'a pas recueilli d'objection de la part du Conseil constitutionnel, ce qui signifie que l'on estime globalement qu'un équilibre a été trouvé entre plusieurs objectifs à valeur constitutionnelle que sont le *respect de la vie privée*, notamment le respect du secret médical, et la *protection de la santé* que ces nouveaux outils vont permettre de développer.

Pour évoquer ce sujet, et apprécier si ce cadre est pertinent et présente de nouveaux intérêts, j'ai le plaisir de recevoir trois utilisateurs chevronnés : le docteur François Bourdillon, directeur général de l'Agence nationale de la santé publique (ANSP) qui a notamment en charge la veille sanitaire et la gestion des crises ; M. Patrick Maddalone, sous-directeur des conditions de travail, de la santé et de la sécurité au travail au ministère du travail qui traitera du sujet des autorités en charge des maladies professionnelles et de la santé des travailleurs ; et M. Christian Saout, membre du collège de la Haute Autorité de santé (HAS), présent au titre d'expert de longue date des usagers du système de santé puisqu'il a été auparavant président de l'association AIDES ainsi que président et secrétaire général du Collectif inter-associatif sur la santé (CISS).

La parole est au directeur général de l'ANSP, le docteur François Bourdillon.

François Bourdillon

Directeur général de l'Agence nationale de la santé publique (ANSP)

Merci M. le président. En remarque liminaire, je souhaiterais dire quelques mots sur Santé publique France, l'Agence nationale de santé publique, dont les missions principales sont la veille, l'alerte et la surveillance épidémiologique, la prévention et la promotion de la santé, ainsi que la préparation et la réponse aux menaces, alertes et crises sanitaires.

Pour assurer sa mission de protection de la santé de la population, Santé publique France dispose d'une centaine de bases de données nominatives pour lesquelles elle assure le traitement et la valorisation scientifique et parfois la collecte. Parmi ces bases de données, on peut citer, par exemple, celle qui concerne les urgences sanitaires pour laquelle Santé publique France reçoit tous les matins cinquante mille lignes de données en provenance des urgentistes, ou la base de données de SOS médecins, ou encore celle du système national d'information inter-régimes de l'assurance maladie (SNIIRAM) sur laquelle nous travaillons quotidiennement. Je pourrais également citer la base de données de toutes les déclarations obligatoires qui sont nominatives, mais également nos grandes cohortes, comme par exemple Coset[146], sans oublier les données des registres que nous pouvons si besoin rapprocher des données du PMSI. Tout ceci montre à quel point nous sommes extrêmement concernés par la problématique des données massives.

Dans ce contexte, la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé qui met en place le système national des données de santé (SNDS) a changé les choses[147]. Tout d'abord, nous sommes plutôt satisfaits de la simplification du formalisme lié au traitement des données à caractère personnel. Nous sommes très concernés par cette loi car, comme le rappelait le président Stasse, Santé publique France dispose d'un accès permanent et étendu au SNDS en

146 Dont l'objectif est de mieux décrire et surveiller, au sein des bénéficiaires de la MSA et du RSI, les liens entre facteurs professionnels et problèmes de santé (musculaires, articulaires, psychiques, cardio-vasculaires, respiratoires, cancer, etc.) pour identifier les risques et formuler des recommandations en matière de prévention.

147 Voir également le décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».

vertu de la loi du 26 janvier 2016 qui précise que le SNDS a notamment pour finalité « *de mettre à disposition des données qu'il rassemble (…) afin de contribuer : (…) à la surveillance, à la veille et la sécurité sanitaires* »[148].

En contrepartie de cette loi, il existe un certain nombre d'obligations.

Parmi ces obligations, il y a la désignation d'un correspondant informatique et liberté – dispositif que nous avions déjà mis en place –, la mise en place d'une procédure d'habilitation des personnels pour l'accès aux données du SNDS, et l'établissement d'un registre des études accessible sur demande – tout élément que nous avions déjà anticipé avant la loi « santé » de 2016.

Il faut également tenir compte de la mise en œuvre du règlement européen (RGPD), qui souligne la nécessité de développer une politique de maîtrise des risques liée à l'accès aux traitements et à la valorisation des données. Ceci est un élément très important, car il importe que le citoyen, le malade, accorde sa confiance à l'Agence – qui dispose de données nominatives – dans l'usage de ses données.

Notons que notre objectif, par rapport à la centaine de bases de données dont nous disposons et qui sont pour la plupart dans le SNDS, est clairement de donner du sens, de la valeur, de l'intérêt, aux données dans le cadre de décisions de politiques publiques. C'est un travail important, car il faut bien comprendre qu'au-delà du fait de disposer d'une base de données, il faut également disposer de professionnels (épidémiologistes, statisticiens et gestionnaires de données) pour pouvoir construire des algorithmes, faire des travaux statistiques, analyser les données et leur donner du sens pour *in fine* les publier. Parfois, l'Agence peut être amenée à croiser des bases de données, voire à les chaîner les unes avec les autres, comme par exemple les données des structures mobiles d'urgence et de réanimation (SMUR) avec celles des urgences hospitalières.

Dans ce contexte, il est important pour nous, d'une part, de respecter le droit et, d'autre part, d'appliquer les conditions de la mise en œuvre de la loi. Au sujet du droit, il est très important que tous les aspects « informatique et libertés » soient respectés, que toutes nos études et tous nos travaux, lorsqu'ils sont définis, passent devant des comités de protection des personnes, ou, lorsque les données sont réutilisées pour avis, que l'on passe devant le comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (CEREES), avant l'autorisation de la CNIL.

Pour ce faire, nous nous sommes organisés au sein de Santé publique France pour prendre en compte les nouvelles règles du SNDS :

- d'une part, en créant une direction *ad hoc*, la direction de l'appui, du traitement et d'analyse des données (Data), dans le but de répondre au droit dans ce domaine pour y inclure la qualité, la pertinence et la traçabilité des données. C'est cette direction qui dispose d'un accès permanent et qui a la charge de l'animation du système de données au regard du SNDS ;

148 Ordonnance n° 2016-462 du 14 avril 2016 portant création de l'Agence nationale de santé publique, et décret n° 2016-523 du 27 avril 2016 relatif à la création de l'Agence nationale de santé publique.

- d'autre part, en inscrivant l'Agence dans un processus de qualité et de maîtrise des risques. Le principal risque étant pour le SNDS le risque de rupture de confiance du fait de la perte ou de la divulgation de données.

C'est cette même organisation que nous avons utilisée pour répondre au règlement européen (RGPD). Nous avons mis en place un registre des signalements. Ce registre est déjà en place sous la responsabilité du délégué à la protection des données (DPD)[149], et nous conduisons des travaux pour être en capacité de certifier nos traitements – la certification de nos logiciels au regard des référentiels de sécurité étant dévolue au ministère de la santé – pour mettre en place les codes de bonne conduite pour le bon usage des données ; travail considérable qui demande à être rappelé à l'ensemble des épidémiologistes qui ont toujours envie d'utiliser les bases, de mener des études et de donner du sens à des données.

Je terminerai sur un dernier point, celui de la notion d'intérêt public de l'analyse de nos bases de données. Pour encadrer cette notion, Santé publique France s'est organisée à travers :

- une programmation pluriannuelle définissant un programme de travail à cinq ans ;

- une validation par le conseil scientifique de cette programmation pluriannuelle ;

- un passage devant le comité collégial d'évaluation des projets de toute étude menée par Santé publique France ;

- la révision en interne par les pairs de tout rapport sortant de l'Agence et, lorsqu'il s'agit d'une publication internationale, son référencement à travers les comités de lecture.

C'est là notre garantie d'utiliser au mieux nos données tout en respectant le droit.

Pour conclure, je rappellerai qu'il existe aujourd'hui de nombreux besoins. Nous disposons de données nominatives – donc sensibles – pour répondre à nos missions, en particulier de sécurité sanitaire mais aussi de santé publique. La confiance qui nous est faite amène à une certaine forme de responsabilité vis-à-vis des données, qui est à la fois une responsabilité scientifique, une responsabilité de protection des données et une responsabilité de santé publique.

François Stasse
Conseiller d'État honoraire, administrateur de l'Institut national de la santé et de la recherche médicale (INSERM),
modérateur de la table ronde

Merci beaucoup. Je donne maintenant la parole à M. Maddalone.

149 Le délégué à la protection des données (DPD ou DPO pour « *Data Protection Officier* ») est l'ancien correspondant informatique et liberté (CIL).

Patrick Maddalone
Sous-directeur des conditions de travail, de la santé et de la sécurité au travail au ministère du travail

Je souhaiterais évoquer le volet « travail », qui est peut-être le parent pauvre de ce qui a été évoqué jusqu'à présent dans le cadre du SNDS et de l'accès aux données de santé. Cet éclairage me semble important, car les données que l'on a collectées dans le cadre dit « de santé publique » doivent aussi être mises en regard de toutes celles que l'on collecte dans un autre cadre : celui du monde du travail et de l'activité professionnelle.

Dans ce contexte, et en termes de santé, comment définir l'approche du ministère du travail ?

La première chose à souligner est la responsabilité de l'État en matière de « protection sanitaire », notion à la fois de santé publique et de santé au travail. C'est la raison pour laquelle la politique de santé doit prendre en compte les conditions de vie et de travail des citoyens.

Pour ce faire, une notion importante a été introduite dans le code de la santé publique, aux articles L. 1411-1 et L. 2111-1 : celle d'*exposome*, c'est-à-dire l'intégration sur la vie entière, personnelle et professionnelle, de l'ensemble des déterminants non génétiques qui influent sur notre santé[150].

Cette importance de la traçabilité des expositions tout au long de la vie se retrouve également soulignée dans le troisième Plan santé au travail (PST 3)[151], qui indique les grandes orientations de la politique et de la stratégie du ministère du travail en faveur des conditions de travail. Soulignons qu'il s'agit là d'un document conçu avec les partenaires sociaux, au sein du groupe permanent d'orientation du Conseil d'orientation des conditions de travail (COCT)[152], qui, en 2016, en pleine discussion du projet de loi « travail »[153], ont réussi à trouver un accord unanime sur les lignes directrices et structurantes du PST 3. Ces orientations innovantes, au-delà des trois axes stratégiques principaux définis par le COCT (privilégier la prévention plutôt que la réparation, favoriser la qualité de vie au travail et renforcer le dialogue social), précisent par ailleurs qu'il faut dépasser l'approche segmentée que l'on pouvait avoir des risques, et notamment ne plus avoir cette frontière infranchissable entre la santé publique et la santé au travail.

Enfin, il doit être noté que l'on trouve dans le PST 3, et plus précisément au sein du troisième axe « support », transversal, un objectif qui est la connaissance

150 L'article 1 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé présente le concept d'exposome « *comme l'intégration sur la vie entière de l'ensemble des expositions qui peuvent influencer la santé humaine* ».

151 Ministère du travail, de l'emploi, de la formation professionnelle et du dialogue social, *Plan santé au travail 2016-2020*, téléchargeable sur le site du ministère : https://travail-emploi.gouv.fr/IMG/pdf/pst3.pdf

152 *Ibid*., p. 3.

153 Le projet de loi « travail » visait à instituer de nouvelles libertés et de nouvelles protections pour les entreprises et les actifs. Il a donné lieu à la loi n° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels.

des systèmes de données de santé au travail, et donc la volonté de se poser la question de savoir de quel système d'information nous avons besoin pour intégrer la totalité des données de santé au travail, notamment celles indiquées dans le dossier médical individuel et celles collectées par la médecine du travail (services autonomes ou interentreprises).

1) À ce stade, nous avons là une première opposition entre l'engagement de la responsabilité de l'État et la nécessité que l'État a à avoir connaissance d'un certain nombre de données lui permettant d'agir, ou de réagir, en matière règlementaire. C'est typiquement le cas, par exemple, dans les affaires d'amiante où, en 2004, l'État a été reconnu responsable en raison de sa carence fautive à prendre les mesures de prévention des risques liés à l'exposition des travailleurs aux poussières d'amiante[154]. Il faut donc que l'État prenne en compte ces éléments-là pour ajuster la règlementation et donc les règles pour protéger les salariés, mais en disposant toutefois de données actualisées pour pouvoir (ré)agir ainsi que l'a précisé le Conseil d'État dans un arrêt récent[155] – ce qui signifie que dès que l'État entrera en possession de l'information nécessaire, il aura obligation d'agir pour faire évoluer la règlementation.

Derrière cette première opposition, il y a le respect de la confidentialité des données, celles-ci étant parfois individuelles.

Dans ce contexte, quelle exploitation des données de santé au travail peut-elle être faite par le ministère du travail ?

Le dossier médical en santé au travail[156]

Actuellement, le dossier médical en santé au travail (DMST) est un dossier médical papier, tenu à jour dans chacun des services de santé au travail. Il peut être informatisé, on parle alors de dossier médical informatisé en santé au travail (DIST). Lorsque le salarié change d'entreprise, il doit demander la transmission de ce document à son service de santé au travail.

Notons qu'il existe dans la loi du 8 août 2016[157] la volonté de mettre en place un dispositif de suivi individuel de l'état de santé des salariés, et des modalités particulières d'hébergement des DMST pour les contrats courts[158]. Pour ce faire,

154 CE, Ass., 3 mars 2004, *Ministre de l'emploi et de la solidarité c. consorts Bourdignon et autres*, n°s 241150, 241151, 241152 et 241153.

155 CE, ch. réunies, 31 mars 2017, *Fédération générale des transports et de l'équipement de la Confédération française démocratique du travail*, n° 393190.

156 L'article L. 4624-8 du code du travail précise qu'« *un dossier médical en santé au travail, constitué par le médecin du travail, retrace dans le respect du secret médical les informations relatives à l'état de santé du travailleur, aux expositions auxquelles il a été soumis ainsi que les avis et propositions du médecin du travail, notamment celles formulées en application des articles L. 4624-3 et L. 4624-4. Ce dossier ne peut être communiqué qu'au médecin de son choix, à la demande de l'intéressé. En cas de risque pour la santé publique ou à sa demande, le médecin du travail le transmet au médecin inspecteur du travail. Ce dossier peut être communiqué à un autre médecin du travail dans la continuité de la prise en charge, sauf refus du travailleur. Le travailleur, ou en cas de décès de celui-ci toute personne autorisée par les articles L. 1110-4 et L. 1111-7 du code de la santé publique, peut demander la communication de ce dossier* ».

157 Loi n° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels.

158 Article L. 4625-1-1 du code du travail.

nous avons, au ministère du travail, depuis la publication de la loi, commencé à travailler à la création de ce fichier qui permettrait aux intérimaires changeant de société à la fin de leurs contrats de bénéficier d'un suivi permanent et ne pas avoir systématiquement une remise à zéro de leur exposition professionnelle.

Mais cette approche souligne la nécessité de pouvoir identifier clairement le salarié. Peut-on, par exemple, utiliser le numéro d'inscription au répertoire national d'identification des personnes physiques (NIRPP ou NIR)[159] ou, depuis la réforme de 2016, l'identifiant national de santé (INS) ?[160]

Nous avons, au ministère du travail, regardé attentivement les textes qui ont été publiés, notamment le décret du 27 mars 2017[161]. Nous en déduisons que l'utilisation de l'INS reste difficile dans le cadre de ce que l'on souhaite, c'est-à-dire pouvoir disposer d'un élément nous permettant de suivre un individu donné, quels que soient les emplois occupés et leurs services de santé au travail.

Il doit être noté que le centre interservices de santé et de médecine du travail en entreprise (CISME)[162], rebaptisé PRESANCE[163], qui regroupe la quasi-totalité des services de santé au travail interentreprises (SSTI), a saisi le ministère de la santé au motif que sa lecture des textes l'amenait à considérer que l'on pouvait utiliser l'INS, et donc mettre en place un système national qui permette cette traçabilité.

2) La seconde opposition concerne les partenaires sociaux qui, après avoir participé à l'élaboration du PST 3 dans le cadre du groupe permanent d'orientation du Conseil d'orientation des conditions de travail (COCT), ont décidé de créer un groupe de travail pour réfléchir à l'exploitation des données en santé au travail.

La question est alors de savoir si l'on peut créer un système d'information national des données en santé au travail.

Et l'on voit tout de suite le clivage – c'est la seconde opposition – entre l'avantage d'avoir une traçabilité des expositions à des substances dangereuses pour déterminer si l'activité professionnelle est à l'origine de la maladie décelée par le médecin de santé, et le risque que cela représente pour le salarié dans le cadre des protections actuelles. Ainsi des débats existent, par exemple sur les tests salivaires qui permettent de déterminer si un salarié est sous l'emprise de stupéfiants ; ce qui, en cas de résultat positif, interdit au salarié de conduire tout véhicule de société pour ne pas mettre en danger la vie d'autrui. Mais que faire de ces informations si ces tests salivaires ne sont pas effectués par un personnel de santé ?

159 Également appelé « numéro de sécurité sociale », cet identifiant, composé de treize chiffres et d'une clé de contrôle de deux chiffres, est construit à partir de l'état civil transmis par les mairies.

160 La loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé définit le NIR comme identifiant national de santé (INS).

161 Décret n° 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) comme identifiant national de santé (INS).

162 Le centre interservices de santé et de médecine du travail en entreprise (CISME) est une association à but non lucratif créée en 1942 qui représente quelques 240 services de santé au travail interentreprises (SSTI) auprès des petites sociétés.

163 Depuis son assemblée générale extraordinaire du 16 octobre 2017, le nouveau nom du CISME est PRESANCE. Les lettres composant ce sigle proviennent des mots : prévention, santé, services, entreprises, censés mieux caractériser l'activité des 240 services de santé au travail interentreprises (SSTI).

Un autre danger est le risque de sélection. Par exemple, la règlementation sur la prévention des risques d'exposition aux rayonnements ionisants prévoit notamment des valeurs limites d'exposition (effet doses) et un classement des travailleurs exposés. En ce cas, le salarié doit-il connaître son degré d'exposition avant de postuler chez un nouvel employeur ? Le risque est que si le futur employeur prend connaissance de cette information, il n'embauche pas le salarié. De la même façon, si ce dernier a accès à des informations passées d'exposition à des substances cancérigènes, il y a un risque que le salarié développe une pathologie de type maladie professionnelle qui sera alors imputée au nouvel employeur.

C'est pourquoi, au ministère du travail, nous regardons avec attention les travaux des partenaires sociaux, qui, d'ailleurs, depuis 2016, ont évolué dans leur approche de ces problématiques. Nous sommes ainsi passé du « on ne touche pas à ces données de santé » au « il faut s'en préoccuper, car de très nombreux tiers utilisent déjà ces données de santé ».

N'oublions pas, dans ce schéma, l'arrivée des organismes complémentaires (mutuelles) qui commencent à réaliser des actions de prévention dans les entreprises, et qui disposent également de données de santé, pas forcément utilisées dans une volonté de traçabilité mais plutôt dans une optique plus « commerciale ».

Enfin, le ministère du travail s'intéresse à la stratégie nationale de santé, car le dossier médical partagé (DMP)[164] peut aussi, à notre sens, être un élément nous permettant, s'il comportait un volet professionnel et si l'on pouvait y déposer des éléments concernant l'exposition professionnelle, d'avoir une réelle traçabilité.

En conclusion, il faut souligner qu'il s'agit là d'un sujet important qui reste au cœur des préoccupations du ministère du travail, et qui, également, a fortement évolué dans les mentalités, de sorte qu'aujourd'hui les partenaires sociaux ne semblent plus opposés à aborder cette question.

Bien sûr, le ministère du travail regarde attentivement ce qui se passe au niveau de la santé publique, en rappelant qu'il ne faut pas oublier le volet « travail » qui reste un aspect très important dans l'exploitation des données de santé.

François Stasse
Conseiller d'État honoraire, administrateur de l'Institut national de la santé et de la recherche médicale (INSERM),
modérateur de la table ronde

Merci beaucoup pour votre intervention. La parole est à M. Saout.

164 Le carnet de santé numérique, créé par la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie (article 3), conserve et sécurise les informations personnelles de santé.

Christian Saout
Membre du collège de la Haute Autorité de santé (HAS), président de la commission d'évaluation économique et de santé publique

Merci M. le président. Comme vous l'avez indiqué dans votre discours d'introduction à cette séance, j'évoquerai essentiellement ici le point de vue des associations engagées sur cette question de l'accès aux données de santé et de la protection sanitaire, et non pas celui de la Haute Autorité de santé (HAS) – qui, par ailleurs, est fort consommatrice de ces données, avec d'autres, pour notamment y adosser ses recommandations.

Tout d'abord, j'évoquerai quelques premiers éléments d'appréciation sur ce qui s'est passé après le vote de la loi « santé » de 2016 et l'article relatif au système national des données de santé (SNDS) et au recours au SNDS[165].

1. Des progrès mécaniques mais incertains

1.1. On devrait observer des progrès mécaniques en protection sanitaire avec le rassemblement des bases de données. Assez clairement, il y a un élargissement du périmètre de ce qui est accessible aujourd'hui par rapport à ce qui était accessible hier. Cela devrait donc permettre à la fois d'accéder à plus de données et de les apparier davantage entre elles.

1.2. On devrait aussi avoir mécaniquement des effets grâce à l'élargissement des requêteurs potentiels sur la base de données, y compris *via* les organisations de la société civile – associations « loi de 1901 » et organisations non gouvernementales (ONG) – qui peuvent aujourd'hui accéder à ces données pour les traiter et/ou améliorer les informations nécessaires à leurs plaidoyers. Même certaines assurances complémentaires, qui auparavant n'avaient pas accès à ces données, peuvent y accéder, à condition que cela ne soit pas pour sélectionner les risques, la loi « santé » de 2016 interdisant ce type d'utilisation[166]. En revanche, ces mêmes assurances complémentaires peuvent utiliser ces données pour améliorer la protection sanitaire du groupe humain auquel elles s'intéressent à partir de l'analyse d'un certain nombre de données.

1.3. Un troisième aspect concerne la double approche particulièrement enrichissante de « données ouvertes » et d'« accès régulé ». Récemment, en effet, un certain nombre de données de l'assurance maladie ont été mises en ligne, en libre accès, et sont ainsi accessibles sans condition particulière en dehors de la capacité à requêter sur lesdites bases de données, parfois au travers de documents

165 Selon la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, les accès aux données du SNDS s'effectuent « *dans des conditions assurant la confidentialité et l'intégrité des données et la traçabilité des accès et des autres traitements* » conformément au schéma défini par l'arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé. Voir également le décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».

166 Article L. 1461-1 du code de la santé publique (créé par la loi n° 2016-41 du 26 janvier 2016, article 193).

facilitant ces requêtes et appelés « *data mart* »[167], mais aussi à travers le système – déjà évoqué – de l'accès auprès de l'Institut national des données de santé (INDS) avec la vérification de l'intérêt public de la demande.

1.4. Toutefois cette approche présente des limites pour les acteurs associatifs, ceux-ci ayant une propension particulière à construire des données plutôt qu'à utiliser celles déjà existantes. Des limites apparaissent également car les données existantes reflètent insuffisamment la réalité et restent éloignées du vécu des patients. L'on a donc tendance à aller chercher ou à reconstruire des données, notamment à travers des outils d'enquête spécifiques, qui permettent d'exprimer plus favorablement une préoccupation, par exemple la « qualité de vie », pour laquelle il existe très peu d'informations dans les bases de données publiques.

Un autre aspect du monde associatif est la faiblesse de sa culture en matière de collecte et de traitement des données. Sans doute est-ce dû au fait que les associations ont comme principal objectif des préoccupations d'aide, de soutien, et de collecte de fonds pour la recherche, plutôt que des préoccupations de documentation des faits sociaux autours des personnes qui présentent un intérêt ou dont elles ont la charge. Et aussi sans doute parce que l'on renvoie cette responsabilité à l'État qui étant propriétaire des données est supposé faire ce travail.

Enfin, il faut souligner la faiblesse des moyens financiers des associations de patients ou d'usagers dont le modèle économique ne permet pas de financer des emplois de spécialistes chargés de formuler ces requêtes sur ces bases de données. Le défi est donc de taille pour ces associations, quand bien même existerait cette culture du partage et du traitement des données.

1.5. Des éléments encourageants apparaissent cependant dans le monde associatif, qui montrent que celui-ci commence à s'intéresser plus fortement aux données. On peut ainsi prendre l'exemple du projet intitulé « Moi, patient » dans le domaine de l'insuffisance rénale et qui a commencé à collecter les données à partir de la fin de l'année 2017 sur la qualité de vie des patients, notamment dialysés ; données qui pourront être appareillées avec des données d'hospitalisation et/ou de prise en charge. Il y a également une autre réalisation intéressante dans le domaine du cancer du sein, intitulée « Seintinelles », à travers la création d'une base de données regroupant les informations de vingt-cinq mille femmes. Cette association répond aux questions des personnes, volontaires ou malades, qui la sollicite, et permet de collaborer avec les chercheurs en participant à leurs études à travers la collecte des données personnelles de santé.

La culture de l'accès à la donnée, sans doute acquise dans les associations de lutte contre le sida en raison du phénomène d'épidémie, commence aussi à se développer dans le domaine de la prise en charge d'une pathologie. Dans ce contexte, quelles sont les attentes de protection sanitaire que l'on peut recenser dans le monde associatif ?

167 Un « *data mart* » (en français, entrepôt ou magasin de données) est un jeu de données conçu pour répondre aux besoins spécifiques d'une communauté d'usagers.

2. Les attentes de protection sanitaire sont toujours très fortes parmi les associations

2.1. Pertinence des soins

Les attentes vis-à-vis de la pertinence des soins sont extrêmement importantes. Et cette pertinence peut être fortement améliorée grâce à l'analyse des informations contenues dans les bases de données. En effet, ces informations, présentées notamment par la Fédération hospitalière de France (FHF), révèlent des écarts extrêmement importants, voire surprenants, d'un établissement à l'autre ou d'un endroit à l'autre du territoire, pour des actes chirurgicaux identiques. On constate ainsi, par exemple, que le nombre d'opérations de la prostate en France peut, d'un département à l'autre, à population comparable, varier de un à quatre[168].

Ces informations se révèlent un outil très puissant de la pertinence des soins, comme elles peuvent également être un outil nécessaire à la pertinence des stratégies de soins.

2.2. Pertinence des stratégies de soins

Aujourd'hui, dans un monde où explosent les maladies chroniques, ce qui nous préoccupe c'est la pertinence du parcours de soins. C'est de savoir, par exemple, si telle orientation, à tel moment, à été faite dans l'intérêt du patient. Et le chaînage des données entre une base de données comme celle du Programme de médicalisation des systèmes d'information (PMSI)[169] où l'on a les données hospitalières, et la base de données de ville (anciennement base SNIIRAM[170]) permet de voir si les stratégies de soins sont les plus adaptées. Il s'agit d'outils que nous utilisons à la HAS quand on a des recommandations à faire sur des stratégies de soins, où lorsque l'on a, par exemple dans la commission que je préside, à évaluer économiquement une stratégie de soins.

2.3. Pertinence des actions

L'utilisation de ces informations permet également de cibler des actions, comme par exemple dans le cadre de la lutte contre le sida. Mais, à l'époque, la mise en place de la déclaration des cas de séropositivité, succédant à celle des cas de sida, a soulevé une polémique car elle n'apparaissait pas aux yeux de certains assez sécurisée. Nous avons ainsi perdu deux à trois ans sur une surveillance de l'épidémie qui aurait pu être plus salutaire pour l'ensemble de la nation, avec une

168 Voir : Morgane Le Bail, Zeynep Or (dir.), *Atlas des variations de pratiques médicales – Recours à dix interventions chirurgicales*, publié en 2016 par le ministère de la santé, l'agence technique de l'information sur l'hospitalisation et l'institut de recherche et documentation en économie de la santé (Irdes). Publication téléchargeable sur Internet (www.irdes.fr).

169 Le programme de médicalisation des systèmes d'information (PMSI) a été rendu obligatoire par la loi n° 91-748 du 31 juillet 1991 portant réforme hospitalière. Cet outil a pour but de permettre de décrire, pour évaluation et analyse, l'activité de soins d'un hôpital.

170 Créée par la loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale pour 1999, la base de données SNIIRAM (Système national d'information inter-régimes de l'assurance maladie) contient les données relatives à la santé des assurés sociaux. Elle est mise en œuvre par la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS) aux fins de contribuer à une meilleure gestion des politiques de santé.

capacité à mieux surveiller cette épidémie et sans doute à diligenter les actions utiles là où elles auraient été très fructueuses.

L'utilisation de ces informations permet également de repérer un certain nombre de comportements, notamment si on les corrèle avec des usages alimentaires, ou des phénomènes de circulation des populations, pour adapter les actions.

2.4. Pertinence de l'allocation de ressources

Malgré la mauvaise conjoncture dans laquelle nous sommes plongés, nous avons réussi, en 2017, à respecter l'objectif national de dépenses de l'assurance maladie (ONDAM)[171]. Toutefois, la pertinence des allocations de ressources reste, pour l'administration publique, une préoccupation quotidienne. Et l'accès aux données, notamment des résultats en vie réelle de l'administration de certains produits de santé très onéreux, permet, dans le cas de résultats non probants de revoir les accords de prix conditionnés admis par le Comité économique des produits de santé (CEPS).

2.5. L'exhaustivité des accès à l'information

Dans ce contexte d'attente forte à l'amélioration de la protection sanitaire, il faut noter l'existence d'une limite : le manque d'exhaustivité des accès aux bases de données. En effet, si de nombreuses bases de données ont été intégrées dans le système national des données de santé (SNDS), d'autres en ont été écartées. Il s'agit notamment des bases de données de type « registres » qui existent pour certaines maladies particulières, et dont le support est très souvent une organisation privée de type « loi de 1901 ».

C'est par exemple le cas de la très importante base « Reins », gérée par l'agence de la biomédecine, dont les associations n'arrivent pas à obtenir l'accès, alors même que celui-ci s'avèrerait particulièrement important en France où les chiffres (30 % de greffes et 70 % de dialyse) sont totalement inversés par rapport, par exemple, à ceux de la Grande Bretagne (70 % de greffes et 30 % de dialyse), et alors même que le coût économique de la dialyse est très largement supérieur à celui de la greffe. Si cette base était intégrée au SNDS, cela permettrait d'analyser les données établissement par établissement, contrairement aux informations que nous possédons et dont la granularité régionale ne permet pas d'étudier les comportements d'un établissement à l'autre ; ceci, alors même que l'on aurait besoin de ce type d'approche pour relever le défi d'accès à la greffe de reins.

Dans ce contexte, et face à ces outils puissants de collecte et de traitement de l'information, se pose la question des nouveaux risques encourus par les individus, au-delà des moyens de sécurisation importants mis en place.

171 Créé en 1996, et voté chaque année par le Parlement au moment du vote de la loi de financement de la sécurité sociale (LFSS), l'objectif national de dépenses d'assurance maladie (ONDAM) fixe l'objectif (estimé, mais non plafonné) des dépenses à ne pas dépasser en matière de soins. Pour 2017, le projet de LFSS (PLFSS) fixait le montant de l'ONDAM à 190,7 Md€, en progression de 2,1 % par rapport à 2016.

3. Des risques à surveiller

3.1. Stigmatisation des groupes humains : observance et comportements à risque

Sur la question de l'observance, deux arrêtés[172] ont tenté de moduler le niveau de remboursement des personnes utilisant un masque oxygénant dans l'apnée du sommeil. Le Conseil d'État a annulé ces deux textes, au motif qu'ils n'avaient pas de base légale[173].

Ainsi la tentation existe à partir de la collecte et du traitement des données de santé de vouloir moduler, comme dans l'exemple précédent, un remboursement, ou, demain, observer un comportement à risque pour exiger un changement d'attitude. Toutefois, l'intention peut ne pas être forcément mauvaise lorsque l'on sait, par exemple, que l'observance des médicaments dans l'hypertension artérielle est d'environ 50 %, et que l'on a ici à la fois un intérêt de santé publique à améliorer le suivi de la thérapeutique et un intérêt économique à faire que les prescriptions soient suivies. Comment le faire et jusqu'où aller ? Ce sont là des éléments dont il faut absolument discuter.

3.2. Renforcement des tensions : « savoir pour agir »

Comme l'ont fait remarquer les intervenants précédents, la création du SNDS oblige la puissance publique. Avec la gestion centralisée des données de santé, il est en effet de moins en moins possible d'affirmer « ne pas savoir », au motif que les informations sont éparpillées dans plusieurs bases de données ; de sorte que l'exigence de transparence devient de plus en plus forte.

Dans ce contexte, l'opinion publique et les organisations de la société civile ont, par conséquent, du mal à comprendre que, grâce à ces nouveaux outils technologiques, l'on progresse dans les savoirs, sans agir sur les leviers d'action. Ainsi, par exemple, si l'on reprenait l'enquête de l'assurance maladie menée il y a cinq ans sur les opérations de la prostate, on s'apercevrait que les résultats sont aujourd'hui les mêmes que ceux d'hier. Ce qui signifie que le savoir construit il y a cinq ans n'a pas permis d'engager des actions pour corriger cette situation. Cela constitue à la fois un « échec » et un élément de tension, notamment pour les patients.

3.3. Incompréhension croissante : données *versus* témoignages

Un autre sujet de préoccupation est la montée de l'incompréhension, notamment avec le monde associatif qui, très souvent, produit de nombreux témoignages de patients connaissant des problèmes avec tel ou tel médicament. Il s'agit généralement de témoignages que les associations essaient d'agréger au travers d'éléments chiffrés, alors même que les informations contenues dans les bases de données ne font rien ressortir de tel. D'où l'impossibilité de discuter le problème au fond.

172 Arrêtés du 9 janvier 2013 et du 22 octobre 2013 portant modification des modalités d'inscription et de prise en charge du dispositif médical à pression positive continue pour traitement de l'apnée du sommeil et prestations associées au chapitre 1er du titre Ier de la liste des produits et prestations remboursables prévue à l'article L. 165-1 du code de la sécurité sociale.

173 CE, juge des référés, ordonnance du 14 février 2014, *Union nationale des associations de santé à domicile et autres*, n° 374699 ; CE, 28 novembre 2014, *Union nationale des associations de santé à domicile et autres*, nos 366931, 374202, 374353.

Deux exemples récents permettent de mesurer cette incompréhension. Le premier exemple concerne le médicament Lévothyrox[174] contre lequel les associations ont enregistré de nombreuses plaintes de patients, alors même que rien n'apparaissait dans les bases de données publiques. Ce qui a eu pour effet d'augmenter la tension et l'incompréhension entre les différents acteurs du monde de la santé et les patients. Le second exemple concerne l'implant de contraception définitive Essure[175], sur lequel un certain nombre de femmes ont jugé utile de donner l'alerte – et sans doute à juste raison. Or selon l'Agence nationale de sécurité du médicament (ANSM), il n'y avait aucun élément pouvant corroborer leurs doutes dans les bases de données ; alors même que, quelques mois plus tard, la société pharmaceutique Bayer retirait son produit de la vente en France – ce qui montre que le produit n'était pas dépourvu d'effets secondaires. On voit ici combien cette tension avec la société civile peut trouver à se renouveler.

3.4. Inégalités d'accès aux évaluations des traitements médicaux

Les inégalités face aux traitements sont liées au fait qu'un certain nombre de données, appelées « les données de vie réelle »[176] – c'est-à-dire les données relatives aux effets d'un traitement qui a été prescrit –, ne sont pas recensées dans les bases de données du SNDS et, de ce fait, ne sont pas accessibles, alors même que les personnes sont de plus en plus confrontées à l'introduction rapide sur le marché de très nombreuses innovations thérapeutiques. De sorte que l'on prend actuellement de plus en plus de traitements qui sont encore en fin de phase II, c'est-à-dire toujours à l'étude ; ce qui conduit à prendre un certain nombre de risques sans les surveiller ou les analyser. C'est un sujet de préoccupation à travailler dans le cadre de l'accès aux bases de données.

Conclusion

Dans ce contexte, il faut regarder le monde associatif comme présentant un espoir raisonné, à la fois, de progrès en matière de « démocratie sanitaire » – le savoir permettant l'action –, et de pertinence de la protection sanitaire qui permet de mieux diligenter les actions nécessaires.

Je terminerai cette intervention sur un élément d'alerte – qui, bien que n'ayant rien à voir avec les données publiques collectées par la puissance publique, a, en revanche, tout à voir avec les données privées collectées par la puissance privée. En effet, à quoi cela sert-il d'avoir interdit l'usage des données publiques pour

174 En mars 2017, le laboratoire pharmaceutique allemand Merck présente une nouvelle formule du Levothyrox (médicament indiqué dans la prise en charge des hypothyroïdies et utilisé chaque jour par 2,7 millions de personnes en France) qui, très rapidement, est accusée de provoquer de nombreux effets secondaires.

175 Fabriqué par la firme allemande Bayer, l'implant Essure est un petit ressort souple (4 cm) implanté sous anesthésie locale dans les trompes pour déclencher une cicatrisation qui va les obstruer. En France, plus de mille femmes ont été confrontées à un dysfonctionnement du dispositif entre 2013 et 2017. En septembre 2017, Bayer a stoppé la commercialisation de ces implants en Europe et, en juillet 2018, dans le monde.

176 B. Bégaud, D. Polton, F. von Lennep, *Les données de vie réelle, un enjeu majeur pour la qualité des soins et la régulation du système de santé - L'exemple du médicament*, éd. ministère des solidarités et de la santé, décembre 2017 (rapport public téléchargeable sur les sites : https://solidarites-sante.gouv.fr ou www.ladocumentationfrancaise.fr).

sélectionner les risques dans le monde de l'assurance, dès lors que l'on peut acheter ces mêmes informations aujourd'hui sur Internet ? Et que ceux qui le souhaitent peuvent stratifier une clientèle en fonction des risques. C'est un sujet important sur lequel l'État doit rester attentif. Ceci, sans même mentionner les risques liés au profilage des populations et sur lesquels de nombreux experts – comme par exemple Éric Sadin[177] – se sont déjà prononcés.

François Stasse
Conseiller d'État honoraire, administrateur de l'Institut national de la santé et de la recherche médicale (INSERM),
modérateur de la table ronde

Merci beaucoup. Je me tourne vers M. Bourdillon pour qu'il veuille bien nous préciser ses réflexions sur le risque de « perte de confiance » qu'il a évoqué précédemment. Je vois bien ce risque en cas de fuite d'informations confidentielles au sein même du système, mais ce n'est pas sur ce point que porte mon interrogation. Je souhaiterais faire le lien entre ce que vous avez dit et un article très récent de l'un de vos confrères, le professeur Grimaldi[178] sur la crise du Lévothyrox. J'ai trouvé qu'il avait développé une réflexion très originale en disant que l'on avait mal pris le problème parce que l'on a dit aux premiers patients qui se sont plaints du changement de formule de ce médicament, à l'instar des médecins de Molière, « ce n'est rien, vous avez des vapeurs, il n'est pas possible que vous ayez des effets indésirables puisqu'il s'agit de la même molécule ». Et le professeur Grimaldi, qui est une sommité sur le plan médical, a dit « ce n'est pas ça la réalité, la réalité c'est qu'il y a un vrai problème ». Et le vrai problème il le nomme avec ses collègues l'effet « nocebo », par symétrie avec l'effet « placebo »[179], c'est-à-dire qu'un simple changement de formule ou de présentation du médicament est susceptible de provoquer de véritables réactions négatives chez certains patients – ici sur quelques milliers de patients parmi les centaines de milliers prenant ce médicament contre les troubles de la thyroïde.

Dans ce contexte, mon interrogation par rapport aux bases des données de santé est la suivante : pensez-vous que, parce que nous disposons maintenant d'outils informatiques de collecte et de traitement des informations de santé, nous sommes susceptibles de réagir plus rapidement et plus efficacement en cas de problème, et pouvoir dire de manière pertinente que nous avons repéré de vrais effets négatifs ? Même si, pour des esprits rationnels, le fait qu'il s'agisse d'un médicament ayant la même molécule ne devrait poser aucune complication. De sorte que le problème puisse être pris par le bon bout. Pensez-vous que les nouvelles bases de données vont permettre de créer cet effet positif ?

177 É. Sadin, *La vie algorithmique. Critique de la raison numérique*, éd. L'échappée, Paris, 2015. Voir également du même auteur, aux mêmes éditions : *La Silicolonisation du monde. L'irrésistible expansion du libéralisme numérique* (2016) ; et *L'intelligence artificielle ou l'enjeu du siècle. Anatomie d'un antihumanisme radical* (2018).

178 Le professeur André Grimaldi, diabétologue à la Pitié-Salpêtrière.

179 Voir notamment : X. Bertagna, Ph. Bouchard, A. Grimaldi, J.-L. Wémeau, J. Young et X. Bertagna, Lévothyrox : « Il faudra avoir une expertise sociologique de cette invraisemblable "crise" », *in Le Monde*, 28 décembre 2017.

François Bourdillon

Directeur général de l'Agence nationale de la santé publique (ANSP)

La base de données dont il est question ici est une base de pharmacovigilance. Il s'agit de l'intégration de données sur les effets indésirables d'un produit et la capacité à donner du sens à des signalements. Il convient de tenir compte des délais d'intégration des signalements dans cette base, ainsi que du temps d'analyse.

Dans le cas de l'affaire du Lévothyrox, il s'agissait de signaux très importants car nombreux, mais considérés comme faibles car relevant du registre subjectif. Pour ce qui me concerne, je ne suis pas pharmaco-vigilant, mais je pense qu'il faut avant tout savoir quel sens donner aux signes et, surtout, quelle politique publique mettre en place pour agir.

En tout état de cause, si l'on évoque l'effet « nocebo », il faut aussi parler de l'effet placebo qui montre que parfois un traitement sans aucune substance active peut agir sur le patient. À l'inverse, plus vous avez de patients qui se plaignent, notamment à travers les réseaux sociaux, plus vous avez une caisse de résonnance qui peut amplifier le fameux effet « nocebo ».

Lorsque l'on étudie l'affaire du Lévothyrox, on y découvre des éléments de compréhension : il s'agit d'un produit à marges très étroites où le patient peut facilement être surdosé ou sous dosé et donc présenter des signes de psycho-simulation ou d'apathie. Toujours est-il que, dans ce cas précis, ce n'est pas la base de données de pharmacovigilance qui a parlé, mais la base de données des réseaux sociaux.

Aujourd'hui, il convient désormais d'être à l'écoute du monde des réseaux sociaux, et de savoir donner du sens aux signalements reçus, ce que savent très bien faire, par exemple, les sociologues.

Christian Saout

Membre du collège de la Haute Autorité de santé (HAS), président de la commission d'évaluation économique et de santé publique

Je pense qu'il s'agit là essentiellement d'un problème de communication et d'éducation à la santé. L'enrichissement de la base de données dépend de chacun d'entre-nous, car l'on peut tous saisir soi-même les effets indésirables des médicaments dans une base de pharmacovigilance.

Dans l'affaire du Lévothyrox les personnes ne l'ont pas fait, sans doute parce qu'elles n'avaient pas connaissance de cette possibilité, ou parce qu'on leur avait dit que l'on ne voyait pas pourquoi ce traitement créait des difficultés alors qu'il ne le faisait pas auparavant. Or dès que le site de télé-déclaration de pharmacovigilance a été connu, il a reçu neuf mille déclarations. J'y vois pour ma part la preuve d'un engagement fort des patients. Cela est d'autant plus important que l'on s'oriente vers des médicaments qui, pour des raisons d'innovation, vont arriver de moins en moins « finalisés » devant les patients – sans doute pour sauver des vies, comme

dans le cadre des nouveaux protocoles de soins du VIH il y a vingt ans. Et si nous n'apprenons pas cette « pharmacovigilance citoyenne », qui est une responsabilité que nous devons tous avoir à l'esprit, les bases de données ne pourront jamais restituer ce qu'on ne leur a pas donné en éléments de base et donc produire de la connaissance.

Échanges avec la salle

Question à M. Maddalone

Vous avez évoqué la volonté des partenaires sociaux d'avoir une traçabilité des expositions aux risques encourus par les travailleurs. Je souhaiterais savoir comment, dans le dossier sur la pénibilité au travail[180] *– dont le dispositif a dû être aménagé en 2017 pour exclure quatre facteurs de pénibilité*[181] *–, le ministère du travail a apprécié la complexité de ce dispositif et la charge de travail imposée aux entreprises par rapport aux objectifs de santé publique ?*

Patrick Maddalone

Je pense qu'il existe une confusion entre un dispositif de réparation avec effet de seuil – le « compte pénibilité » ou compte personnel de prévention de la pénibilité (C3P), devenu compte professionnel de prévention (C2P) –, et la difficulté pour les entreprises de savoir si leurs employés dépassent les limites d'exposition fixées par le législateur. Ce dossier a amené les chefs d'entreprises à se poser de très nombreuses questions : que faire en-dessous du seuil ? De la prévention ou choisir de ne rien faire puisque les engagements sont respectés ? Que faire au-dessus du seuil ? Refaire les calculs pour essayer de passer en-dessous et éviter les déclarations ? Entrer dans une logique de réparation ?

Pour avoir participé à de nombreuse réunions sur ce sujet, où les référentiels étaient présentés et discutés par branche d'activités pour aider les entreprises à classer les salariés, on a eu cette confusion assez vite entre l'obligation qui pèse sur tous les employeurs d'évaluer les risques – obligation qui n'a rien à voir avec le « compte pénibilité » –, et le dispositif sur la pénibilité qui vise à réparer une exposition à des facteurs de risques limitant l'espérance de vie du salarié.

Au final, si l'employeur déclare un salarié au titre de la pénibilité, ce dernier aura une traçabilité de ses expositions et pourra s'en prévaloir en fin de carrière pour obtenir réparation.

Selon moi, il faudrait impérativement que l'on puisse, tout au long de la vie professionnelle du salarié et sans se préoccuper des effets de seuils, avoir une historicité de l'exposition à tous les facteurs de risque, y compris ceux qui ont été enlevés par l'ordonnance du 22 septembre 2017[182]*, pour pouvoir faire un lien entre l'activité du salarié et une pathologie qu'il pourrait déclarer.*

180 Loi n° 2010-1330 du 9 novembre 2010 portant réforme des retraites ; loi n° 2014-40 du 20 janvier 2014 garantissant l'avenir et la justice du système de retraites.
181 Ordonnance n° 2017-1389 du 22 septembre 2017 relative à la prévention et à la prise en compte des effets de l'exposition à certains facteurs de risques professionnels et au compte professionnel de prévention.
182 *Ibid*.

Je rappelle aussi que sur le nouveau compte professionnel de prévention (C2P), les dix facteurs sont toujours maintenus[183]*. On demande en effet au chef d'entreprise de faire de la prévention sur ces dix facteurs, sinon dans certains cas une pénalité peut s'appliquer ; sachant qu'il y a six facteurs qui continuent de faire l'objet d'une déclaration*[184] *et que les quatre autres font l'objet d'une réparation dans le cadre d'une déclaration de maladie professionnelle avec un taux d'incapacité permanente (IPP) d'au moins 10 %.*

Au sujet de la traçabilité, il doit être noté que la ministre du travail et la ministre des solidarités et de la santé ont confié, le 10 novembre 2017, au professeur Frimat[185] *une mission sur l'exposition aux agents chimiques dangereux pour déterminer de quelle façon l'on pouvait avoir cette traçabilité*[186]*. Pour ma part, je reste convaincu que la solution réside dans une exploitation des données de santé qui sont actuellement à la disposition des médecins du travail et qui ne sont pas aujourd'hui utilisées.*

Question du public

Je souhaiterais savoir jusqu'où peut aller le caractère intrusif du retour de ces informations de santé ? Je pense, par exemple, à l'identification des facteurs de risques pour telle personne ou groupe de personnes, avec une immixtion de la personne publique dans la vie de chaque citoyen en le prévenant, ou en le faisant prévenir par un professionnel de santé, ou encore en essayant d'entrer dans une logique de prévention qui serait très proactive et donc très intrusive. Quelle est aujourd'hui l'approche de ces questions ? Dans quels domaines ? Court-on un risque ou existe-t-il un intérêt de santé publique à ce que l'exploitation des bases de données de santé conduisent à des approches qui pourraient être très intrusives, voire particulièrement attentatoires à la liberté ou à la responsabilité personnelle ?

François Bourdillon

Aujourd'hui, la plupart des banques de données permettent de classer des groupes, des comportements à risque, ou des personnes exposées à certains facteurs spécifiques et, en conséquence, de construire une politique de santé

183 Dix facteurs de risques professionnels sont regroupés sous trois catégories (article L. 4161-1 du code du travail) : 1) Contraintes physiques marquées : manutentions manuelles de charges ; postures pénibles définies comme positions forcées des articulations ; vibrations mécaniques ; 2) Environnement physique agressif : agents chimiques dangereux, y compris les poussières et les fumées ; activités exercées en milieu hyperbare ; températures extrêmes ; bruit ; 3) Certains rythmes de travail : travail de nuit dans les conditions fixées aux articles L. 3122-2 à L. 3122-5 ; travail en équipes successives ; travail répétitif caractérisé par la réalisation de travaux impliquant l'exécution de mouvements répétés, sollicitant tout ou partie du membre supérieur, à une fréquence élevée et sous cadence contrainte.

184 Seuls six facteurs sont à déclarer par l'employeur : les activités exercées en milieu hyperbare, les températures extrêmes, le bruit, le travail de nuit, le travail en équipes successives alternantes et le travail répétitif.

185 Paul Frimat, professeur universitaire et praticien hospitalier de l'université de Lille.

186 P. Frimat (dir.), *Mission relative à la prévention et à la prise en compte de l'exposition des travailleurs aux agents chimiques dangereux*, éd. ministère du travail, Paris, septembre 2018 (téléchargeable sur le site Internet de La documentation Française : www.ladocumentationfrancaise.fr).

publique. Nous sommes ainsi en mesure de préciser, par exemple, quelle catégorie de personnes fume ou consomme beaucoup d'alcool, et d'agir en conséquence.

Les nouvelles stratégies de bases de données, comme la bio-surveillance menée depuis quelques années au sein de Santé publique France visent, par exemple, à doser les toxiques (chimiques ou issus des métaux) dans le sang des personnes. Et l'on arrive à restituer, en fonction d'expositions professionnelles ou en habitat – c'est-à-dire en air intérieur –, une corrélation entre ce type d'exposition et l'existence de ces substances toxiques. Objectivement, lorsque l'on passe devant les comités de protection des personnes (CPP)[187] *on est obligé de dire que si l'on trouve des résultats inquiétants, par exemple trop de plomb chez un enfant, on doit agir pour que cet enfant ne soit plus exposé à ce type de substance. C'est le côté vertueux de cette approche, aspect qui ne donne pas lieu à débat ni ne change la vie des personnes concernées. Mais dans d'autres systèmes, par exemple touchant aux substances psycho-actives, il pourrait y avoir dans les résultats d'analyse certaines connotations « perverses » qui pourraient se retourner contre les principaux intéressés. Au final, tout cela pose des questions de consentement, de droit légal et de qualité d'analyse du CPP.*

Question à M. Bourdillon

Ne serait-il pas pertinent de revoir notre conception des registres, tels qu'on les fabrique en France, maintenant que l'on dispose des socles de données pouvant remplir une partie des besoins ? Autrement dit, pourrait-on concevoir les registres de données avec des professionnels de santé comme étant des socles très minimaux de données, mais que l'on arrive à apparier très largement avec les données médico-administratives pour en faire, à travers une politique plus harmonisée, des outils beaucoup plus puissants et aussi plus réactifs, tant l'on est frappé de constater une hétérogénéité des conditions d'accès et de gouvernance, mais aussi, d'une certaine manière, une incapacité à agréger ces registres lorsqu'on a besoin de résultats globaux ?

François Bourdillon

La plupart des registres sont sur des cohortes qui sont suivies dans le temps, menées sur des initiatives individuelles hospitalières ou associatives, et inscrites dans des temporalités extrêmement différentes et qui peuvent, selon les régions, avoir des définitions de données variables, ou différentes, d'un territoire à l'autre. Il est donc très important, à partir du moment où la puissance publique finance ces registres, qu'il existe un minimum de cahier des charges.

Il y a aussi la question de la propriété des données qui est très importante. Si, par exemple, demain, une association dépose son bilan, à qui appartient la base de données ? Peut-on la récupérer et l'utiliser ? Il faut savoir que la France a une politique des registres très inférieure à celle de beaucoup de pays européens,

187 Voir les articles L. 1121-1 à L. 1126-11 du code de la santé publique.

et que de telles données sont indispensables pour redresser les données du système national inter-régimes d'assurance maladie (SNIIRAM) et faire en sorte que l'on ait des prévalences et des incidences – par exemple s'agissant des cancers – réparties sur l'ensemble du territoire, alors que l'on ne dispose que d'une douzaine ou d'une vingtaine de registres sur l'ensemble du territoire.

C'est pourquoi ces registres pourraient intégrer à terme le SNDS. Et l'on devrait les considérer, à partir du moment où ils sont financés par les pouvoirs publics, comme une propriété intellectuelle des pouvoirs publics. C'est ce que l'on a fait pour les centres nationaux de référence (CNR)[188] *qui collectionnent l'ensemble des souches virales ou bactériennes de manière à ce que ces souches, très importantes sur le plan génotypique, puissent être conservées en tant que propriété de l'État.*

Christian Saout

Je suis persuadé que l'on peut faire beaucoup mieux avec nos registres, notamment en termes d'harmonisation ou de socle commun obligatoire, mais je pense qu'il faut le faire avec les initiateurs de ces registres, car c'est très souvent un travail intuitu personae – untel avec un sens de l'engagement très poussé ayant réussi à créer un registre dans le domaine pédiatrique, de l'accouchement, etc. Il ne faut donc pas que ces personnes se sentent dépossédées ou écartées de leurs travaux par un cahier des charges dans lequel ils auront du mal à se reconnaître.

S'agissant de l'exploitation des données de santé qui menacerait la liberté individuelle, j'y vois, comme tout le monde, un grand risque potentiel de perte de confiance. Il faut donc savoir dans quel esprit l'on collecte toutes ces données ; sachant que, pour ce qui nous concerne, c'est évidemment dans un esprit d'optimisation de nos politiques publiques. J'évoquais la tentation française de vouloir contrôler les niveaux de remboursement, ou les comportements. Nous sommes en effet dans un pays riche qui consacre beaucoup d'argent au système de soins, à l'assurance maladie ; c'est probablement pour qu'il se déploie de manière optimale, mais c'est aussi probablement pour que, lorsque nous sommes face à un risque personnel, il soit en situation de pouvoir nous aider à traiter ce risque et à y mettre fin, c'est-à-dire à aller mieux ou à guérir. Mais nous ne ferons pas non plus de soixante millions de Français soixante millions de gens vertueux qui s'alimenteront à l'eau plate et consommeront force fruits et légumes, viande blanche ou poisson. Nos vies sont ce qu'elles sont, et malgré les risques que nous prenons nous n'avons pas envie de nous retrouver contrôlés de quelque manière que ce soit. Je pense qu'il faut être extrêmement vigilant avec ces questions-là, car elles sont fortement présentes dans notre quotidien et reviendront régulièrement se poser avec les progrès technologiques.

188 Les centres nationaux de référence (CNR) sont des laboratoires localisés dans les établissements publics ou privés de santé, d'enseignement ou de recherche, qui aident Santé publique France dans ses missions de surveillance des maladies infectieuses.

On évoquait précédemment la pénalisation. Il est vrai qu'en matière de santé publique la sanction fonctionne assez bien, mais la générosité fonctionne également ! Il existe ainsi des stratégies qui, au lieu de diminuer le remboursement, consistent à donner des bons, ou des actions positives à des personnes pour qu'elles deviennent observantes à quelque chose. Et il est assez singulier que le premier acte de la puissance publique voulant favoriser l'observance était un acte pris dans la catégorie « pénalisation » plutôt que celle de « soutien et encouragement ». C'est assez symptomatique de notre état d'esprit collectif.

François Stasse
Conseiller d'État honoraire, administrateur de l'Institut national de la santé et de la recherche médicale (INSERM),
modérateur de la table ronde

Merci M. Saout de ces précisions fort opportunément rappelées. J'ajoute que personne n'a oublié les statistiques surprenantes que vous avez évoquées sur la diversité des pratiques médicales d'un département à l'autre – départements comparables – et qui présentent, par exemple, une différence de un à quatre dans la pratique chirurgicale de la prostate. C'est là une situation d'autant plus incroyable que l'État se donne énormément de mal pour réduire tout gaspillage en la matière, fut-ce au détriment du personnel hospitalier ou des patients.

Dans ce contexte, on peut donc sans doute légitimement imaginer que les futurs ministres de la santé attendent avec impatience la mise en place d'un nouvel outil informatique qui pourrait gommer ces différences étonnantes et passer, si je reprends l'exemple précédent, peut-être à une différence de un à un entre départements, ou à tout le moins tendre vers ce résultat. C'est là un travail que la France peut et doit finaliser.

Je remercie encore une fois nos trois intervenants pour leurs propos passionnants et le public pour sa participation active au débat, et lève la séance.

Le secret médical partagé

Les contours de la notion d'équipe de soins, périmètre à l'intérieur duquel le partage des informations relatives au patient n'exige pas de recueillir son consentement préalable, a été profondément réformée par la loi « santé » du 26 janvier 2016 en vue de favoriser les partages de données entre les différents soignants. D'une part, alors qu'auparavant le partage ne se réalisait qu'au sein d'une équipe de soins constituée dans un même établissement de santé, une telle équipe peut désormais comprendre des soignants relevant de différentes structures d'accueil, entraînant un déplacement des frontières du secret médical. D'autre part, le partage des données ne concerne plus uniquement la prise en charge sanitaire du patient, mais peut désormais porter sur des informations de nature médico-sociale et sociale (conditions d'hébergement, environnement familial, etc.).

La mise en œuvre de cette réforme, qui accompagne la relance du dispositif du dossier médical personnel, qui devient le dossier médical partagé (DMP)[189], devrait favoriser un rapprochement salutaire des secteurs sanitaires et médico-social et participer ainsi d'un décloisonnement de la prise en charge des patients. Cette réforme suscite néanmoins des craintes légitimes au regard des atteintes qu'elle est susceptible de porter au respect du secret médical.

Sommaire

189 Le dossier médical partagé (DMP) est un carnet informatique sécurisé créé à l'initiative de chaque patient qui rassemble l'ensemble de ses informations médicales. Il est accessible aux professionnels de santé autorisés.

Biographie des intervenants

Les fonctions mentionnées sont celles exercées à la date de la conférence

Modérateur

Pascale Fombeur
Présidente de la 1re chambre de la section du contentieux du Conseil d'État

Diplômée de l'Institut d'études politiques de Paris, ancienne élève de l'École nationale d'administration, Pascale Fombeur intègre le Conseil d'État en 1994, au sein de la section du contentieux, puis de la section sociale. Elle y exerce ensuite les fonctions de coresponsable du centre de documentation en 1998 et 1999, de commissaire du Gouvernement auprès de la 1re sous-section du contentieux de 2000 à 2003, et de secrétaire générale adjointe chargée de la gestion des tribunaux administratifs et des cours administratives d'appel, de 2003 à 2007. En 2007, elle devient directrice des affaires civiles et du sceau au ministère de la justice. Réintégrant le Conseil d'État en 2010, elle y est nommée présidente de la 1re chambre de la section du contentieux en 2013. Elle est par ailleurs membre du conseil d'orientation de l'Agence de la biomédecine.

Intervenants

Anne Laude
Professeure, doyenne de la faculté de droit de l'université Paris-Descartes, codirectrice de l'Institut droit et santé

Agrégée des universités, Anne Laude est actuellement professeure à l'université Paris-Descartes, codirectrice avec Didier Tabuteau de l'Institut droit et santé, ainsi que doyenne de la faculté de droit de l'université Paris-Descartes. Elle est également directrice du master 2 droit des industries des produits de santé de l'université Paris-Descartes et professeure à l'Institut d'études politiques de Paris en droit de la santé. Elle est directrice scientifique du Lamy « *Droit de la santé* » et auteure de nombreux ouvrages en droit de la santé, dont *Les droits des malades* avec Didier Tabuteau (éd. PUF, coll. *Que Sais-je ?*, 2016).

Agnès Martinel
Conseillère à la 2e chambre civile de la Cour de cassation

Titulaire d'une maîtrise en droit et ancienne élève de l'École nationale de la magistrature, Agnès Martinel est nommée auditeur de justice en 1988. Elle occupe successivement les fonctions de juge au tribunal d'instance de Béthune (1990-1992), au tribunal de grande instance de Bobigny (1992-1998), puis au tribunal de grande instance de Paris (1998-2002). Elle est nommée conseillère référendaire à la chambre sociale de la Cour de cassation en 2002, et est détachée auprès du Conseil d'État en 2011 en qualité de maître des requêtes. Depuis 2015, Agnès Martinel est conseillère à la deuxième chambre civile de la Cour de cassation.

Jacques Lucas
Vice-président du Conseil national de l'ordre des médecins

Au Conseil national de l'ordre des médecins (CNOM), le docteur Jacques Lucas a assuré successivement les fonctions de président de la section de l'exercice professionnel, puis de secrétaire général de l'institution. Il est, depuis juin 2007, vice-président du Conseil national, délégué général au numérique. Dans cette dernière fonction, il a été l'auteur de nombreux rapports du CNOM portant sur la déontologie médicale et, en particulier, de huit livres blancs dans le domaine des nouvelles technologies de l'information et de la communication (NTIC) en santé : Informatisation de la santé (2008) ; Télémédecine (2009) ; Dématérialisation des documents médicaux (2010) ; Déontologie médicale sur le *web* (2011) ; Vadémécum télémédecine (2014) ; Santé connectée (2015) ; Information, communication, réputation numérique, publicité (2016) ; Médecins et patients dans le monde des *data*, des algorithmes et de l'intelligence artificielle (2018). Un cours en ligne ouvert à tous (*Massive Open Online Course* ou *MOOC*) est en préparation en 2019 sur l'exercice professionnel et la déontologie médicale.

Actes – Le secret médical partagé

Pascale Fombeur
Présidente de la 1re chambre de la section du contentieux du Conseil d'État,
modératrice de la table ronde

Les précédentes tables rondes nous ont permis d'entrevoir toutes les potentialités que recèlent les données de santé existantes et d'évoquer leur utilisation dans un intérêt collectif. La présente séance, que j'ai le privilège et le plaisir de présider, nous ramène au patient lui-même et à la communication des données qui le concernent dans l'intérêt de sa propre prise en charge.

Nous allons donc, lors de cette dernière table ronde, porter notre attention sur l'utilisation des données de santé, mais au profit du patient lui-même.

Comment, en effet, cette communication des données de santé doit-elle être conciliée avec cet élément fondamental de la relation entre le médecin et son patient qu'est la protection, le respect du secret médical ?

Nous savons que le secret médical est inhérent à l'exercice même de la médecine. Déjà, le serment d'Hippocrate[190] au Ve siècle avant Jésus-Christ énonce : « *tout ce que je verrai ou entendrai au cours du traitement, ou même en dehors du traitement, concernant la vie des gens, si cela ne doit jamais être répété au-dehors, je le tairai, considérant que de telles choses sont secrètes* »[191]. Cette formule inspire le serment qui est prêté aujourd'hui par les jeunes médecins. Pour autant, même s'il trouve son origine dans le colloque singulier entre le patient et son médecin, le secret médical est avant tout « institué dans l'intérêt des patients » ainsi que le rappelle le code de déontologie médicale[192].

Dès lors, ce secret, qui vaut même entre médecins, ne doit pas se retourner contre le patient lui-même. Dans l'intérêt de sa prise en charge médicale, il doit pouvoir connaître des atténuations. Dès le code de déontologie médicale de 1947[193], des cas de communication d'informations couvertes par le secret médical sont envisagés. Ainsi, si un malade vient voir spontanément un médecin consultant ou un médecin spécialiste, celui-ci doit chercher à s'enquérir auprès du malade du nom de son médecin traitant, afin – dit le code de déontologie – de lui faire part

190 Hippocrate de Cos (vers 460-377 av. J.-C.), médecin grec et philosophe, considéré comme le « père de la médecine ».

191 Serment médical d'Hippocrate, traduit par J. Jouanna, *Hippocrate*, éd. Fayard, Paris, 1992.

192 « *Le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi. Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris* ». Code de déontologie médicale, article 4 (article R. 4127-4 du code de la santé publique).

193 Le premier code de déontologie médicale a été publié le 28 juin 1947 (décret n° 47-1169 du 27 juin 1947 portant code de déontologie médicale).

de ses observations et éventuellement de la possibilité d'une intervention, sauf opposition du malade[194].

De même, toujours dans le code de 1947, on voit que si le malade fait appel, en absence de son médecin habituel, à un second médecin, celui-ci doit informer le médecin habituel de l'évolution de la maladie pendant son absence[195].

En cas de prise en charge collective, notamment en milieu hospitalier, la jurisprudence de la Cour de cassation – dont Mme Martinel nous parlera – permet également de longue date un certain partage de l'information[196]. Le Conseil d'État, dans une décision de section de 1972[197], adopte une position similaire dans le cas d'un centre médical géré par une fédération de sociétés mutualistes : bien sûr, il résulte du code pénal que c'est du malade seul que dépend le sort des secrets qu'il a confiés à un médecin, ou que celui-ci a pu déduire de son examen, mais, dans le même temps, lorsqu'un malade s'adresse à un organisme qui pratique la médecine collective c'est, dit cette décision, « *nécessairement à l'ensemble du personnel médical de cet organisme que, sauf prescription particulière de la part de ce malade, le secret médical est confié* ».

La loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé conforte ces principes jurisprudentiels, en introduisant dans le code de la santé publique l'article L. 1110-4, déjà évoqué précédemment, qui rappelle l'étendue du secret médical et traite de la question du secret médical partagé. Ainsi, « *Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant.*

Excepté dans les cas de dérogation, expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tout professionnel de santé, ainsi qu'à tous les professionnels intervenant dans le système de santé.

Deux ou plusieurs professionnels de santé peuvent toutefois, sauf opposition de la personne dûment avertie, échanger des informations relatives à une même personne prise en charge, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible. Lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe. (…) ». Telle est la disposition prévue par la loi du 4 mars 2002. La suite de l'article prend en compte le développement des échanges électroniques de données personnelles de santé entre professionnels.

194 Article 43, dont la méconnaissance a été reconnue comme une faute professionnelle (CE, sect., 8 juin 1956, *Amestoy*, Rec. p. 240).
195 Article 57, code de déontologie médicale de 1947.
196 Voir par exemple : C. cass., 1re Civ., 12 février 1963, pourvoi n° 98 ; C. cass., 1re Civ., 26 mai 1964, pourvoi n° 276.
197 CE, sect., 11 février 1972, *Sieur Crochette*, n° 76799, Rec. p. 138.

Deux hypothèses sont ainsi envisagées. La première correspond à l'échange d'informations entre deux ou plusieurs professionnels, avec l'accord, ou du moins l'absence d'opposition, du patient ; ces professionnels sont des professionnels de santé, mais pas nécessairement des médecins. La seconde hypothèse correspond au partage du secret médical par une même équipe de soins dans un établissement de santé ; cette fois-ci il y a une présomption d'accord du patient.

L'exposé des motifs de la loi du 4 mars 2002 souligne à cet égard que la médecine moderne est en effet devenue très souvent une affaire d'équipe, et les informations sont nécessairement partagées, dans l'intérêt du malade, entre membres d'une équipe médicale et, plus largement, entre les professionnels de santé qui prennent en charge une personne. Les travaux parlementaires montrent le souci de prendre en compte les évolutions dans les modes de prise en charge des soins, marquées notamment par la spécialisation, par la nécessité de conforter les réseaux de soins, par le caractère collectif de la prise en charge hospitalière, où interviennent de plus en plus des équipes pluridisciplinaires. La bonne transmission de l'information est en effet devenue un enjeu majeur pour assurer l'efficacité et la continuité de la prise en charge.

Peut-on, dans ce même but, partager le secret médical avec des personnes qui ne seraient pas des professionnels de santé ? Le Conseil d'État a été confronté à cette question dans un contexte très particulier, celui de la santé en milieu carcéral, à l'occasion d'un recours contre une circulaire de 2012 sur le partage d'informations entre professionnels[198]. Dans ce contexte, il a été amené à vérifier de façon très fine que les informations communiquées étaient bien nécessaires à l'accomplissement par l'administration pénitentiaire des missions que la loi lui confie, qui incluent notamment la protection de l'intégrité physique des personnes détenues, et il a, de même, rappelé que ces informations devaient être communiquées aux seuls professionnels ayant besoin d'en disposer à cette fin[199].

Si, fort heureusement, dans l'immense majorité des cas le contexte est très différent, c'est toutefois le même questionnement qui est présent : celui de la nécessité ou non – la loi du 26 janvier 2016 de modernisation de notre système de santé utilise même la notion de « stricte nécessité » – de communiquer certaines informations à des professionnels qui interviennent en dehors du champ médical pour assurer la meilleure prise en charge de la personne[200]. Et l'enjeu est d'autant plus fort qu'il s'agit, pour beaucoup, de personnes fragiles ou vulnérables : enfants, personnes handicapées, personnes âgées en perte d'autonomie, etc. Le médecin n'est pas seul à intervenir, le relais doit être assuré avec l'ensemble des professionnels qui participent à la prise en charge de la personne, que ce soit à l'hôpital, mais aussi de plus en plus à domicile, ou en établissement social ou médico-social.

198 Circulaire interministérielle n° DGS/MC1/DGOS/R4/DAP/DPJJ/2012/94 du 21 juin 2012 relative aux recommandations nationales concernant la participation des professionnels de santé exerçant en milieu carcéral à la commission pluridisciplinaire unique (CPU) prévue par l'article D. 90 du code de procédure pénale ou à la réunion de l'équipe pluridisciplinaire prévue par l'article D. 514 du même code et au partage d'informations opérationnelles entre professionnels de santé et ceux de l'administration pénitentiaire et de la protection judiciaire de la jeunesse.

199 CE, ssr, 22 octobre 2014, *Section française de l'Observatoire international des prisons*, n° 362681.

200 Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, articles 92, 96 et 193.

C'est dans cet esprit que la loi du 26 janvier 2016 innove en proposant une conception élargie de l'équipe de soins et, plus encore, en étendant la possibilité d'échanger des informations de santé, au-delà des seuls professionnels de santé, avec tous les professionnels qui participent à la prise en charge du patient. En complément, elle rénove le dossier médical personnel, qui devient un « dossier médical partagé »[201], et ouvre également aux médecins la possibilité de consulter le « dossier pharmaceutique » du patient[202].

Pour aborder toutes ces questions, j'ai le privilège d'avoir à mes côtés trois intervenants. C'est d'abord vers Mme Anne Laude, professeure agrégée, doyenne de la faculté de droit de l'université Paris Descartes où elle dirige le mastère de droit des industries des produits de santé, et codirectrice de l'institut droit et santé, que je me tournerai pour qu'elle nous présente les innovations de la loi de 2016 et nous en expose les enjeux. Mme Agnès Martinel, conseillère à la deuxième chambre civile de la Cour de cassation, après avoir été conseillère référendaire à la chambre sociale, puis maître des requêtes en service extraordinaire au Conseil d'État, mettra ensuite en perspective les apports de la loi de 2016 grâce à l'éclairage de la jurisprudence tant civile que pénale sur ces questions. Et, enfin, le docteur Jacques Lucas, qui s'investit au Conseil national de l'ordre des médecins depuis de très nombreuses années, et qui en est le vice-président depuis 2007 et le délégué général au numérique, nous apportera le regard du praticien en évoquant les attentes et les interrogations de ses confrères, ainsi que les travaux engagés par le Conseil national de l'ordre pour aider les professionnels dans la mise en œuvre de la loi et de ses décrets d'application.

Je donne la parole à Mme Laude.

Anne Laude

Professeure, doyenne de la faculté de droit de l'université Paris-Descartes, co-directrice de l'Institut droit et santé

Merci Mme la présidente. L'histoire du secret médical a suscité des interprétations diverses. Tantôt il est regardé comme un principe fondateur de l'art médical, notamment par les tenants de la continuité de la morale médicale depuis Hippocrate, et tantôt, au contraire, il est analysé comme une obligation professionnelle formalisée tardivement en France par le code pénal en 1810.

Le secret médical a évolué au gré des transformations de notre système de santé, mais il s'est néanmoins imposé comme la pierre angulaire de la relation médicale. La loi du 4 mars 2002 a inscrit, dans la partie législative du code de la santé publique consacrée aux droits des personnes malades, le principe du secret médical auquel elle a donné d'ailleurs une nature juridique nouvelle puisque, de devoir du médecin, le secret médical, ou plus exactement le secret des informations, est devenu un droit du malade.

201 *Ibid*., articles 95 et 96.
202 *Ibid*., article 97.

Dans le même temps, pourtant, la loi de 2002 a consacré – ce qui peut paraître paradoxal – la notion de « secret partagé », parce qu'elle a pris en compte finalement les limites du colloque singulier ; les limites à la fois pour le malade lui-même, qui peut souhaiter un accompagnement par ses proches, ou par sa personne de confiance, et les limites pour l'équipe de soins qui a besoin de recourir au secret partagé.

Ultérieurement, d'autres textes, comme par exemple la loi n° 2007-293 du 5 mars 2007 réformant la protection de l'enfance, ont également permis le partage de l'information médicale au sein d'une équipe pluridisciplinaire dans un autre domaine. Puis, progressivement, différents textes sont venus décliner les principes liés au partage des données de santé dans toute une variété de secteurs médicaux et sociaux – je songe ici, par exemple, à la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, ou à la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, dite loi « HPST ».

Cependant, ces différents textes, qui ont prévu le régime du secret médical partagé dans le domaine social ou sanitaire, ne prévoyaient rien quant au régime du secret médical partagé dans le secteur médico-social. Il n'y avait donc dans ce secteur aucun cadre législatif. De sorte que, pour le partage ou l'échange de données personnelles dans ce secteur, concernant notamment les personnes âgées ou handicapées, il était fait application notamment des principes contenus dans la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Il y avait donc une différence de régime selon les secteurs. Et à l'heure où la continuité des soins entre la ville, l'hôpital et le secteur médico-social n'est plus à démontrer, à l'heure où les (nouvelles) formes d'organisation de la médecine, les changements de la pratique médicale ou la possibilité de prendre en charge des patients par des acteurs pluridisciplinaires et nombreux sont effectives, à l'heure où la maîtrise des dépenses de l'assurance maladie est comptée, à l'heure, enfin, où il est nécessaire de disposer de données permettant la garantie de l'efficacité et la permanence du système de santé, la loi « santé » de 2016 apportait une modification de taille en instituant un décloisonnement et la mise en place d'une meilleure coordination entre professionnels de santé – mais pas seulement – qui suppose un plus grand partage d'informations et des supports appropriés.

La loi « santé » de 2016 a introduit ces modifications essentiellement par deux dispositions : en modifiant les conditions du partage de données, et en refondant le dossier médical personnel qui est devenu le dossier médical partagé (DMP).

À l'époque, l'objectif du législateur était d'assurer l'homogénéité de l'échange et du partage des données de santé par le biais de la modification de l'article L. 1110-4 du code de la santé publique. Ce texte, issu de la loi de 2016, a fait l'objet d'une correction, notamment d'erreur matérielle, par l'article 5 de l'ordonnance du 12 janvier 2017 ; l'erreur consistant dans le fait que la rédaction du texte en 2016 conduisait à exclure les établissements de santé, les laboratoires de biologie médicale ou encore les hôpitaux des armées du partage et de l'échange du secret médical, alors qu'auparavant ils étaient soumis à cette obligation. L'ordonnance de

2017 corrige donc cette erreur rédactionnelle et rend le dispositif cohérent avec l'objectif poursuivi par le législateur.

Pour ce qui concerne les supports, on notera que la loi « santé » de 2016 a redéfini les contours des supports appropriés à l'extension du partage d'informations en redéfinissant le dossier médical partagé dans les dispositions des articles L. 1111-14 et suivant du code de la santé publique.

Antérieurement, le législateur avait certes posé le principe d'un dossier médical personnel pour chaque patient. Cependant, ce dispositif initial avait été subordonné par un système qui pouvait apparaître comme dissuasif, puisque le niveau de prise en charge des actes et des prestations de soins par l'assurance maladie était en réalité conditionné par l'autorisation ou non que le patient donnait à l'accès de son dossier. Cela a contribué peut-être – mais ce n'est sans doute pas la seule raison – à l'échec du dossier médical partagé (DMP), auquel la loi « HPST » a tenté de remédier mais sans succès. Gageons que la loi « santé » de 2016, qui substitue au dossier médical personnel le dossier médical partagé, y parvienne davantage.

Alors précisément, quelles sont les nouvelles modalités de ce secret partagé ?

On notera que le premier paragraphe de l'article L. 1110-4 du code de la santé publique pose les principes du droit au respect de la vie privée et du secret des informations concernant la personne. Mais, alors qu'antérieurement ce principe se limitait au secteur sanitaire, la loi « santé » de 2016 – c'est la nouveauté – contribue à élargir ces principes à l'ensemble des professionnels et des établissements, qu'il s'agisse des établissements du secteur médico-social ou des professionnels sanitaires, sociaux ou médico-sociaux. Le secret des informations va donc couvrir, non seulement, la prise en charge dans le secteur sanitaire, mais aussi les informations de la prise en charge dans les autres secteurs sanitaires et médico-sociaux.

Par ailleurs, l'arrêté du 25 novembre 2016[203] a distingué, comme la loi – et notamment l'article L. 1110-4 – le commandait, l'échange du partage des données. L'échange de données consiste, en fait, à communiquer des informations à un ou plusieurs destinataires qui sont clairement identifiés par un émetteur connu. En revanche, le partage de données va beaucoup plus loin puisqu'il consiste à mettre à disposition d'une catégorie de professionnels, fondés à en connaître, des informations. Le partage se traduit donc bien par la mise à disposition, par exemple sur une plateforme informatisée, d'informations relatives à un même patient pris en charge.

L'accès des professionnels à cette base de données doit répondre à un certain nombre de conditions que l'on va analyser. Mais la loi « santé » de 2016, et plus spécialement l'article L. 1110-4, prévoit un certain nombre de points communs entre l'échange et le partage de données.

203 Arrêté du 25 novembre 2016 fixant le cahier des charges de définition de l'équipe de soins visée au 3° de l'article L. 1110-12 du code de la santé publique.

Tout d'abord, la loi précise et élargit le nombre de professionnels qui sont susceptibles d'échanger ou de partager les informations. Le décret du 20 juillet 2016[204] liste ainsi une catégorie de personnes considérées comme professionnelles, qui vont pouvoir partager des informations avec les professionnels de santé. La liste est longue. Je ne la déclinerai pas dans sa globalité, mais l'on peut citer, par exemple, les ostéopathes, les chiropracteurs ou les assistants maternels. De manière un peu plus spécifique, sont visés également les particuliers accueillant des personnes âgées ou handicapées – ce qui interroge car il ne s'agit pas vraiment là de « professionnels ». Inversement, on se demande pourquoi les aidants, par exemple, ne sont pas visés par le texte si la catégorie des particuliers accueillant des personnes âgées ou handicapées est visée. Comme on le voit, la liste est longue et pose un certain nombre de difficultés, mais elle reste *a priori* limitative.

L'autre point commun dans la loi « santé » entre l'échange d'informations et le partage des données vise, cette fois-ci, les informations qui peuvent être partagées.

Le texte énonce, qu'il s'agisse de partage ou d'échange, que les professionnels qui participent à la prise en charge d'une même personne peuvent échanger ou partager des informations relatives à la personne, à condition qu'il s'agisse d'informations « *strictement nécessaires à la coordination ou à la continuité des soins* »[205]. Le décret du 20 juillet 2016 précise que la notion d'information strictement nécessaire doit se comprendre dans le sens où il ne s'agit que des informations qui sont dans le périmètre de la mission des professionnels concernés. Autrement dit, ce périmètre, s'il est important, risque de poser un certain nombre de difficultés puisque, précisément, c'est aussi pour l'élargir que l'on veut permettre le partage d'informations entre les professionnels de santé et ces autres professionnels. De sorte que la délimitation précise de ce qu'est leur champ d'activité professionnelle – les seules informations « strictement nécessaires » – risque de poser un certain nombre de difficultés.

Le législateur pose aussi un autre point commun entre l'échange d'informations et le partage des données, puisqu'il prévoit un droit d'opposition, aussi bien dans l'un que dans l'autre cas, avec une difficulté quant à l'effectivité de ce droit d'opposition pour le patient qui, pris en charge à un moment de sa vie où il est particulièrement perturbé, aura sans doute d'autres soucis que de demander à ce que soit écrit noir sur blanc le fait qu'il s'oppose au partage d'informations.

Ces points communs étant précisés, le législateur fixe ensuite le régime entre l'échange d'informations et le partage des données.

L'échange d'information est possible sous réserve qu'il s'agisse de professionnels qui partagent de manière effective à la prise en charge du patient des informations « strictement nécessaires » à la coordination, ou à la prévention et à son suivi. Et le législateur précise le régime juridique de ce partage d'informations en indiquant que, bien évidemment, le patient doit être informé préalablement à cet échange

204 Décret n° 2016-994 du 20 juillet 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel.
205 Article L. 1110-4, II, du code de la santé publique.

d'informations. Mais ensuite le consentement n'est pas exprès, il s'agit simplement d'un consentement présumé.

En revanche, le régime juridique du partage d'informations est, quant à lui, distinct dans la mesure où il obéit notamment à un régime différent, selon qu'il y a ou non une équipe de soins. C'est la grande nouveauté de la loi « santé » de 2016 que d'avoir défini, pour la première fois, ce qu'est une équipe de soins. L'équipe de soins est entendue ici comme un ensemble de professionnels qui réalisent, non seulement, un acte de diagnostic thérapeutique, mais aussi de compensation du handicap – puisque l'on vise d'autres secteurs que le seul secteur sanitaire –, de soulagement de la douleur, ou de prévention de la perte d'autonomie.

Plus précisément, le législateur a précisé trois manières d'appréhender l'équipe de soins.

La première manière est que l'on parle d'équipe de soins lorsque des professionnels exercent dans un même établissement de santé, qu'il s'agisse d'un établissement sanitaire, médico-social ou social. Autrement dit, l'équipe de soins se définit ici au regard du critère de l'unicité d'appartenance à un même établissement – et le décret d'application fixe une liste d'établissements à laquelle je renvoie.

La deuxième manière d'appréhender la notion d'équipe de soins, c'est finalement le patient lui-même qui pourra la déterminer – la qualité de membre de l'équipe de soins pouvant être reconnue par le patient lui-même, qui peut ainsi s'adresser à un certain nombre de personnes. Cependant, le législateur n'a pas laissé toute liberté au patient. Il n'a autorisé que l'intégration des professionnels dans cette équipe à laquelle le patient va pouvoir s'adresser pour la réalisation d'un certain nombre d'actes, qui sont des consultations ou des actes prescrits par un médecin auquel il a confié sa prise en charge. Le choix par le patient de son équipe de soins ne peut donc se faire que dans ce cadre précis.

Enfin, la troisième manière d'appréhender la notion d'équipe de soins, et donc du partage de l'information entre ces personnes, est le partage qui peut exister entre professionnels d'une même structure. Pour répondre à l'exigence ici d'une organisation formalisée, il n'est pas nécessaire d'avoir recours à la création d'une personne morale *ad hoc*. Cependant, l'arrêté du 25 novembre 2016[206] a précisé que l'équipe de soins, par exemple, pouvait être une équipe de soins dans le cadre du programme « territoire de santé numérique » de régulation du SAMU[207] ou une équipe de soins réalisant des opérations transfusionnelles.

L'équipe de soins ainsi définie devra opérer un partage d'informations, ou respecter des règles différentes selon que l'information est partagée entre les membres d'une même équipe ou en dehors de l'équipe de soins. Entre les membres de l'équipe de soins, le principe est simple : on informe toujours le patient et le consentement est présumé. En revanche, lorsque le partage d'informations se fait en dehors de l'équipe de soins, le principe que le législateur a posé requiert

206 Arrêté du 25 novembre 2016 fixant le cahier des charges de définition de l'équipe de soins, *préc.*
207 Le Service d'aide médicale urgente (SAMU) organise le traitement des urgences en dehors de l'hôpital.

son consentement préalable obligatoire, lequel peut être donné par tout moyen, notamment dématérialisé.

Par ailleurs, le législateur prévoit que le consentement est valable tant qu'il n'a pas été retiré, qu'il doit être strictement limité à la durée de la prise en charge et qu'il doit être pertinent et non excessif.

On notera également que dans les cas plus fréquents où les informations – susceptibles d'être partagées – du patient sont hébergées par un tiers, la situation se complique. En effet, la loi « santé » de 2016, en application des dispositions de l'article L. 1111-8 du code de la santé publique, prévoit précisément que, alors que la personne devait initialement donner son consentement express, désormais ce consentement disparaît au profit d'une formule qui se veut plus souple, puisque le texte vise désormais que « *l'hébergement (…) est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime* ».

L'obligation pour la personne de justifier son opposition à l'hébergement des données de santé pour un motif légitime va donc renforcer la contrainte qui pèse sur les personnes dont les données sont traitées – ce que l'on peut regretter et qui risque d'exposer les droits et libertés individuelles des patients à un certain nombre de menaces.

Par ailleurs, pour permettre ce partage d'informations, le législateur a modifié le cadre juridique du dossier médical partagé (DMP), puisqu'antérieurement chaque professionnel qui entendait consulter ce DMP devait obtenir le consentement du patient. Désormais, depuis 2016, il suffit d'avoir un consentement initial à l'ouverture du DMP pour que « *chaque professionnel de santé, quels que soient son mode et son lieu d'exercice, reporte dans le dossier médical partagé, à l'occasion de chaque acte ou consultation, les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge* »[208]. Bien évidemment, cette disposition facilite le partage des données de santé, sauf pour un type d'acteur – ce qui est assez paradoxal alors que l'on voulait unifier le régime sanitaire et médico-social –, puisqu'il est prévu à l'article L. 1111-6 du code de la santé publique que le médecin coordinateur, visé au code de l'action sociale et des familles, dans les établissements d'hébergement pour personnes âgées, devra au contraire toujours demander, et être autorisé au cas par cas, pour consulter le dossier médical partagé. On peut donc regretter ici que la coordination que l'on voulait fixer au régime du partage des données de santé n'ait pas été poussée jusqu'à son terme.

Au final, le volume des données personnelles qui peuvent désormais être partagées est plus important et le cercle des personnes qui peuvent partager ces données s'est lui-même considérablement élargi. Ce qui *a contrario* signifie que les personnes soumises au secret médical partagé sont plus nombreuses, ou que le secret médical est dilué.

L'appréhension des nouvelles dispositions législatives sur le secret médical partagé soulève un certain nombre d'interrogations. Je n'en citerai que quelques unes.

208 Article L. 1111-15 du code de la santé publique.

La première interrogation que l'on peut souligner est que l'analyse du DMP montre que les problématiques relatives au secret professionnel, jusqu'ici consacré sur la relation médecin-patient, vont se déplacer vers des questions de protection des données informatiques. Par ailleurs, ce que l'on peut souligner c'est que le régime, qui voulait unifier les règles en matière de partage et d'échange d'informations à tous les secteurs, aboutit à une certaine complexité juridique ; complexité accrue, par exemple, par le fait – et cela est quelque peu paradoxal – que lorsque les informations sont fournies à un hébergeur de données de santé, le consentement exprès n'est plus possible. En revanche, ce que le texte demande, c'est la présence d'un médecin pour vérifier les données qui sont hébergées. Ainsi, dans le même temps, on veut bien élargir le partage entre des professionnels qui ne sont plus seulement des professionnels de santé, mais on considère que seul un médecin peut être garant des informations qui sont hébergées.

Soulignons une autre difficulté qui est la protection de la confidentialité des données vis-à-vis des tiers non autorisés. Cela risque d'être une question cruciale. Peut-être que l'évolution des techniques, comme par exemple la « *blockchain* »[209], pourra, d'ici quelques années, nous aider et nous rassurer sur la protection de cette chaîne d'informations.

Mais pour le moment, dans le contexte actuel, le danger est de générer une dissémination des données de santé à tous les professionnels. Certes, cette dissémination peut être garante d'une meilleure prise en charge du patient, mais elle soulève des questions dans ses limites et, surtout, dans les atteintes qu'elle peut porter à l'effacement du secret médical. Plus généralement, les nouvelles dispositions de la loi « santé » de 2016 peuvent nous conduire à nous interroger sur la notion même de « secret médical ».

À l'origine, la doctrine établissait un lien entre secret médical et colloque singulier. Ce secret a été, depuis longtemps, élargi et considéré comme le privilège d'une profession. Or, désormais, le partage des données représente un élargissement considérable des frontières du secret médical. Ce n'est donc plus la qualité de l'information qui permettra, demain, d'appréhender et de définir le secret médical, mais davantage la qualification donnée à l'information. Le grand enjeu du futur sera donc d'assurer et de garantir la confidentialité de ces informations et de ces données. C'est de cette garantie dans le système d'information que dépendra la confiance des patients dans notre système de santé.

Pascale Fombeur
Présidente de la 1re chambre de la section du contentieux du Conseil d'État,
modératrice de la table ronde

Merci pour cette présentation très claire des dispositions du nouveau régime juridique et des enjeux et questions qu'il soulève. On voit la subtilité de la loi qui recherche un équilibre entre l'impératif de protection de la personne et l'utilisation de ses informations médicales qui sont nécessaires à son suivi.

209 La « *blockchain* » ou chaîne de blocs est une technologie informatique qui permet de stocker et de transmettre des informations de façon sécurisée, transparente et sans organe central de contrôle.

Je me tourne maintenant vers Mme Martinel pour qu'elle nous explique les répercussions que ces nouvelles dispositions peuvent avoir sur la jurisprudence du juge pénal et du juge civil, et nous montrer à la lumière de cette jurisprudence les enjeux de toutes ces questions.

Agnès Martinel

Conseillère à la 2e chambre civile de la Cour de cassation

Merci Mme la présidente. je souhaiterais en effet présenter les répercussions de la loi « santé » de 2016, que Mme Laude vient de nous décrire, sur une jurisprudence qui, pour l'instant, n'existe pas. C'est-à-dire que je vais me livrer, dans cette intervention, à un exercice de « jurisprudence fiction ».

Pourquoi une telle approche ? Tout simplement parce que la loi date du 26 janvier 2016 et que ce sont d'abord les juridictions du fond qui sont saisies. Or la plupart des contentieux étant à charge d'appel, ils n'arriveront à la Cour de cassation qu'en 2018-2019.

Quelques mots d'abord sur l'évolution de la jurisprudence de la Cour de cassation. Cette évolution est intéressante car l'on y retrouve beaucoup d'éléments évoqués lors des tables rondes précédentes.

La question du secret médical a été posée à la Cour de cassation dès la fin du XIXe siècle, dans une affaire qui concernait le médecin du peintre Jules Bastien-Lepage[210], le docteur Watelet[211]. Cet arrêt a posé le principe d'un secret médical absolu, qui ne connaît aucune exception ou dérogation[212]. Et la chambre criminelle qui, pendant tout le début du XXe siècle, sera essentiellement saisie de ce type de procès maintiendra cette position extrêmement rigide consistant à dire que ce secret protège un intérêt public, mais pas des intérêts privés, et qu'il ne peut en aucune manière y être dérogé. Aucune excuse n'est admise, et même si le médecin n'a pas eu d'intention de nuire l'infraction d'atteinte au secret médical est constituée.

La première brèche sur cette jurisprudence est portée, en 1992, par la réforme du code pénal[213]. À l'époque, se pose la question délicate des informations qui doivent être divulguées dans l'intérêt des autorités judiciaires ou médicales. La loi pose deux exceptions : l'une pour les cas où elle *impose* aux médecins de révéler un secret, et l'autre pour les cas où elle *autorise* cette révélation. Puis, au début des années 1990, on va assister à un assouplissement de plus en plus grand, lié au fait que la chambre criminelle de la Cour de cassation n'est plus la seule chambre qui est saisie d'affaires de secret médical ; et l'on commence à voir des chambres civiles

210 Jules Bastien-Lepage (1848-1884), peintre naturaliste français.

211 C. cass., Crim., 19 décembre 1885, *Watelet*, Pal. 1886, I, 176, rapport Tanon, D.188.I347.

212 Poursuivi par le Parquet pour avoir enfreint l'article 378 du code pénal de l'époque (1810), et condamné en première instance, puis en appel, le docteur Watelet se pourvoit en cassation. La Cour rejette son pourvoi en précisant dans ses attendus que la disposition de l'article 378 « *est générale et absolue et qu'elle punit toute révélation du secret professionnel sans qu'il soit nécessaire d'établir à la charge du révélateur l'intention de nuire* ».

213 Le code pénal de 1810 a été remplacé par un nouveau code pénal le 1er mars 1994.

qui sont saisies parce ce que se pose la question du respect du secret médical vis-à-vis de l'assureur – qui est aussi une des grandes questions posée à la Cour de cassation.

À cette époque, on assiste donc à un changement de paradigme dans la jurisprudence. Le secret médical n'est plus lié à un intérêt public, mais vient protéger l'intérêt du patient. Toute cette jurisprudence sera ensuite très bien retranscrite dans la loi du 4 mars 2002[214] qui pose le principe d'un secret médical dont le but est de protéger l'intérêt du patient.

Toute cette jurisprudence des chambres civiles est en permanence maintenue, et elle a comme pivot essentiel le consentement du patient. C'est-à-dire que le secret peut être levé et partagé si l'on a ce consentement qui, d'ailleurs, peut s'exprimer sous diverses formes.

On notera qu'ensuite, à partir de 2002, s'annonce l'ère du partage des informations avec la loi du 4 mars 2002[215] qui crée une première avancée sur cette question. Puis, le monde judiciaire est ensuite confronté à la loi du 5 mars 2007 réformant la protection de l'enfance[216] avec les premières expériences de partage des informations qui seront beaucoup plus élargies. Enfin, en 2016, une nouvelle loi[217] vient entériner tout ce qui a été fait auparavant en élargissant le champ des professionnels soumis au secret médical, en arrivant à un système qui me semble à la fois très réfléchi et très abouti puisqu'il pose toutes les conditions et toutes les nuances de ce que peut-être la jurisprudence de la Cour de cassation n'avait pas su déceler auparavant – mais nul n'ignore que c'est chaque fois que se pose une situation particulière que la jurisprudence avance pas à pas.

Aussi, après ce qui vient d'être brillamment précisé par Mme Laude, je retiens de la loi « santé » de 2016 trois points qui, selon moi, pourront avoir une influence directe sur la jurisprudence de la Cour de cassation.

- Le premier constat est que ce texte, non seulement, ne modifie pas la conception de la loi du 4 mars 2002 qui fait du secret médical un droit pour le patient, mais encore l'amplifie avec un système qui vient conforter le droit à opposition. Et nous verrons que toute la jurisprudence à laquelle je faisais précédemment allusion sur la question du consentement du patient à la délivrance de l'information restera, selon moi, le pivot de la jurisprudence des chambres civiles, notamment en ce qui concerne le lien avec l'assureur, l'employeur – dont on parlait dans la table ronde précédente –, et les experts, car se pose aussi la question du partage du secret médical lorsqu'un litige est en jeu et que viennent s'opposer au secret médical tous les principes des droits de la défense, notamment le principe du contradictoire qui veut que toutes les parties puissent avoir accès aux pièces du dossier.

214 Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, dite loi « Kouchner ». Cette loi place le malade au centre de toutes les décisions qui le concernent. Voir également le décret n° 2006-6 du 4 Janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique (dispositions règlementaires).
215 *Ibid*.
216 Loi n° 2007-293 du 5 mars 2007 réformant la protection de l'enfance.
217 Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

- Le deuxième point concerne essentiellement la jurisprudence de la chambre criminelle de la Cour de cassation. En effet, le texte de la loi « santé » de 2016 élargit le champ des dépositaires du secret. C'est une réalité qui, au regard de la jurisprudence de la chambre criminelle, aujourd'hui sur l'incrimination d'atteinte au secret professionnel, peut avoir un risque d'élargissement du champ de la répression, c'est-à-dire que plus l'on partage ce secret, plus l'information circule, et plus les dépositaires du secret sont nombreux et plus le risque de répression est important. Je décrirai ensuite quelle est la jurisprudence de la chambre criminelle – pour l'instant assez restrictive – de l'incrimination, qui peut avoir des risques d'évolution vers une extension de la répression.

- Le troisième et dernier point – qui rejoint un peu ce qui a été dit auparavant – montre que s'il existe un élargissement des dépositaires, les conditions de l'échange et du partage sont définies de manière très stricte. Pour préciser ces aspects, je vous donnerai quelques pistes, car la jurisprudence de la Cour de cassation, qui semble faire l'objet d'un renouveau aujourd'hui, a déjà pris en compte, depuis quelques temps, cette question de la nécessité de l'information médicale. C'est-à-dire que, certes, il peut y avoir partage, ou échange, mais encore faut-il que l'échange de l'information soit nécessaire à la situation en cours.

Secret médical, respect de la vie privée et consentement du patient

Nous sommes là dans le cas du partage consenti, qui est une jurisprudence de la Cour de cassation depuis le début des années 1990. L'arrêt fondateur date du 3 janvier 1991 de la première chambre civile de la Cour de cassation[218] et concerne les médecins conseil des compagnies d'assurance. À l'époque, se posait la question de savoir, lorsqu'un assuré avait remis volontairement des documents médicaux au médecin conseil de la compagnie d'assurance, si celui-ci avait autorisé le médecin conseil à utiliser ces documents et à les divulguer. La réponse de la première chambre civile a été claire et assez ouverte en 1991, puis l'on note ensuite un resserrement comme si la première chambre civile avait vu que peut-être elle était allée trop loin.

Dans un premier temps, en 1991, la première chambre civile a considéré que le simple fait de remettre ces documents était en réalité une renonciation volontaire – qui est presque une renonciation présumée – à se prévaloir du secret médical. Ainsi, en remettant les documents, le patient, d'une certaine manière, autorise le médecin conseil de la compagnie d'assurance à les utiliser.

On perçoit qu'après, dans l'évolution postérieure, la première chambre civile – ainsi que la deuxième chambre civile qui a eu des contentieux à traiter – a un peu restreint son obligation puisqu'elle a considéré que tout cela était strictement subordonné à la renonciation de l'assuré. Elle n'a donc pas clairement précisé si la renonciation devait être expresse ou tacite : quand elle est expresse il n'y a aucune difficulté, mais quand elle est tacite tout va dépendre des circonstances relevées dans le dossier.

218 C. cass., 1re Civ., 3 janvier 1991, pourvoi n° 89-13.808.

Si jamais cette renonciation n'est pas constatée, la seule solution dont dispose le juge dans un contentieux d'assurance est de désigner un expert. Mais la Cour de cassation n'a pas autorisé non plus les experts à utiliser tous les documents, et elle considère que le patient peut toujours s'opposer à la remise des documents à l'expert. Dans ces cas-là, l'impasse dans laquelle se trouve la juridiction est résolue par une autre façon de voir les choses, c'est-à-dire que la juridiction doit tenir compte des éléments qui figurent dans le contrat d'assurance et des déclarations qui ont été faites pour en tirer toutes les conséquences sur le litige, mais sans que les documents n'aient été divulgués ou partagés.

Cette jurisprudence a certainement vocation à se maintenir. On sent qu'elle a aussi infiltré tout le droit de la sécurité sociale, puisque l'on sait, par exemple, qu'en matière de prestations la deuxième chambre civile a énoncé le principe selon lequel le simple fait de demander des prestations sociales n'implique pas la levée du secret médical. Cela paraît évident, pourtant il y a eu des plaideurs qui ont soulevé ce principe devant la Cour de cassation. Et l'on peut dire que, de ce point de vue, la loi « santé » de 2016 n'aura pas vraiment beaucoup d'impact sur la jurisprudence de la Cour de cassation, et se maintiendra avec ce pivot de la renonciation au secret médical.

La question du partage élargi

Cet aspect concerne le champ pénal. Jusqu'à présent, la chambre criminelle de la Cour de cassation considère que toute personne qui reçoit une confidence dans l'exercice de la profession n'est pas, pour ce motif-là, tenue au secret professionnel. Pour ce faire, la chambre criminelle utilise depuis des années le concept de « *confident nécessaire* ». Ainsi, faut-il que cette divulgation fasse de ladite personne le confident nécessaire.

Jusqu'à présent cette jurisprudence a été très contenue. On a ainsi, par exemple, écarté la responsabilité d'un journaliste qui avait divulgué une information parce que l'on ne savait pas si elle provenait d'un professionnel de santé. Dans cette hypothèse, la responsabilité pénale n'a pas été retenue. Notons cependant le fait que la loi « santé » de 2016 accumule les secrets qui seront soumis notamment aux professions médico-sociales – un secret professionnel et un secret médical qui va entourer les données de santé qui seront divulguées –, ce qui peut laisser penser que les incriminations seront plus nombreuses et qu'inévitablement le champ de la répression s'élargira.

La question du partage encadré

De ce point de vue, la loi a respecté un certain équilibre dans la mesure où elle a élargi le champ des professionnels concernés. Je pense même qu'elle a restreint le champ des informations qui peuvent être échangées. Le terme « *strictement nécessaire* » me paraît à cet égard un progrès par rapport au texte précédent.

On peut également préciser que la Cour de cassation a, depuis un certain temps, une jurisprudence qui prend en compte cette nécessité. En 1997, la première chambre civile avait admis, dans un procès qui concernait le respect de l'obligation de

concurrence entre des médecins dans une clinique, que l'expert chargé d'examiner tous les documents concernant l'activité desdits médecins, dans l'instance en cours, alors que le principe du contradictoire s'appliquait, ne communique pas à la procédure le nom des patients de ces médecins.

Elle a donc, dans une certaine proportionnalité, appliqué le secret médical en admettant que des informations soient communiquées, mais sans le nom des patients, ce qui limitait le risque d'atteinte au secret médical.

On peut noter deux arrêts récents qui vont en ce sens :

- Un arrêt de la chambre sociale[219] à propos d'un kinésithérapeute qui avait communiqué au Conseil de l'ordre des médecins le tirage papier d'un dossier médical et qui ensuite avait été licencié par l'établissement. La chambre sociale de la Cour de cassation a considéré que dans cette hypothèse il ne pouvait pas y avoir partage du « secret » puisque l'information avait été délivrée dans un but étranger à la continuité des soins – le dossier ayant été communiqué pour permettre à ce médecin de se défendre devant le Conseil de l'ordre des médecins.

- Un arrêt de la chambre sociale du 20 avril 2017[220] concerne l'expert mandaté par le comité d'hygiène et de sécurité. La question était de savoir si cet expert était dépositaire du secret médical, au sens de l'article L. 1110-4 du code de la santé publique. La chambre sociale répond par la négative et revient à la restriction de l'information et de l'activité en précisant que cet expert n'était pas en relation avec l'établissement, qu'il n'intervenait pas dans le système de santé pour les besoins de la prise en charge des personnes, et que donc il n'était pas dépositaire du secret médical. Il s'agit là d'une interprétation très liée à la nécessité qui, avec le texte indiquant noir sur blanc cette proportionnalité, permettra à la Cour de cassation de moduler les conditions de délivrance des informations de données de santé et des informations médicales.

Pascale Fombeur

Présidente de la 1re chambre de la section du contentieux du Conseil d'État,
modératrice de la table ronde

Merci beaucoup Mme Martinel pour cette présentation très riche. Nous avons jusqu'à présent abondamment parlé du droit tel qu'il a été écrit par le législateur et tel qu'il est interprété par le juge. Nous allons maintenant nous interroger sur la façon dont ce droit peut être mis en pratique. Pour cela, j'ai le plaisir de donner la parole au docteur Lucas pour que, face à toute cette complexité, il nous explique comment ses confrères perçoivent les choses et comment le Conseil de l'ordre des médecins les accompagne pour mettre en pratique les nouveaux textes.

219 C. cass., Soc., 1er décembre 2015, pourvoi n° 14-22.133.
220 C. cass., Soc., 20 avril 2017, pourvois n°s 15-27.927 et 15-27.955.

Jacques Lucas
Vice-président du Conseil national de l'ordre des médecins

Merci Mme la présidente. Je remercie également Mme la présidente de la section du rapport et des études, ainsi que les président et président adjoint de la section sociale pour leur aimable invitation à participer à ce colloque.

Les difficultés et la complexité, qui ont été clairement exposées par Mme Laude, sont très certainement aisément compréhensibles par l'auditoire de cette assemblée, mais vous comprendrez qu'elles suscitent un trouble important et de l'incompréhension de la part du corps médical, élevé dans le magistère – édicté d'ailleurs par la Cour de cassation – que le secret était général et absolu ; alors que l'on s'aperçoit, selon même la conclusion de Mme Laude, que ce n'est peut-être pas de cette façon-là qu'il faut le concevoir.

Dans ce contexte, le rôle de l'Ordre est d'essayer d'apporter un regard à la fois suffisamment paisible et précis, presque aussi précis que le droit qu'il va se permettre, chemin faisant, de critiquer.

Notre premier propos est de savoir comment rendre immédiatement compréhensibles la loi et les règlements dans leur exercice pour les médecins au regard de la déontologie professionnelle.

Le deuxième point est de savoir comment s'interprètent, selon le Conseil national – s'il peut s'autoriser devant les membres du Conseil d'État à être producteur de doctrine –, les articles du code de déontologie dans la société numérique par rapport à un exercice plus académique – le code de déontologie médicale ayant été écrit dans sa première version en 1947 et adapté dans une version générale en 1995 – ; ou bien s'il faut réécrire les articles de déontologie médicale.

Le troisième élément est de savoir comment s'analyse l'application du secret professionnel du médecin. Aucun article du code de la santé publique relatif à la déontologie médicale ne parle de secret médical. Dans tous les codes de déontologie, il est fait mention du secret professionnel du médecin et des différents professionnels de santé. Je préciserai ensuite comment nous concevons cette interprétation, et comment s'analyse l'implication du secret professionnel du médecin dans un monde où les pathologies sont totalement différentes de ce qu'elles étaient en 1947 – où il y avait essentiellement des pathologies aiguës dont le patient guérissait ou parfois malheureusement décédait. Et comme ces patients ont guéri de plus en plus grâce au progrès médical, nous sommes entrés dans l'ère des pathologies chroniques, ère qui impose de partager des informations couvertes par le secret entre les différents médecins et professionnels de santé et les différentes structures de soins auxquelles le patient va avoir recours. Dans ce contexte, on est obligé de prendre en compte la nécessité d'abattre les frontières au niveau du partage des informations entre la médecine de ville et l'hôpital, puisque le patient passe de l'un à l'autre selon les nécessités de son état de santé et pas seulement selon les règles de droit.

Le quatrième aspect est de savoir comment transposer le terme de « colloque singulier », remontant à 1934 – et qu'avait exprimé le docteur Georges Duhamel –, dans une société médicale telle qu'elle évolue depuis 1980, où s'est organisée la médecine de groupe et où l'on parle des maisons de santé pluriprofessionnelles. Comment, en effet, s'applique la protection des données et le secret dans ces maisons pluriprofessionnelles ou dans les parcours de soins ?

C'est sur ces notions que nous avons produit et rendu publiques les recommandations du Conseil national de l'ordre des médecins sur les échanges et le partage d'informations au sein de l'équipe de soins prenant en charge une personne[221].

Rappel historique.

La loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé a posé deux principes, codifiés par la rédaction de l'article L. 1110-4 du code de la santé publique d'alors, pour l'application du secret couvrant les informations personnelles en santé. Premier point : avec l'accord de la personne, plusieurs professionnels de santé peuvent échanger des informations la concernant. Second point : le secret qui couvre ces données est implicitement partagé pour l'accès au dossier du patient entre les professionnels de santé qui constituent l'équipe de soins dans un établissement.

L'Ordre souligna de longue date l'inégalité déontologique de fait entre les médecins et les autres professionnels de santé, selon qu'ils exerçaient en établissement où le secret était partagé, ou selon qu'ils exerçaient en ville où le secret n'était pas partagé implicitement puisqu'il fallait demander le consentement.

La loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, par la modification de l'article L. 1110-4 du code de la santé publique, permet de satisfaire à notre demande. Nous y avions d'ailleurs, dans les travaux préparatoires à la loi, contribué de façon importante. Toutefois, la rédaction dudit article L. 1110-4, qui supprime les « professionnels de santé » en indiquant simplement les « professionnels qui concourent », ainsi que la définition de l'équipe de soins dans l'article L. 1110-12 du même code, introduit une confusion regrettable puisqu'elle ne distingue pas les professionnels de santé des autres professionnels intervenant dans le champ médico-social et social. Dans ce contexte, le Conseil national de l'ordre des médecins considère qu'il aurait été préférable de maintenir, dans les usages pratiques, la distinction entre les professionnels de santé et ceux qui n'en sont pas. C'est-à-dire qu'il y aurait eu une équipe de prise en charge élargie et, au sein de cette équipe, une équipe de soins. Cette idée a failli prospérer, mais le Parlement a balbutié et les amendements déposés en ce sens ont été rejetés.

Bien évidemment, nous ne contestons pas le fait que les autres professionnels interviennent opportunément dans la prise en charge des personnes, surtout compte tenu du vieillissement de la population et de l'augmentation des

221 Conseil national de l'Ordre des médecins, *Échanges et partage d'informations au sein de l'équipe de soins prenant en charge une personne*. Recommandations du Conseil national de l'Ordre des médecins, février 2017.

pathologies au long cours où se pose, au nom du principe éthique de bienfaisance, le fait que d'autres professionnels concourent à la prise en charge des personnes. Mais nous observons que si ces personnes sont soumises à la rigueur du code pénal, puisqu'elles ont également leurs secrets professionnels, les professionnels de santé ont, en quelque sorte, la « double peine » puisqu'ils peuvent comparaître en droit pénal et en droit disciplinaire, puisqu'il n'est pas considéré que le même fait est du « *bis in idem* »[222] et que les deux juridictions puissent siéger séparément.

La puissance règlementaire a d'ailleurs perçu cette difficulté générée par la loi, puisque le décret n° 2016-994 du 20 juillet 2016 relatif à la mise en application de la loi « santé » prévoit que des recommandations, qui s'apparentent en quelque sorte à du droit souple, concernant le partage des données au sein d'une équipe de soins et entre ces deux catégories – les professionnels et les non professionnels de santé – feront l'objet de recommandations élaborées par la Haute Autorité de santé (HAS) avec le concours des conseils nationaux des ordres professionnels. En quelque sorte, il y a une difficulté dans la loi ; le décret ne résout pas la difficulté, mais transpose la difficulté à résoudre à la HAS et aux ordres professionnels.

Avant de commencer à produire ces recommandations, je souhaiterais évoquer la différence entre l'*échange* qui est la transmission d'une information d'un point A vers un point B – comme, par exemple, les courriels sécurisés en santé –, et le *partage* qui consiste à se connecter à une base où se trouvent les données – dont le dossier médical partagé (DMP) en est l'illustration. Mais il existe des dossiers informatisés dans les structures de soins, que ce soit les établissements ou les maisons de santé pluriprofessionnelles. Et le problème se pose donc également à ce niveau.

En ce qui concerne les régimes juridiques entre le « droit d'opposition » et le régime du « consentement », il faut bien évidemment que, dans les deux cas, le patient ait été informé. Mais qui saurait me dire à quoi consent réellement le patient, même après cette information, quand il accepte le traitement de ses données ? Surtout lorsque l'on voit la facilité avec laquelle, après avoir téléchargé une application, il clique « j'accepte » sans avoir lu les conditions générale d'usage ! On voit donc qu'il y a là, sur le plan éthique, une très grande nécessité d'information publique. Or si nous avons beaucoup évoqué les bases publiques tout au long de ce colloque où se trouvent des données produites par les professionnels de santé – qui vont jusqu'au certificat de décès, c'est dire si nous allons au bout de la production de données –, nous n'avons que peu parlé des bases privées, alors même qu'y sont recueillies des données massives – généralement d'ailleurs en dehors de la zone du règlement général sur la protection des données (RGPD)[223], bien que ledit règlement puisse s'appliquer également aux États-Unis –, qui sont directement produites par les personnes elles-mêmes et collectées sans professionnels de santé médiateurs.

222 La règle « *non bis in idem* » (ou « *ne bis in idem* ») signifie que nul ne peut être poursuivi ou condamné deux fois pour le même fait.

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

En conclusion de mon propos, et pour en revenir plus précisément au cœur de notre sujet, on notera que le décret n° 2016-994 du 20 juillet 2016 précise, pour application de la loi « santé », que seules sont prises en considération les « *informations strictement nécessaires* ». Dès lors, on peut s'interroger sur l'ajout par le législateur de l'adverbe « strictement » alors que le mot « nécessaire » aurait peut-être été suffisant, car définir ce qui est « strictement nécessaire » est particulièrement compliqué. En outre, dans le périmètre de la mission des professionnels de santé, c'est aussi quelque peu compliqué, notamment parce que l'article 51 de la loi « HPST »[224] a permis d'avoir des délégations de tâches, et que l'on parle aujourd'hui de *pratiques avancées* que le législateur a prévues dans la même loi, et que les missions de ces professionnels de santé et des autres professionnels vont probablement évoluer avec le temps.

Dans ce contexte, qu'en est-il de la notion d'information partagée « strictement nécessaire » ? L'information couverte du caractère secret peut être détenue par l'un des membres de l'équipe de soins, qu'il soit médecin, professionnel de santé ou autre professionnel des secteurs médico-sociaux et sociaux. Il appartient à chaque dépositaire de l'information de savoir ce qu'il doit en faire dans l'intérêt du patient, et dans les conditions et les limites de la loi et des textes pris pour son application. C'est pourquoi il est assez illusoire – ainsi que je l'ai déjà précisé – de définir ce qui est « strictement nécessaire ». En toute hypothèse, la non communication d'une information qui s'avèrerait avoir entraîné des conséquences dommageables pour le patient ouvrirait un contentieux en responsabilité sur lequel se prononcerait le juge – on imagine sans peine que si l'on dit au médecin « ne vous inquiétez pas », cela va créer des contentieux et le juge dira ce qu'il faut faire, ce qui aura pour conséquence de mettre le professionnel dans un état d'intranquillité pour savoir s'il doit ou non partager les informations.

Cet argument plaide donc en faveur de la « mise en partage » de toutes les informations objectives, dont le professionnel a eu connaissance. En revanche, toutes les informations données en confidence, ou impliquant un tiers, ou sans rapport direct avec la prise en charge, sont par nature exclues de ce champ. De sorte que l'on en revient à l'origine hippocratique de la notion de secret qui rassemble *tout ce que j'ai vu, entendu ou compris, admis dans l'intérieur des maisons*, et ce ne sont peut-être pas strictement les données proprement médicales.

C'est pourquoi nous envisageons de faire prospérer les propositions suivantes.

Notre première recommandation sur les notions d'échange et de partage est de souligner que ne peuvent être mises en partage que les seules informations formalisées, au même titre que ce qui est prévu pour la communication du dossier médical. Il nous paraît en effet que, dans le cadre d'une équipe qui ne comporterait que des professionnels de santé, il n'est pas pertinent de définir par profession et *a priori* les informations qui pourraient être partagées et celles qui ne le pourraient pas. On voit d'ailleurs que la grille d'habilitation du dossier médical personnel (DMP) arrive à cette conclusion.

224 Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

La deuxième recommandation que nous formulons, c'est que soient mises en partage entre tous les professionnels de santé membres de l'équipe de soins, sauf opposition du patient, toutes les informations formalisées contenues dans son dossier. En revanche, le partage d'informations entre les professionnels de santé, membres de l'équipe de soins, et les autres professionnels membres de cette même équipe mais qui ne sont pas des professionnels de santé, doit être paramétré dans le système informatique support du dossier, afin que ces données puissent être filtrées.

Notre troisième recommandation porte sur le paramétrage informatique des accès aux bases de données où sont contenus les dossiers. Ces accès doivent permettre de sélectionner les informations formalisées inscrites dans le dossier qui sont rendues accessibles aux non professionnels de santé, afin qu'ils puissent accomplir leur mission. Si les données auxquelles ils ont ainsi accès leur paraissent insuffisantes, les autres communications pourront leur être transmises par la voie des échanges, sous la responsabilité du médecin ou du professionnel de santé qui les détient. Dans ce contexte, comment assurer la protection des informations ou respecter le caractère secret qu'elles ont ? Tout simplement en informant le patient sur ses droits.

La quatrième recommandation concerne la connaissance de ses droits par le patient. Ceci suppose que l'information lui a été donnée, de manière générale, à travers une communication publique et un dispositif d'affichage du même type que ceux qui l'informent du traitement informatisé des dossiers pour application de la loi « informatique et liberté »[225]. En premier lieu, le médecin, comme tous les autres professionnels de santé membres de l'équipe de soins, doit demander au patient s'il a bien pris connaissance des informations générales qui lui ont été données, s'il les a comprises, s'il n'a pas d'observations à faire à ce professionnel de santé, afin qu'il les complète. En deuxième lieu, les membres de l'équipe de soins doivent être informés de leur devoir au regard du respect du secret professionnel et des dispositions des codes. Pour ce qui concerne les professionnels de santé, cette information doit leur être délivrée par la communication des ordres professionnels au tableau desquels ils sont inscrits. Et pour ce qui concerne les autres professionnels, ils doivent en être informés par l'organisme de tutelle auquel ils se rattachent. Enfin, en troisième lieu, les sécurités informatiques doivent être assurées, puisqu'il s'agit d'une obligation déontologique comme le rappelle le Conseil national de l'ordre des médecins.

La dernière recommandation énonce que l'accès aux informations, qui peuvent être partagées dans les dossiers, doit être informatiquement identifié, horodaté et tracé avec conservation des traces dans le système d'information. Cela suppose un moyen d'identification du professionnel ayant accédé au dossier, soit par carte à puce, soit par un moyen offrant les mêmes garanties. L'utilisation d'un identifiant et d'un mot de passe impose que le mot de passe soit créé par le professionnel sous son identité, selon les recommandations de la CNIL, et qu'il soit suffisamment complexe et changé régulièrement. Un des membres de l'équipe de soins doit

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

être identifié comme l'interlocuteur du responsable de la sécurité du système d'information dans lequel les membres de l'équipe de soins sont identifiés. Et nous aurons à nous poser la question s'il ne doit pas y avoir un « délégué à la protection des données » au regard du règlement général sur la protection des données (RGPD) dans les structures qui regroupent les professionnels de santé – sachant que les grosses structures ne posent pas de problème pour les établissements puisque c'est une obligation, en revanche pour les petites structures cela peut se discuter.

Telles sont les recommandations qui seront adressées à la Haute Autorité de santé, afin de produire, à travers ces opinions, les recommandations qui doivent être publiées pour la parfaite application de l'article L. 1110-3 II du code de la santé publique ; à moins que cela ne s'avère une mention décrétale qui restera sans suite, auquel cas nous essaierons de faire prospérer nos propositions.

Pascale Fombeur

Présidente de la 1re chambre de la section du contentieux du Conseil d'État,
modératrice de la table ronde

Merci beaucoup docteur Lucas pour votre exposé ainsi que pour la primeur de ces recommandations transmises à la Haute Autorité de santé. Ceci est extrêmement intéressant et nous montre que, pour pouvoir respecter les principes déontologiques, il faut savoir prendre des mesures organisationnelles très concrètes, quand bien même elles s'avèreraient parfois contraignantes pour les professionnels. J'espère que les médecins et les autres professionnels soumis à ces obligations – également dans l'intérêt du patient – pourront accepter ces recommandations élaborées en lien avec la HAS, sachant combien leur tâche est lourde, mais aussi à quel point les enjeux sont importants notamment pour l'ensemble des patients.

Échanges avec la salle

Question au docteur Lucas

Je souhaiterais rebondir sur les propos du docteur Lucas en les mettant en regard de l'exercice pratique des professionnels. Depuis des années on parle du dossier médical partagé (DMP), mais sans véritable avancée. De sorte qu'il existe un décalage entre ce DMP et les nombreuses applications informatiques créées quasi-quotidiennement par de « jeunes pousses » qui, au demeurant, ne sont pas forcément hébergeurs de données de santé – et dont on ignore comment elles gèrent la confidentialité des données. Or, aujourd'hui, les professionnels de santé sont parfois tentés d'utiliser ces applications nouvelles tout simplement parce qu'elles les aident dans leur exercice pratique de coordination entre le médecin, l'infirmier et le pharmacien. Dans ce contexte, comment aider concrètement les professionnels de santé à s'y retrouver dans cet écheveau à la fois juridique et technologique ?

Jacques Lucas

Je pense qu'il faut décliner les grands principes de la loi et les traduire dans la réalité concrète. Pour répondre à votre question, sachez que nous militons, par exemple – mais nous ne sommes pas les seuls –, pour qu'existe un label public sur les applications et les objets connectés que les professionnels de santé pourraient utiliser et qui n'ont, pour l'instant, pas statut de dispositif médical au sens de la règlementation européenne et française – sachant que cela concerne plutôt les dispositifs médicaux de classes I et II. Ce label public devrait garantir à la fois la fiabilité et la sécurité de ces applications et, surtout, permettre de résoudre le problème de l'hébergement des données. J'espère donc que les travaux initiés au ministère de la santé vont reprendre rapidement avec une représentation des usagers, des patients, de la Haute Autorité de santé, et des industriels et créateurs de « jeunes pousses ». J'ajoute que j'ai beaucoup apprécié la conclusion de Mme Laude sur le fait que l'analyse du secret médical devrait sans doute porter davantage sur la protection et la confidentialité des données médicales, ainsi que sur leurs conditions d'accès.

Question à Mme Laude

À la suite des changements législatifs des années 2000, vous avez précisé que l'on serait passé du secret médical, vu comme une obligation du médecin, au secret médical vu comme un droit du patient qui peut ainsi en disposer à sa guise, c'est-à-dire s'en prévaloir ou décider de partager ses données. Dans ce contexte, existe-t-il des garde-fous à la vente par le patient de ses propres données ?

Anne Laude

La vente de ses propres données par le patient est possible, mais encore faut-il qu'il en dispose. En règle générale, les données dont on a parlé précédemment sont des données qui sont chez le professionnel de santé, ou dans le dossier médical partagé, ou encore déposées chez des tiers dans le cadre d'applications fonctionnant sur téléphones portables. Bien sûr le patient a connaissance de toutes ces informations, sur lesquelles d'ailleurs il a des retours (positionnement sur une échelle de valeurs, bilan, etc.). Pour autant, peut-il ou va-t-il les vendre ? Je ne pense pas que la question se pose ou se posera en ces termes. En effet, ne serait-ce pas plutôt ceux qui recueillent ces informations, par exemple les grandes sociétés de l'Internet, qui risquent de revendre à des tiers ces données, afin qu'ils puissent apprécier le comportement du patient et donc le cibler pour lui proposer des produits ou des services particuliers liés à son profil, voire ne pas l'accepter dans certains cas en tant que client (assurance, prêt immobilier, etc.). Tout cela peut donc représenter une valeur marchande non négligeable pour ces tiers que de disposer de ces données et vouloir les vendre à des opérateurs divers.

Les garde-fous existent cependant. Ils sont spécifiques au droit de la protection des données, avec la limite souvent évoquée de la territorialité. Il importe en effet de savoir où est hébergé celui qui, au final, dispose de ces données, puisque la loi applicable et le régime de protection dont disposera l'usager ou le patient seront différents selon les cas.

Question du public

Au niveau de l'Assistance publique-Hôpitaux de Paris (AP-HP), nous disposons d'un système d'information particulièrement riche en données dénommé Orbis qui, à l'instar du dossier médical partagé, mais en plus performant, permet la création d'un dossier patient hospitalier unique et partagé au niveau des équipes médicales et soignantes pour l'ensemble des trente-neuf hôpitaux de l'AP-HP. Dans ce contexte, les directeurs et les gestionnaires d'hôpitaux, ou le personnel administratif, peuvent-ils être associés au partage de ces données, sachant que pour l'instant les données qu'on leur communique sont surtout liées aux affaires pré-juridictionnelles, c'est-à-dire concernant des patients se plaignant, par exemple, des conditions de soins au cours de leur séjour hospitalier ?

Jacques Lucas

Sachez qu'il m'a été demandé de participer, en tant que personnalité qualifiée, à l'étude du système d'information de l'AP-HP. Projet auquel j'ai répondu favorablement aux fins de faire passer quelques messages, comme par exemple celui-ci : quand un patient entre dans un établissement pour un épisode de soins, il se confie à l'équipe de soins ; mais quand il entre dans le même établissement pour un autre épisode de soins, alors qu'il y possède un dossier unique, selon

la loi son consentement devra être demandé puisqu'il va passer d'une équipe de soins à une autre. Et la question va être particulièrement importante avec les groupements hospitaliers de territoires qui vont se situer au niveau massif – pratiquement – de l'AP-HP. Il y a donc là un vrai sujet à explorer, sauf à vouloir laisser les choses se faire naturellement – il faut aussi savoir faire confiance au bon sens. Cependant, juridiquement, il faudrait arriver à imposer l'existence d'un dossier unique dans les structures des établissements, et pas uniquement au niveau de l'AP-HP, de sorte que les règles de consentement du transfert du dossier à une autre équipe de soins soient appliquées.

Par ailleurs, sur ces fonctionnements, il existe, en dehors de votre fonction, des médecins du département de l'information médicale (DIM). Et, à notre sens, les médecins DIM ne doivent pas être uniquement chargés du codage des actes par rapport à la tarification à l'activité (T2A)[226]*. Ils devraient être associés, avec le chef d'établissement, aux habilitations pour les accès aux bases où se trouvent les données personnelles.*

Anne Laude

La directive sur la mobilité des patients[227] *prévoit un dossier médical et l'interopérabilité des services au niveau européen. En revanche, je ne crois pas qu'elle précise quoi que ce soit sur le régime d'accès et de protection des données de santé. Elle affirme bien la confidentialité et le secret médical mais, précisément, par rapport à ce que l'on est en train de voir (partage ou information). De sorte que le risque est grand de se retrouver, demain, sur le territoire européen, avec des législations totalement différentes. Il serait donc opportun d'arriver à uniformiser les choses, au moment où le dossier médical pourra également circuler à l'intérieur du territoire européen, au risque sinon de disposer de règles très disparates et difficilement applicables.*

Question du public

Nous avons vu arriver avec soulagement la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, car il nous semblait que les termes très génériques employés, comme ceux issus par exemple des article L. 1110-4 et L. 1110-12 du code de la santé publique, validaient des pratiques de terrain déjà existantes au sein des équipes médico-sociales, à savoir le partage informel d'informations. Pourtant, dans le même temps, il nous semblait voir apparaître la soumission de l'ensemble de l'équipe de soins, y compris les professionnels du secteur médico-social, au secret professionnel ; d'autant plus que le V de l'article L. 1110-4 punit à la fois celui qui révèle et celui qui sollicite la révélation de ces informations.

226 La tarification à l'activité (T2A) est le mode de financement des établissements de santé publics et privés. Elle a été instaurée par la loi n° 2003-1199 du 18 décembre 2003 de financement de la sécurité sociale pour 2004.

227 Directive n° 2011/24/UE du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (applicable depuis le 25 octobre 2013 dans les États membres de l'Union européenne).

Cependant, tout cela offrait un discours clair aux équipes de soins sur le droit de partager les données de santé, avec les précautions liées à ce partage. Or, depuis de nombreuses semaines, nous nous heurtons à un mouvement sur le terrain où certains praticiens dénient cette soumission des professionnels du secteur médico-social au secret professionnel, notamment en s'appuyant sur l'article L. 1110-4 du code de la santé publique qui emploie le terme de « secret des informations » et non celui de « secret professionnel ». Dans ce contexte, ne sommes-nous pas dans l'erreur en cherchant à imposer aux professionnels médico-sociaux le secret professionnel ?

Anne Laude

Il est vrai que le texte que vous évoquez ne mentionne pas le terme de « secret médical ». D'ailleurs, ni le code de la santé publique, ni le code pénal ne le mentionnent, car on vise en réalité le secret professionnel. Et le code de la santé publique vise, quant à lui – et comme vous l'évoquiez –, le secret des informations concernant le patient, tout en répertoriant, à la fois dans sa partie législative et règlementaire, une liste de professionnels qui, faisant ou non partie de l'équipe de soins, vont devoir obéir à un même régime juridique pour partager ces informations. Ces professionnels sont soumis aux règles imposées par le code de la santé publique pour partager ces informations ou les échanger et, à ce titre, s'ils ne les respectent pas ils seront soumis au code pénal.

Agnès Martinel

Il faut bien comprendre que la définition du secret est plus dans le contenu de l'information. Et c'est là que l'on rejoint le terme « médical ». En effet, si l'information n'est pas médicale, on n'est pas dans la protection d'une donnée médicale. On peut alors être dans un secret professionnel qui est autre. La Cour de cassation distingue, par exemple, le secret de l'avocat dans une procédure et le secret médical, considérant que les informations données par l'avocat et les informations médicales données par l'avocat dans une procédure sont couvertes par le secret médical, mais pas par le secret professionnel de l'avocat. Ce dernier ne peut pas violer le secret médical quand il détient l'information, mais il peut porter atteinte à son secret professionnel. On voit ainsi à quel point l'information médicale reste sanctuarisée, ce qui est une chose positive au regard des données de santé.

Nous avons donc là deux notions du secret : le secret professionnel « classique », et le secret professionnel pour les informations médicales. En attendant que les chambres de la Cour de cassation se prononcent sur cette question, je pense qu'il est important de noter qu'il existe une protection du secret autour de l'information médicale, qu'elle soit échangée verbalement ou de façon numérique.

Jacques Lucas

Ce qui est paradoxal, c'est que – comme vous le souligniez – tout cela se passait autrefois autour de la machine à café et qu'il n'y avait pas de problème. Mais à partir du moment où des textes voulant stabiliser et rassurer apparaissent, cela pose d'autres interrogations. Il serait donc hautement souhaitable que la Haute Autorité de santé et les Ordres produisent un guide avec des recommandations, pour avoir une portée plus importante que si c'est uniquement le Conseil national de l'ordre qui le fait. Nous souhaitons que de telles recommandations soient faites, mais nous savons qu'elles sont très difficiles à faire. J'intervenais récemment à un colloque à l'Union nationale des associations familiales (UNAF) avec les mandataires de justice qui faisaient état de l'augmentation des personnes actuellement placées sous tutelle dont on peut craindre que le nombre augmente ; dans ce contexte, les mandataires de justice doivent-ils avoir accès à tout ? Il existe quand même des secrets de l'intimité de la personne, secrets qui la constituent en tant que personne, qui n'ont pas vocation à être partagés et qui diffèrent des secrets médicaux la concernant. Par exemple, si le mandataire de justice sait que la personne est diabétique, cela ne me semble pas attentatoire à ses libertés, mais s'il apprend que durant sa jeunesse cette personne a eu des comportements préjudiciables, qu'elle-même a dû taire, et qu'elle s'est structurée autour de ce secret, c'est très différent. Il y a donc là une interrogation éthique très importante à mener.

Pascale Fombeur

Présidente de la 1re chambre de la section du contentieux du Conseil d'État,
modératrice de la table ronde

Je remercie chacun des membres de la table ronde pour ses interventions ainsi que le public pour son écoute attentive et ses questions, et clôture cette séance.

Jean-Denis Combrexelle
Président de la section sociale du Conseil d'État

Jean-Denis Combrexelle a commencé sa carrière au ministère de l'industrie avant de devenir conseiller au tribunal administratif de Lyon (1982-1989). Nommé maître des requêtes au Conseil d'État en 1994, il est commissaire du Gouvernement devant les formations contentieuses de 1995 à 1999. Rapporteur général de la Commission pour les simplifications administratives au secrétariat général du Gouvernement de 1999 à 2000 et directeur adjoint des affaires civiles et du Sceau au ministère de la justice en 2000 et 2001, Jean-Denis Combrexelle a été directeur des relations du travail de 2001 à 2006, puis directeur général du travail au ministère du travail et de l'emploi de 2006 à 2014. Il est président de la section sociale du Conseil d'État depuis 2014.

Le thème de ce colloque, santé et protection des données, nous concerne tous. C'est particulièrement le cas à travers la notion du dossier médical partagé (DMP). Nous pourrions même aller jusqu'à dire que nous détenons tous, aujourd'hui, dans notre poche, un véritable DMP sous forme de « mobile multifonction »[228]. Cet appareil contient en effet de nombreuses informations nous concernant (données bancaires, indications de géolocalisation, pratiques sportives, rythme cardiaque, etc.). En revanche, ce que l'on ignore c'est ce que deviennent ces données. Et il n'est pas exclu, au détour d'une « acceptation » informatique dont on n'aurait pas mesuré toute la portée, que l'on a peut-être autorisé le transfert puis le stockage de ces données dans le « nuage ». Certes, les juristes et les informaticiens présents à cette journée ont précisé qu'il existe, pour ce faire, des procédures et des voies de droit. Mais c'est oublier qu'il existe aussi beaucoup de monde, y compris parmi le public de ce colloque, qui ignore tout de ces procédures. Pire, il y a aussi beaucoup de personnes qui sont volontaires pour transférer ces données *via* des outils logiciels spécifiques comme *Skype*, *Snapchat*, *Facebook*, etc. pour mettre à la disposition d'un réseau virtuel les informations les plus intimes ou les plus précises les concernant et touchant notamment à leur santé.

Là est le paradoxe. Que nous soyons ou pas professionnels de santé, fonctionnaires nationaux ou européens, régulateurs, avocats, etc., nous avons tous eu à connaître les notions de droits de la personne et de libertés publiques à propos notamment des dispositions de la loi « santé » sur les données massives en matière de santé.

228 Voir vocabulaire des télécommunications (liste de termes, expressions et définitions adoptés), *in JORF* n° 0008 du 11 janvier 2018, texte n° 135.

Mais, pour autant, nous constatons que s'organisent des circuits parallèles de données de santé, échappant pour l'essentiel à la loi nationale et au juge, sur des questions aussi essentielles que le contenu de la donnée et surtout de ses destinataires. On imagine ainsi sans peine l'intérêt que revêtent ces données pour un assureur, un employeur ou un publicitaire. Et c'est l'un des premiers paradoxes de ce colloque, avec ce sentiment que sur un champ aussi sensible il existe de puissants et multiples circuits parallèles qui sont loin d'être sous contrôle.

Si l'on revient au champ des réformes en cours, on s'aperçoit que la santé exige que soient utilisées toutes les potentialités du traitement des données massives, ceci d'autant plus que *via* le système d'information des organismes de sécurité sociale, devenu le système national des données de santé (SNDS), nous disposons en France d'une quantité de données parmi les plus importantes au monde. Bien sûr nous ne sommes pas les seuls, mais nous faisons partie des pays les plus avancés en la matière.

À l'heure des données massives, il est aujourd'hui attendu, grâce à une utilisation optimale de ces immenses bases de données, des avancées considérables et sans précédent en matière de santé publique. Il faut, en conséquence, organiser leur exploitation au mieux de l'intérêt général en les ouvrant davantage aux chercheurs et aux préventeurs.

Mais le droit *à la santé* doit être concilié avec le droit *de la santé* qui intègre l'exigence du respect des libertés publiques. La donnée de santé n'est pas, en effet, une donnée comme une autre. Elle touche au plus près la protection de la vie privée et les droits de la personne. À l'évidence, c'est l'une des données les plus sensibles. Elle doit donc faire l'objet de protection *et* de garanties adéquates. Ce sont ces deux exigences qui sont souvent rappelées par le Conseil constitutionnel. Elles ne s'opposent pas, mais elles doivent être conciliées. Cela a d'ailleurs été l'objet de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

Lors des tables rondes de ce colloque, les meilleurs spécialistes de la matière, qu'ils aient été concepteurs de la réforme, professionnels de santé ou régulateurs, sont venus exposer les grandes questions qui se posent actuellement.

S'il fallait tirer les conclusions des quatre tables rondes de ce colloque, celles-ci seraient les suivantes.

1) Tout d'abord, il faudrait s'entendre sur la définition des données, notamment au niveau national – ce qui n'est pas acquis –, mais aussi et surtout au niveau de l'Union européenne et de l'ensemble du monde tant les données sont aujourd'hui mondialisées, avec une force de frappe sans pareil des firmes géantes du numérique[229] et bientôt des entreprises chinoises.

Une régulation au niveau mondial est une nécessité, mais elle interpelle la France et l'Union européenne. La première question est de savoir dans quelle mesure le « logiciel intellectuel européen » pourrait inspirer les autres systèmes

229 Les firmes *Google*, *Apple*, *Facebook*, *Amazon* et *Microsoft*, regroupées sous l'acronyme GAFAM.

juridiques. Et, seconde question, comme la régulation n'est pas seulement affaire de règlements et de lois, mais aussi de mise en œuvre entre notamment l'Union européenne et les autres pays, de savoir comment tous ces pays coopéreront entre eux. La matière est très sensible, notamment pour les droits des personnes, mais aussi pour les groupes d'individus devenus potentiellement des cibles de la statistique médicale.

2) Le deuxième point est qu'il faut maintenant mettre en œuvre au niveau national la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

Comme il a été rappelé précédemment, nous sommes actuellement à une étape intermédiaire entre la mise en œuvre de la loi « santé » de 2016 et la transposition du règlement européen dit « RGPD ». Dans ce contexte, tout est affaire de responsabilité et de confiance. Que l'on mette des curseurs trop rigides et la recherche et la place de la France seront atteints ; or notre pays doit avoir une place très importante en matière de recherche et notamment de recherche médicale. Que l'on mette des curseurs trop souples et les droits de la personne ne seront plus garantis.

À la manœuvre, il y a des instances de régulation (Commission nationale de l'informatique et des libertés, etc.), des instances d'instruction de facilitation (l'Institut des données) et – comme l'a souligné le vice-président Sauvé – un méga-régulateur qui est le juge. Mais *in fine* la régulation dépendra tout autant des individus que des institutions. Seuls les individus, qu'ils soient chercheurs ou professionnels de santé, donneront de la chair à ces deux notions essentielles que sont la confiance et la responsabilité.

3) Le troisième point est que l'accès aux données est aussi essentiel que le contenu des données. Il doit y avoir une correspondance entre les deux. Les exigences de la recherche n'impliquent pas l'accès à toutes les données, mais à des données non réidentifiables. En revanche, le suivi médical de la personne implique la connaissance des parcours de santé à travers le dossier médical. Et le souci de protection implique des limites face à des acteurs comme, par exemple, l'employeur ou l'assureur. Là aussi tout est une question d'équilibre et de proportionnalité – et l'on rejoint ici les exigences du règlement européen.

Cela suppose également que les utilisateurs aient les moyens d'exploiter les données. M. Saout disait précédemment qu'il y avait là une interrogation concernant les associations[230]. Mais il faut y ajouter l'État qui est responsable lorsqu'il n'exploite pas suffisamment les données, et qui doit avoir les moyens et doit donner les moyens à ces différentes institutions d'exploiter les données de santé. Il y a là aussi un enjeu qui est extrêmement important. La donnée en soi est une donnée brute. Tout dépend donc de l'exploitation et des moyens qui sont donnés pour cette exploitation.

Enfin, en dépit de toutes les révolutions technologiques et juridiques – par exemple, sur le sujet des données médicales –, il nous reste le thème cher du « secret médical » ; notion qui demeure un guide central, voire un garde-fou,

230 Voir la table ronde n° 3 dans le présent ouvrage.

pour l'ensemble des acteurs du champ de la santé. Certes, ce secret médical doit s'enrichir pour pouvoir s'adapter, mais la loi, les ordres et les juges y contribuent, et il demeure plus que jamais d'actualité avec deux principes essentiels : celui du *consentement* et celui de l'*intérêt du malade*.

Parallèlement au monde que nous avons étudié durant ce colloque, se crée, pour demain, un autre monde où les mêmes données n'obéissent plus exactement aux mêmes règles de contrôle et, disons, à la même philosophie. La principale interrogation est précisément de savoir si nous restons sur ces questions de l'utilisation des données de santé, dans un monde connu, mais transformé par les potentialités de la société de l'information, avec simplement une nécessaire adaptation des règles et des normes existantes. Ou si, notamment en matière de santé, nous ne sommes pas à l'orée d'un monde totalement nouveau dans lequel les règles actuelles, même profondément réformées, n'auraient plus guère de sens et de portée.

Récemment, la firme *Google* a lancé à travers une filiale une cohorte de dix mille volontaires équipés d'un ensemble d'objets connectés pour suivre pendant quatre ans leur état de santé. Cela va jusqu'à placer des microprocesseurs sous le matelas pour enregistrer les mouvements du corps pendant le sommeil. Des prélèvements seront effectués sur les sécrétions, le génome des volontaires sera décrypté. Les données seront mises à la disposition des chercheurs. Le but avoué – en tout cas annoncé – est de mieux comprendre la transition entre bonne santé et maladie, et – toujours selon les concepteurs du projet – d'essayer de prolonger la durée de vie des personnes concernées.

L'Homo deus, pour reprendre le titre du livre d'Harari[231], aura peut-être une espérance de vie augmentée, mais la contrepartie en sera lourde puisque ce sera la fin de l'intimité et l'acceptation de l'intrusion de ceux qui garantissent la santé. Dans ces conditions, la notion de consentement va commencer à prendre un tour singulièrement nouveau par rapport à toutes les réflexions que l'on a pu mener jusqu'à présent. C'est ce que traduit le titre d'un article récent paru dans *Les Échos* par la formule : « adieu l'humanisme, bonjour le *dataism* »[232], c'est-à-dire l'idée que les bases ou les banques de données bouleversent complètement la notion de données.

Cette conférence nous réunit dans les locaux qui abritent le Conseil d'État. La tradition de cette institution est d'être ancrée dans la réalité des choses, en essayant d'avoir une vision du futur pour régir le présent, à l'image de ce qui a été fait, par exemple, sur les questions de bioéthique.

Nous avons le même enjeu, aujourd'hui, en matière de données de santé. À nous de faire en sorte de réfléchir et d'agir pour que la sombre prévision de Michel Foucault[233] dans *Les mots et les choses*[234] s'avère fausse : « *L'homme est une*

231 Y. N. Harari, *Homo deus - Une brève histoire de l'avenir*, éd. Albin Michel, Paris, 2017.
232 G. Koenig, « Adieu l'humanisme, bonjour le *dataism* », *in Les Echos*, 21 novembre 2017.
233 M. Foucault (1926-1984), philosophe français.
234 M. Foucault, *Les mots et les choses – Une archéologie des sciences humaines*, éd. Gallimard, Paris, 1966.

invention dont l'archéologie de notre pensée montre aisément la date récente. Et peut-être la fin prochaine. Si ces dispositions [les dispositions propres au savoir moderne] *venaient à disparaître comme elles sont apparues, si par quelque événement dont nous pouvons tout au plus pressentir la possibilité, mais dont nous ne connaissons pour l'instant encore ni la forme ni la promesse, elles basculaient, comme le fit au tournant du XVIII^e^ siècle le sol de la pensée classique, – alors on peut bien parier que l'homme s'effacerait, comme à la limite de la mer un visage de sable* »[235].

Autrement dit, l'enjeu auquel nous sommes confrontés doit à la fois tenir compte de ce qui se passe aujourd'hui – la question du règlement, de la loi « santé » –, et de tout ce qui se passe en matière de santé. Dans ce contexte, c'est de notre responsabilité à tous d'être particulièrement vigilants – même si cela sort du cadre que nous avons précédemment fixé – sur ce qui se passe à la fois en France, au niveau de l'Union européenne et aussi au-delà de nos frontières.

Avant de clôturer définitivement ce colloque, je souhaiterais remercier tous ceux qui ont contribué à l'organisation de cette journée, au premier rang desquels les intervenants qui ont beaucoup travaillé pour nous présenter des exposés riches et pertinents, les présidents des tables rondes qui nous ont consacré une partie de leur temps, sans oublier la section du rapport et des études et la section sociale qui ont été les chevilles ouvrières de ce colloque, avec un remerciement particulier pour Mme la présidente de Boisdeffre, ainsi que pour Mme Lafeuille, M. Tabuteau et M. Malverti. Enfin, je remercie également le public pour son écoute attentive et sa participation active à nos échanges.

235 *Ibid*., p. 398.

Annexes

1. Normes applicables

1.1. – Règlement de l'Union européenne

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

(…)

Considérant ce qui suit :

(1) La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données à caractère personnel la concernant. (…)

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

(52) Des dérogations à l'interdiction de traiter des catégories particulières de données à caractère personnel devraient également être autorisées lorsque le droit de l'Union ou le droit d'un État membre le prévoit, et sous réserve de garanties appropriées, de manière à protéger les données à caractère personnel et d'autres droits fondamentaux, lorsque l'intérêt public le commande, notamment le traitement des données à caractère personnel dans le domaine du droit du travail et du droit de la protection sociale, y compris les retraites, et à des fins de sécurité, de surveillance et d'alerte sanitaire, de prévention ou de contrôle de maladies transmissibles et d'autres menaces graves pour la santé. Ces dérogations

sont possibles à des fins de santé, en ce compris la santé publique et la gestion des services de soins de santé, en particulier pour assurer la qualité et l'efficience des procédures de règlement des demandes de prestations et de services dans le régime d'assurance-maladie, ou à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Une dérogation devrait, en outre, permettre le traitement de ces données à caractère personnel, si cela est nécessaire aux fins de la constatation, de l'exercice ou de la défense d'un droit en justice, que ce soit dans le cadre d'une procédure judiciaire, administrative ou extrajudiciaire.

(53) Les catégories particulières 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, y compris le traitement, par les autorités de gestion et les autorités centrales de santé nationales, de ces données, en vue du contrôle de la qualité, de l'information des gestionnaires et de la supervision générale, au niveau national et local, du système de soins de santé ou de protection sociale et en vue d'assurer la continuité des soins de santé ou de la protection sociale et des soins de santé transfrontaliers ou à des fins de sécurité, de surveillance et d'alerte sanitaires, ou à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, sur la base du droit de l'Union ou du droit des États membres qui doit répondre à un objectif d'intérêt public, ainsi que pour des études menées dans l'intérêt public dans le domaine de la santé publique. Le présent règlement devrait dès lors prévoir des conditions harmonisées pour le traitement des catégories particulières de données à caractère personnel relatives à la santé, pour répondre à des besoins spécifiques, en particulier lorsque le traitement de ces données est effectué pour certaines fins liées à la santé par des personnes soumises à une obligation légale de secret professionnel. Le droit de l'Union ou le droit des États membres devrait prévoir des mesures spécifiques et appropriées de façon à protéger les droits fondamentaux et les données à caractère personnel des personnes physiques. Les États membres devraient être autorisés à maintenir ou à introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé. Toutefois, cela ne devrait pas entraver le libre flux des données à caractère personnel au sein de l'Union lorsque ces conditions s'appliquent au traitement transfrontalier de ces données.

(54) Le traitement des catégories particulières de données à caractère personnel peut être nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique, sans le consentement de la personne concernée. Un tel traitement devrait faire l'objet de mesures appropriées et spécifiques de façon à protéger les droits et libertés des personnes physiques. Dans ce contexte, la notion de « santé publique » devrait s'interpréter selon la définition contenue dans le règlement (CE) n° 1338/2008 du Parlement européen et du Conseil (…), à savoir tous les éléments relatifs à la santé, à savoir l'état de santé, morbidité et handicap inclus,

les déterminants ayant un effet sur cet état de santé, les besoins en matière de soins de santé, les ressources consacrées aux soins de santé, la fourniture de soins de santé, l'accès universel à ces soins, les dépenses de santé et leur financement, ainsi que les causes de mortalité. De tels traitements de données concernant la santé pour des motifs d'intérêt public ne devraient pas aboutir à ce que des données à caractère personnel soient traitées à d'autres fins par des tiers, tels que les employeurs ou les compagnies d'assurance et les banques. (…)

(63) Une personne concernée devrait avoir le droit d'accéder aux données à caractère personnel qui ont été collectées à son sujet et d'exercer ce droit facilement et à des intervalles raisonnables, afin de prendre connaissance du traitement et d'en vérifier la licéité. Cela inclut le droit des personnes concernées d'accéder aux données concernant leur santé, par exemple les données de leurs dossiers médicaux contenant des informations telles que des diagnostics, des résultats d'examens, des avis de médecins traitants et tout traitement ou intervention administrés. En conséquence, toute personne concernée devrait avoir le droit de connaître et de se faire communiquer, en particulier, les finalités du traitement des données à caractère personnel, si possible la durée du traitement de ces données à caractère personnel, l'identité des destinataires de ces données à caractère personnel, la logique qui sous-tend leur éventuel traitement automatisé et les conséquences que ce traitement pourrait avoir, au moins en cas de profilage. Lorsque c'est possible, le responsable du traitement devrait pouvoir donner l'accès à distance à un système sécurisé permettant à la personne concernée d'accéder directement aux données à caractère personnel la concernant. Ce droit ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel. Cependant, ces considérations ne devraient pas aboutir à refuser toute communication d'informations à la personne concernée. Lorsque le responsable du traitement traite une grande quantité de données relatives à la personne concernée, il devrait pouvoir demander à celle-ci de préciser, avant de lui fournir les informations, sur quelles données ou quelles opérations de traitement sa demande porte.

(64) Le responsable du traitement devrait prendre toutes les mesures raisonnables pour vérifier l'identité d'une personne concernée qui demande l'accès à des données, en particulier dans le cadre des services et identifiants en ligne. Un responsable du traitement ne devrait pas conserver des données à caractère personnel à la seule fin d'être en mesure de réagir à d'éventuelles demandes.

(65) Les personnes concernées devraient avoir le droit de faire rectifier des données à caractère personnel les concernant, et disposer d'un « droit à l'oubli » lorsque la conservation de ces données constitue une violation du présent règlement ou du droit de l'Union ou du droit d'un État membre auquel le responsable du traitement est soumis. En particulier, les personnes concernées devraient avoir le droit d'obtenir que leurs données à caractère personnel soient effacées et ne soient plus traitées, lorsque ces données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière, lorsque les personnes concernées ont retiré leur consentement au traitement ou lorsqu'elles s'opposent au traitement

de données à caractère personnel les concernant, ou encore lorsque le traitement de leurs données à caractère personnel ne respecte pas d'une autre manière le présent règlement. Ce droit est pertinent, en particulier, lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et n'était pas pleinement consciente des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur l'internet. La personne concernée devrait pouvoir exercer ce droit nonobstant le fait qu'elle n'est plus un enfant. Toutefois, la conservation ultérieure des données à caractère personnel devrait être licite lorsqu'elle est nécessaire à l'exercice du droit à la liberté d'expression et d'information, au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, ou à la constatation, à l'exercice ou à la défense de droits en justice. (…)

Article 4

Définitions

Aux fins du présent règlement, on entend par :

1) « données à caractère personnel », toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

2) « traitement », toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

3) « limitation du traitement », le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur ;

4) « profilage », toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ;

5) « pseudonymisation », le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que

ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ;

6) « fichier », tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;

7) « responsable du traitement », la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ;

8) « sous-traitant », la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

9) « destinataire », la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement ;

10) « tiers », une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel ;

11) « consentement » de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ;

12) « violation de données à caractère personnel », une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ;

13) « données génétiques », les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ;

14) « données biométriques », les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ;

15) « données concernant la santé », les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ; (…)

Article 5

Principes relatifs au traitement des données à caractère personnel

1. Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ;

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ;

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

Article 6

Licéité du traitement

1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

2. Les États membres peuvent maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement pour ce qui est du traitement dans le but de respecter le paragraphe 1, points c) et e), en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal, y compris dans d'autres situations particulières de traitement comme le prévoit le chapitre IX.

3. Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par :

a) le droit de l'Union ; ou

b) le droit de l'État membre auquel le responsable du traitement est soumis.

Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres : les conditions générales régissant la licéité du traitement par le responsable du traitement ; les types de données qui font l'objet du traitement ; les personnes concernées ; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ; la limitation des finalités ; les durées de conservation ; et les

opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi.

4. Lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1, le responsable du traitement, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, entre autres :

a) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ;

b) du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;

c) de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10 ;

d) des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;

e) de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation. (…)

Article 9

Traitement portant sur des catégories particulières de données à caractère personnel

1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée ;

b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans

la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée ;

c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées ;

e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;

f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ;

h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3 ;

i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ;

j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées

et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

3. Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents.

4. Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé. (…)

Article 17

Droit à l'effacement (« droit à l'oubli »)

1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :

a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement ;

c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 ;

d) les données à caractère personnel ont fait l'objet d'un traitement illicite ;

e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;

f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1.

2. Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci.

3. Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire :

a) à l'exercice du droit à la liberté d'expression et d'information ;

b) pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3 ;

d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement ; ou

e) à la constatation, à l'exercice ou à la défense de droits en justice. (…)

1.2. – Normes françaises

1.2.1. - Code de la santé publique

Partie législative

Première partie : Protection générale de la santé

Livre Ier : Protection des personnes en matière de santé

Titre Ier : Droits des personnes malades et des usagers du système de santé

Chapitre préliminaire : Droits de la personne

Article L. 1110-4

I. - Toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations la concernant.

Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tous les professionnels intervenant dans le système de santé.

II. - Un professionnel peut échanger avec un ou plusieurs professionnels identifiés des informations relatives à une même personne prise en charge, à condition qu'ils participent tous à sa prise en charge et que ces informations soient strictement

nécessaires à la coordination ou à la continuité des soins, à la prévention ou à son suivi médico-social et social.

III. - Lorsque ces professionnels appartiennent à la même équipe de soins, au sens de l'article L. 1110-12, ils peuvent partager les informations concernant une même personne qui sont strictement nécessaires à la coordination ou à la continuité des soins ou à son suivi médico-social et social. Ces informations sont réputées confiées par la personne à l'ensemble de l'équipe.

Le partage, entre des professionnels ne faisant pas partie de la même équipe de soins, d'informations nécessaires à la prise en charge d'une personne requiert son consentement préalable, recueilli par tout moyen, y compris de façon dématérialisée, dans des conditions définies par décret pris après avis de la Commission nationale de l'informatique et des libertés.

IV. - La personne est dûment informée de son droit d'exercer une opposition à l'échange et au partage d'informations la concernant. Elle peut exercer ce droit à tout moment.

V. - Le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article est puni d'un an d'emprisonnement et de 15 000 euros d'amende.

En cas de diagnostic ou de pronostic grave, le secret médical ne s'oppose pas à ce que la famille, les proches de la personne malade ou la personne de confiance définie à l'article L. 1111-6 reçoivent les informations nécessaires destinées à leur permettre d'apporter un soutien direct à celle-ci, sauf opposition de sa part. Seul un médecin est habilité à délivrer, ou à faire délivrer sous sa responsabilité, ces informations.

Le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit, son concubin ou son partenaire lié par un pacte civil de solidarité, dans la mesure où elles leur sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès. Toutefois, en cas de décès d'une personne mineure, les titulaires de l'autorité parentale conservent leur droit d'accès à la totalité des informations médicales la concernant, à l'exception des éléments relatifs aux décisions médicales pour lesquelles la personne mineure, le cas échéant, s'est opposée à l'obtention de leur consentement dans les conditions définies aux articles L. 1111-5 et L. 1111-5-1.

VI. - Les conditions et les modalités de mise en œuvre du présent article pour ce qui concerne l'échange et le partage d'informations entre professionnels de santé et non-professionnels de santé du champ social et médico-social sont définies par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés.

Article L. 1110-4-1

Afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, les professionnels de santé, les établissements et services de santé, les hébergeurs de données de santé à caractère personnel et tout

autre organisme participant à la prévention, aux soins ou au suivi médico-social et social utilisent, pour leur traitement, leur conservation sur support informatique et leur transmission par voie électronique, des systèmes d'information conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24. Ces référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés. (…)

Article L. 1110-12

Pour l'application du présent titre, l'équipe de soins est un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes, et qui :

1° soit exercent dans le même établissement de santé, au sein du service de santé des armées, dans le même établissement ou service social ou médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles ou dans le cadre d'une structure de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale figurant sur une liste fixée par décret ;

2° soit se sont vu reconnaître la qualité de membre de l'équipe de soins par le patient qui s'adresse à eux pour la réalisation des consultations et des actes prescrits par un médecin auquel il a confié sa prise en charge ;

3° soit exercent dans un ensemble, comprenant au moins un professionnel de santé, présentant une organisation formalisée et des pratiques conformes à un cahier des charges fixé par un arrêté du ministre chargé de la santé. (…)

Chapitre Ier : Information des usagers du système de santé et expression de leur volonté

Section 3 : Dossier médical partagé et dossier pharmaceutique

Article L. 1111-14

Afin de favoriser la prévention, la coordination, la qualité et la continuité des soins, les bénéficiaires de l'assurance maladie peuvent disposer, dans les conditions et sous les garanties prévues aux articles L. 1110-4 et L. 1110-4-1 et dans le respect du secret médical, d'un dossier médical partagé.

À cette fin, il est créé un identifiant du dossier médical partagé pour l'ensemble des bénéficiaires de l'assurance maladie.

Le dossier médical partagé est créé sous réserve du consentement exprès de la personne ou de son représentant légal.

La Caisse nationale de l'assurance maladie des travailleurs salariés assure la conception, la mise en œuvre et l'administration du dossier médical partagé, dans des conditions prévues par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés. Elle participe également à la conception, à la mise en œuvre et à l'administration d'un système de communication sécurisée permettant l'échange d'informations entre les professionnels de santé.

Ce dossier médical partagé est créé auprès d'un hébergeur de données de santé à caractère personnel agréé dans les conditions prévues à l'article L. 1111-8.

L'adhésion aux conventions nationales régissant les rapports entre les organismes d'assurance maladie et les professionnels de santé, prévues à l'article L. 162-5 du code de la sécurité sociale, et son maintien sont subordonnés à la consultation ou à la mise à jour du dossier médical partagé de la personne prise en charge par le médecin.

Les dispositions de l'alinéa précédent sont applicables dès que l'utilisation du dossier médical partagé est possible sur l'ensemble des territoires auxquels s'applique la présente section.

Article L. 1111-15

Dans le respect des règles déontologiques qui lui sont applicables ainsi que des articles L. 1110-4, L. 1110-4-1 et L. 1111-2, chaque professionnel de santé, quels que soient son mode et son lieu d'exercice, reporte dans le dossier médical partagé, à l'occasion de chaque acte ou consultation, les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge. À l'occasion du séjour d'une personne prise en charge, les professionnels de santé habilités des établissements de santé reportent dans le dossier médical partagé, dans le respect des obligations définies par la Haute Autorité de santé, un résumé des principaux éléments relatifs à ce séjour. Le médecin traitant mentionné à l'article L. 162-5-3 du code de la sécurité sociale verse périodiquement, au moins une fois par an, une synthèse dont le contenu est défini par la Haute Autorité de santé. La responsabilité du professionnel de santé ne peut être engagée en cas de litige portant sur l'ignorance d'une information qui lui était masquée dans le dossier médical partagé et dont il ne pouvait légitimement avoir connaissance par ailleurs.

Les données nécessaires à la coordination des soins issues des procédures de remboursement ou de prise en charge qui sont détenues par l'organisme dont relève chaque bénéficiaire de l'assurance maladie sont versées dans le dossier médical partagé.

Le dossier médical partagé comporte également des volets relatifs au don d'organes ou de tissus, aux directives anticipées mentionnées à l'article L. 1111-11 du présent code et à la personne de confiance mentionnée à l'article L. 1111-6.

Certaines informations peuvent être rendues inaccessibles par le titulaire du dossier médical partagé.

Article L. 1111-16

Le médecin coordonnateur mentionné au V de l'article L. 313-12 du code de l'action sociale et des familles a accès au dossier médical partagé de la personne hébergée dans l'établissement sous réserve de l'accord de celle-ci ou de son représentant légal.

Le médecin traitant mentionné à l'article L. 162-5-3 du code de la sécurité sociale dispose d'un droit d'accès au dossier médical partagé lui permettant d'accéder, par dérogation au dernier alinéa de l'article L. 1111-15 du présent code, à l'ensemble des informations contenues dans ce dossier.

Article L. 1111-17

I. - Les professionnels de santé accèdent au dossier médical partagé d'une personne hors d'état d'exprimer sa volonté, en présence d'une situation comportant un risque immédiat pour sa santé, sauf si cette personne avait auparavant manifesté son opposition expresse à ce que son dossier soit consulté ou alimenté dans une telle situation.

Le médecin régulateur du centre de réception et de régulation des appels d'aide médicale urgente mentionné à l'article L. 6311-2 qui reçoit un appel concernant une personne accède, sauf si cette personne avait auparavant manifesté son opposition expresse à ce que son dossier soit consulté dans une telle situation, au dossier médical partagé de celle-ci.

II. - Le professionnel de santé recueille, après avoir informé la personne concernée, son consentement pour qu'un autre professionnel de santé à qui il serait nécessaire de confier une partie de la prestation accède à son dossier médical partagé et l'alimente.

Article L. 1111-18

L'accès au dossier médical partagé ne peut être exigé en dehors des cas prévus aux articles L. 1111-15 et L. 1111-16, même avec l'accord de la personne concernée.

L'accès au dossier médical partagé est notamment interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties. L'accès à ce dossier ne peut également être exigé ni préalablement à la conclusion d'un contrat, ni à aucun moment ou à aucune occasion de son application.

Le dossier médical partagé n'est pas accessible dans le cadre de la médecine du travail.

Tout manquement aux présentes dispositions donne lieu à l'application des peines prévues à l'article 226-13 du code pénal.

Le dossier médical partagé est conservé pendant une durée de dix années à compter de sa clôture.

En cas de décès du titulaire, les ayants droit, le concubin ou le partenaire lié par un pacte civil de solidarité peuvent solliciter l'accès au dossier conformément au V de l'article L. 1110-4. L'accès à ce dossier peut également intervenir dans le cadre d'une expertise médicale diligentée aux fins d'administration de la preuve.

Article L. 1111-19

Le titulaire accède directement, par voie électronique, au contenu de son dossier.

Il peut également accéder à la liste des professionnels qui ont accès à son dossier médical partagé. Il peut, à tout moment, la modifier.

Il peut, à tout moment, prendre connaissance des traces d'accès à son dossier. (…)

Livre IV : Administration générale de la santé

Titre VI : Mise à disposition des données de santé

Chapitre préliminaire : Principes relatifs à la mise à disposition des données de santé

Article L. 1460-1

Les données de santé à caractère personnel recueillies à titre obligatoire et destinées aux services ou aux établissements publics de l'État ou des collectivités territoriales ou aux organismes de sécurité sociale peuvent faire l'objet de traitements à des fins de recherche, d'étude ou d'évaluation présentant un caractère d'intérêt public, dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Les traitements réalisés à cette fin ne peuvent avoir ni pour objet ni pour effet de porter atteinte à la vie privée des personnes concernées. Sauf disposition législative contraire, ils ne doivent en aucun cas avoir pour fin l'identification directe ou indirecte de ces personnes.

Les citoyens, les usagers du système de santé, les professionnels de santé, les établissements de santé et leurs organisations représentatives ainsi que les organismes participant au financement de la couverture contre le risque maladie ou réalisant des recherches, des études ou des évaluations à des fins de santé publique, les services de l'État, les institutions publiques compétentes en matière de santé et les organismes de presse ont accès aux données mentionnées au premier alinéa dans les conditions définies par la loi n° 78-17 du 6 janvier 1978 précitée et, le cas échéant, par les dispositions propres à ces traitements.

Chapitre I^er^ : Système national des données de santé

Article L. 1461-1

I. - Le système national des données de santé rassemble et met à disposition :

1° les données issues des systèmes d'information mentionnés à l'article L. 6113-7 du présent code ;

2° les données du système national d'information inter-régimes de l'assurance maladie mentionné à l'article L. 161-28-1 du code de la sécurité sociale ;

3° les données sur les causes de décès mentionnées à l'article L. 2223-42 du code général des collectivités territoriales ;

4° les données médico-sociales du système d'information mentionné à l'article L. 247-2 du code de l'action sociale et des familles ;

5° un échantillon représentatif des données de remboursement par bénéficiaire transmises par des organismes d'assurance maladie complémentaire et défini en concertation avec leurs représentants.

II. - Dans le cadre d'orientations générales définies par l'État, en concertation avec les organismes responsables des systèmes d'information et des données mentionnés au I, la Caisse nationale de l'assurance maladie des travailleurs salariés réunit et organise l'ensemble des données qui constituent le système national des données de santé mentionné au même I. Elle est responsable du traitement.

La méthode d'appariement des données mentionnées au 5° dudit I avec les données correspondantes du système national des données de santé est élaborée

en concertation avec les représentants des organismes qui transmettent les données concernées.

III. - 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° à l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité ;

2° à la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale ;

3° à la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales ;

4° à l'information des professionnels, des structures et des établissements de santé ou médico-sociaux sur leur activité ;

5° à la surveillance, à la veille et à la sécurité sanitaires ;

6° 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.

IV. - 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.

V. - 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.

Article L. 1461-2

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.

Par dérogation au premier alinéa du présent article, les données relatives à l'activité des professionnels de santé publiées par les organismes gestionnaires des régimes obligatoires de base d'assurance maladie, en application de l'article L. 162-1-11 du code de la sécurité sociale, sont réutilisées dans les conditions mentionnées aux articles L. 322-1 et L. 322-2 du code des relations entre le public et l'administration.

Article L. 1461-3

I. - Un accès aux données à caractère personnel du système national des données de santé ne peut être autorisé que pour permettre des traitements :

1° soit 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 ;

2° soit nécessaires à l'accomplissement des missions des services de l'État, des établissements publics ou des organismes chargés d'une mission de service public compétents, dans les conditions définies au III du présent article.

Le responsable de tels traitements n'est autorisé à accéder aux données du système national des données de santé et à procéder à des appariements avec ces données que dans la mesure où ces actions sont rendues strictement nécessaires par les finalités de la recherche, de l'étude ou de l'évaluation ou par les missions de l'organisme concerné.

Seules les personnes nommément désignées et habilitées à cet effet par le responsable du traitement, dans les conditions précisées par le décret en Conseil d'État mentionné à l'article L. 1461-7, sont autorisées à accéder aux données du système national des données de santé.

II. - Les traitements à des fins de recherche, d'étude ou d'évaluation mentionnés au 1° du I du présent article sont autorisés selon la procédure définie au chapitre IX de la loi n° 78-17 du 6 janvier 1978 précitée.

Les personnes produisant ou commercialisant des produits mentionnés au II de l'article L. 5311-1 du présent code ou les organismes mentionnés au 1° du A et aux 1°, 2°, 3°, 5° et 6° du B du I de l'article L. 612-2 du code monétaire et financier ainsi que les intermédiaires d'assurance mentionnés à l'article L. 511-1 du code des assurances sont tenus :

1° soit de démontrer que les modalités de mise en œuvre du traitement rendent impossible toute utilisation des données pour l'une des finalités mentionnées au V de l'article L. 1461-1 ;

2° soit de recourir à un laboratoire de recherche ou à un bureau d'études, publics ou privés, pour réaliser le traitement.

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.

L'accès aux données est subordonné :

a) 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 ;

b) à l'engagement du demandeur de communiquer au groupement d'intérêt public mentionné au même article L. 1462-1, dans un délai raisonnable après la fin de la recherche, de l'étude ou de l'évaluation, la méthode, les résultats de l'analyse et les moyens d'en évaluer la validité.

Le groupement d'intérêt public mentionné audit article L. 1462-1 publie sans délai l'autorisation de la Commission nationale de l'informatique et des libertés, la déclaration des intérêts, puis les résultats et la méthode.

III. - Le décret en Conseil d'État mentionné à l'article L. 1461-7 fixe la liste des services de l'État, 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. Ce décret précise, 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.

Article L. 1461-4

I. - Le système national des données de santé ne contient ni les noms et prénoms des personnes, ni leur numéro d'inscription au répertoire national d'identification des personnes physiques, ni leur adresse. Les numéros d'identification des professionnels de santé sont conservés et gérés séparément des autres données.

II. - Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les données à caractère personnel qui, en raison du risque d'identification directe des personnes concernées, sont confiées à un organisme distinct du responsable du système national des données de santé et des responsables des traitements.

Cet organisme est seul habilité à détenir le dispositif de correspondance permettant de réidentifier les personnes à partir des données du système national des données de santé. Il assure la sécurité de ce dispositif.

III. - La Commission nationale de l'informatique et des libertés peut autoriser l'accès aux données détenues par l'organisme mentionné au II du présent article, dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, quand il est nécessaire :

1° pour avertir une personne d'un risque sanitaire grave auquel elle est exposée ou pour lui proposer de participer à une recherche ;

2° pour la réalisation d'un traitement à des fins de recherche, d'étude ou d'évaluation si le recours à ces données est nécessaire, sans solution alternative, à la finalité du traitement et proportionné aux résultats attendus.

Article L. 1461-5

L'accès aux données de santé autres que celles mentionnées à l'article L. 1461-2 est gratuit pour :

1° les recherches, les études ou les évaluations demandées par l'autorité publique ;

2° les recherches réalisées exclusivement pour les besoins de services publics administratifs.

Article L. 1461-6

Pour les finalités de recherche, d'étude ou d'évaluation, la mise à disposition des données des composantes du système national des données de santé mentionnées aux 1° à 5° du I de l'article L. 1461-1 est régie par le présent chapitre.

Article L. 1461-7

Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés :

1° désigne les organismes chargés de gérer la mise à disposition effective des données du système national des données de santé et détermine leurs responsabilités respectives ;

2° dresse la liste des catégories de données réunies au sein du système national des données de santé et des modalités d'alimentation du système national des données de santé, y compris par les organismes d'assurance maladie complémentaire ;

3° fixe, dans les limites prévues au III de l'article L. 1461-3, la liste des services, des établissements ou des organismes bénéficiant de l'autorisation mentionnée au même III ;

4° fixe les conditions de désignation et d'habilitation des personnes autorisées à accéder au système national des données de santé ;

5° fixe les conditions de gestion et de conservation séparées des données permettant une identification directe des personnes en application de l'article L. 1461-4 et détermine l'organisme à qui sont confiées ces données ;

6° détermine les modalités selon lesquelles les organismes mentionnés au 1° du présent article garantissent à toute personne qui leur en fait la demande, en application de l'article 56 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, que ses données de santé à caractère personnel ne seront pas mises à disposition dans le cadre du 1° du I de l'article L. 1461-3 du présent code.

Chapitre II : Institut national des données de santé

Article L. 1462-1

Un groupement d'intérêt public, dénommé : « Institut national des données de santé », est constitué entre l'État, des organismes assurant une représentation des malades et des usagers du système de santé, des producteurs de données de santé et des utilisateurs publics et privés de données de santé, y compris des organismes de recherche en santé.

Il est notamment chargé :

1° de veiller à la qualité des données de santé et aux conditions générales de leur mise à disposition, garantissant leur sécurité et facilitant leur utilisation dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

2° d'assurer le secrétariat unique mentionné à l'article 54 de la même loi ;

3° d'émettre un avis sur le caractère d'intérêt public que présente une recherche, une étude ou une évaluation, dans les conditions prévues au même article 54 ;

4° de faciliter la mise à disposition d'échantillons ou de jeux de données agrégées mentionnées au V dudit article 54, dans des conditions préalablement homologuées par la Commission nationale de l'informatique et des libertés ;

5° de contribuer à l'expression des besoins en matière de données anonymes et de résultats statistiques, en vue de leur mise à la disposition du public.

Il publie chaque année un rapport transmis au Parlement.

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

(…)

Chapitre II : Conditions de licéité des traitements de données à caractère personnel

Section 2 : Dispositions propres à certaines catégories de données

Article 8

I. - Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I :

1° les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ;

2° les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ;

3° les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical :

- pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme ;

- sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ;

- et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ;

4° les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ;

5° les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;

6° les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ;

7° les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique et dans les conditions prévues à l'article 25 de la présente loi ;

8° les traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé selon les modalités prévues au chapitre IX.

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 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 du chapitre IX ne sont pas applicables.

IV. - De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et soit autorisés dans les conditions prévues au I de l'article 25 ou au II de l'article 26, soit déclarés dans les conditions prévues au V de l'article 22. (…)

Article 27

I. - Sont autorisés par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :

1° sous réserve du I bis de l'article 22 et du 9° du I de l'article 25, les traitements de données à caractère personnel mis en œuvre pour le compte de l'État, d'une personne morale de droit public ou d'une personne morale de droit privé gérant

un service public, qui portent sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ;

2° les traitements de données à caractère personnel mis en œuvre pour le compte de l'État qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

II. - Sont autorisés par arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, par décision de l'organe délibérant chargé de leur organisation, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :

1° sous réserve du I bis de l'article 22 et du 9° du I de l'article 25, les traitements mis en œuvre par l'État ou les personnes morales mentionnées au I qui requièrent une consultation du répertoire national d'identification des personnes physiques sans inclure le numéro d'inscription à ce répertoire ;

2° sous réserve du 9° du I de l'article 25, ceux des traitements mentionnés au I :

-qui ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9 ;

-qui ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents ;

-et qui sont mis en œuvre par des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, soit d'établir des statistiques ;

3° les traitements relatifs au recensement de la population, en métropole et dans les collectivités situées outre-mer ;

4° les traitements mis en œuvre par l'État ou les personnes morales mentionnées au I aux fins de mettre à la disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique définis à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, si ces traitements portent sur des données parmi lesquelles figurent le numéro d'inscription des personnes au répertoire national d'identification ou tout autre identifiant des personnes physiques.

III. - Les dispositions du IV de l'article 26 sont applicables aux traitements relevant du présent article.

IV. - Le 1° des I et II du présent article n'est pas applicable :

1° aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, qui sont soumis au chapitre IX de la présente loi ;

2° aux traitements mis en œuvre afin de répondre à une alerte sanitaire en cas de situation d'urgence, qui sont soumis au V de l'article 22. (…)

Chapitre IX : Traitements de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.

Article 53

Les traitements automatisés de données à caractère personnel ayant pour finalité la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention sont soumis à la présente loi, à l'exception des articles 23 et 24, du I de l'article 25 et des articles 26,32 et 38.

Toutefois, le présent chapitre n'est pas applicable :

1° aux traitements de données à caractère personnel ayant pour fin le suivi thérapeutique ou médical individuel des patients ;

2° aux traitements permettant d'effectuer des études à partir des données recueillies en application du 1° lorsque ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif ;

3° aux traitements effectués à des fins de remboursement ou de contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie ;

4° aux traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale, dans les conditions prévues au deuxième alinéa de l'article L. 6113-7 du code de la santé publique ;

5° aux traitements effectués par les agences régionales de santé, par l'État et par la personne publique désignée par lui en application du premier alinéa de l'article L. 6113-8 du même code, dans le cadre défini au même article ;

6° aux traitements mis en œuvre par les organismes ou les services chargés d'une mission de service public figurant sur une liste fixée par arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la Commission nationale de l'informatique et des libertés, afin de répondre à une alerte sanitaire, dans les conditions prévues au V de l'article 22.

Article 54

I. - Les traitements de données à caractère personnel ayant une finalité d'intérêt public de recherche, d'étude ou d'évaluation dans le domaine de la santé sont autorisés par la Commission nationale de l'informatique et des libertés, dans le respect des principes définis par la présente loi et en fonction de l'intérêt public que la recherche, l'étude ou l'évaluation présente.

II. - La Commission nationale de l'informatique et des libertés prend sa décision après avis :

1° du comité compétent de protection des personnes mentionné à l'article L. 1123-6 du code de la santé publique, pour les demandes d'autorisation relatives aux recherches impliquant la personne humaine mentionnées à l'article L. 1121-1 du même code ;

2° du comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé, pour les demandes d'autorisation relatives à des études ou à des évaluations ainsi qu'à des recherches n'impliquant pas la personne humaine, au sens du 1° du présent II.

Le comité d'expertise est composé de personnes choisies en raison de leur compétence, dans une pluralité de disciplines. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, précise la composition du comité et définit ses règles de fonctionnement. Il peut prévoir l'existence de plusieurs sections au sein du comité, compétentes en fonction de la nature ou de la finalité du traitement. Le comité d'expertise est soumis à l'article L. 1451-1 du code de la santé publique.

Le comité d'expertise émet, dans un délai d'un mois à compter de sa saisine, 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. Le cas échéant, le comité recommande aux demandeurs des modifications de leur projet afin de le mettre en conformité avec les obligations prévues par la présente loi. À défaut d'avis du comité dans le délai d'un mois, l'avis est réputé favorable. En cas d'urgence, ce délai peut être ramené à quinze jours.

Dans des conditions définies par décret en Conseil d'État, l'Institut national des données de santé, prévu à l'article L. 1462-1 du code de la santé publique, peut être saisi par la Commission nationale de l'informatique et des libertés ou le ministre chargé de la santé sur le caractère d'intérêt public que présente la recherche, l'étude ou l'évaluation justifiant la demande de traitement ; il peut également évoquer le cas de sa propre initiative. Dans tous les cas, il rend un avis dans un délai d'un mois à compter de sa saisine.

Les dossiers présentés dans le cadre du présent chapitre, à l'exclusion des recherches mentionnées aux 1° et 2° de l'article L. 1121-1 du code de la santé publique et de celles mentionnées au 3° du même article L. 1121-1 portant sur des produits mentionnés à l'article L. 5311-1 du même code, sont déposés auprès d'un secrétariat unique, qui assure leur orientation vers les instances compétentes.

III. - Pour chaque demande, la Commission nationale de l'informatique et des libertés vérifie les garanties présentées par le demandeur pour l'application des présentes dispositions et la conformité de sa demande à ses missions ou à son objet social. 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 pour ces données réduites.

La commission statue sur la durée de conservation des données nécessaires au traitement et apprécie les dispositions prises pour assurer leur sécurité et la garantie des secrets protégés par la loi.

IV. - Pour les catégories les plus usuelles de traitements automatisés de données de santé à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, la Commission nationale de l'informatique et des libertés peut homologuer et publier des méthodologies de référence destinées à simplifier la procédure d'examen. Celles-ci sont établies en concertation avec le comité d'expertise et des organismes publics et privés représentatifs des acteurs concernés.

V. - Des jeux de données agrégées ou des échantillons, issus des traitements des données de santé à caractère personnel pour des finalités et dans des conditions reconnues conformes à la présente loi par la Commission nationale de l'informatique et des libertés, peuvent faire l'objet d'une mise à disposition, dans des conditions préalablement homologuées par la commission, sans que l'autorisation prévue au I du présent article soit requise.

VI. - La commission peut, par décision unique, délivrer à un même demandeur une autorisation pour des traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques.

Article 55

Nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre les données à caractère personnel qu'ils détiennent dans le cadre d'un traitement de données autorisé en application de l'article 53.

Lorsque ces données permettent l'identification des personnes, leur transmission doit être effectuée dans des conditions de nature à garantir leur confidentialité. La Commission nationale de l'informatique et des libertés peut adopter des recommandations ou des référentiels sur les procédés techniques à mettre en œuvre.

La présentation des résultats du traitement de données ne peut en aucun cas permettre l'identification directe ou indirecte des personnes concernées.

Les données sont reçues par le responsable désigné à cet effet par la personne physique ou morale autorisée à mettre en œuvre le traitement. Ce responsable veille à la sécurité des informations et de leur traitement, ainsi qu'au respect de la finalité de celui-ci.

Les personnes appelées à mettre en œuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal.

Article 56

Toute personne a le droit de s'opposer à ce que des données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement de la nature de ceux qui sont visés à l'article 53.

Dans le cas où la recherche nécessite le recueil de prélèvements biologiques identifiants, le consentement éclairé et exprès des personnes concernées doit être obtenu préalablement à la mise en œuvre du traitement de données.

Les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, peuvent faire l'objet d'un traitement de données, sauf si l'intéressé a, de son vivant, exprimé son refus par écrit.

Article 57

I. - Les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont, avant le début du traitement de ces données, individuellement informées :

1° de la nature des informations transmises ;

2° de la finalité du traitement de données ;

3° des personnes physiques ou morales destinataires des données ;

4° du droit d'accès et de rectification institué aux articles 39 et 40 ;

5° du droit d'opposition institué aux premier et troisième alinéas de l'article 56 ou, dans le cas prévu au deuxième alinéa de cet article, de l'obligation de recueillir leur consentement.

Toutefois, ces informations peuvent ne pas être délivrées si, pour des raisons légitimes que le médecin traitant apprécie en conscience, le malade est laissé dans l'ignorance d'un diagnostic ou d'un pronostic grave.

II. - Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet que la recherche, l'étude ou l'évaluation, il peut être dérogé, sous réserve du III, à l'obligation d'information définie au I :

1° pour les traitements nécessaires à la conservation de ces données à des fins historiques, statistiques ou scientifiques, dans les conditions prévues au livre II du code du patrimoine ;

2° lorsque l'information individuelle se heurte à la difficulté de retrouver les personnes concernées.

Les demandes de dérogation à l'obligation d'informer les personnes de l'utilisation de données les concernant à des fins de recherche, d'étude ou d'évaluation sont justifiées dans le dossier de demande d'autorisation transmis à la Commission nationale de l'informatique et des libertés, qui statue sur ce point.

III. - Par dérogation au I, quand les recherches, les études ou les évaluations recourent à des données de santé à caractère personnel non directement identifiantes recueillies à titre obligatoire et destinées aux services ou aux établissements de l'État ou des collectivités territoriales ou aux organismes de sécurité sociale, l'information des personnes concernées quant à la réutilisation possible de ces données, à des fins de recherche, d'étude ou d'évaluation, et aux modalités d'exercice de leurs droits est assurée selon des modalités définies par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés.

Article 58

Sont destinataires de l'information et exercent les droits prévus aux articles 56 et 57 les titulaires de l'exercice de l'autorité parentale, pour les mineurs, ou le représentant légal, pour les personnes faisant l'objet d'une mesure de tutelle.

Par dérogation au premier alinéa du présent article, pour les traitements de données à caractère personnel réalisés dans le cadre de recherches mentionnées aux 2° et 3° de l'article L. 1121-1 du code de la santé publique ou d'études ou d'évaluations dans le domaine de la santé, ayant une finalité d'intérêt public et incluant des personnes mineures, l'information préalable prévue au I de l'article 57 de la présente loi peut être effectuée auprès d'un seul des titulaires de l'exercice

de l'autorité parentale, s'il est impossible d'informer l'autre titulaire ou s'il ne peut être consulté dans des délais compatibles avec les exigences méthodologiques propres à la réalisation de la recherche, de l'étude ou de l'évaluation au regard de ses finalités. Le présent alinéa ne fait pas obstacle à l'exercice ultérieur, par chaque titulaire de l'exercice de l'autorité parentale, des droits d'accès, de rectification et d'opposition.

Pour les mêmes traitements, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale aient accès aux données le concernant recueillies au cours de la recherche, de l'étude ou de l'évaluation. Le mineur reçoit alors l'information prévue aux articles 56 et 57 et exerce seul ses droits d'accès, de rectification et d'opposition.

Pour les traitements mentionnés au deuxième alinéa du présent article, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale soient informés du traitement de données si le fait d'y participer conduit à révéler une information sur une action de prévention, un dépistage, un diagnostic, un traitement ou une intervention pour laquelle le mineur s'est expressément opposé à la consultation des titulaires de l'autorité parentale en application des articles L. 1111-5 et L. 1111-5-1 du code de la santé publique ou si les liens de famille sont rompus et que le mineur bénéficie à titre personnel du remboursement des prestations en nature de l'assurance maladie et maternité et de la couverture complémentaire mise en place par la loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle. Il exerce alors seul ses droits d'accès, de rectification et d'opposition. (…)

2. Éléments de jurisprudence

2.1. – Jurisprudence de la Cour de justice de l'Union européenne

CJCE, 6 novembre 2003, *Bodil Lindqvist*, aff. C-101/01.

(…) 49. Par sa quatrième question, la juridiction de renvoi demande si l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, paragraphe 1, de la directive 95/46.

50. Eu égard à l'objet de cette directive, il convient de donner à l'expression « données relatives à la santé » employée à son article 8, paragraphe 1, une interprétation large de sorte qu'elle comprenne des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne.

51. Il convient donc de répondre à la quatrième question que l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, paragraphe 1, de la directive 95/46. (…)

2.2. – Jurisprudence du Conseil constitutionnel

Décision n° 99-416 DC du 23 juillet 1999, *loi portant création d'une couverture maladie universelle*.

(…) En ce qui concerne l'article 36 :

43. Considérant que l'article 36 modifie les articles L. 161-31 et L. 162-1-6 du code de la sécurité sociale relatifs au contenu et à l'utilisation d'une « carte électronique individuelle inter-régimes » ainsi qu'à sa délivrance à tout bénéficiaire de l'assurance maladie ;

44. Considérant que les requérants font grief à ce dispositif de porter atteinte au respect de la vie privée ; qu'ils font valoir que le système informatisé de transmission d'informations relatives à la santé des titulaires de la carte ne présente pas toutes les garanties et « comporte le risque d'être déjoué » ;

45. 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 ;

46. Considérant qu'aux termes du I de l'article L. 161-31 du code de la sécurité sociale, la carte électronique individuelle « *doit permettre d'exprimer de manière précise l'accord du titulaire ou de son représentant légal pour faire apparaître les éléments nécessaires non seulement à la coordination des soins mais aussi à un suivi sanitaire* » ; que le II du même article dispose : « *Dans l'intérêt de la santé*

du patient, cette carte comporte un volet de santé (...) destiné à ne recevoir que les informations nécessaires aux interventions urgentes ainsi que les éléments permettant la continuité et la coordination des soins » ; qu'en vertu du I de l'article L. 162-1-6 du code de la sécurité sociale, l'inscription, sur la carte, de ces informations est subordonnée dans tous les cas à l'accord du titulaire ou, s'agissant d'un mineur ou d'un majeur incapable, de son représentant légal ; que les personnes habilitées à donner cet accord peuvent, par ailleurs, « *conditionner l'accès à une partie des informations contenues dans le volet de santé à l'utilisation d'un code secret qu'elles auront-elles-mêmes établi* » ; que l'intéressé a accès au contenu du volet de santé par l'intermédiaire d'un professionnel de santé habilité ; qu'il dispose du droit de rectification, du droit d'obtenir la suppression de certaines mentions et du droit de s'opposer à ce que, en cas de modification du contenu du volet de santé, certaines informations soient mentionnées ; qu'en outre, il appartiendra à un décret en Conseil d'État, pris après avis public et motivé du Conseil national de l'Ordre des médecins et de la Commission nationale de l'informatique et des libertés, de fixer la nature des informations portées sur le volet de santé, les modalités d'identification des professionnels ayant inscrit des informations sur ce volet, ainsi que les conditions dans lesquelles, en fonction des types d'information, les professionnels de santé seront habilités à consulter, inscrire ou effacer les informations ; que la méconnaissance des règles permettant la communication d'informations figurant sur le volet de santé, ainsi que celle des règles relatives à la modification des informations, seront réprimées dans les conditions prévues par le VI de l'article L. 162-1-6 du code de la sécurité sociale ; que les sanctions pénales prévues par ces dernières dispositions s'appliqueront sans préjudice des dispositions de la section V du chapitre VI du titre II du livre deuxième du code pénal intitulée « Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques » ; qu'enfin, le législateur n'a pas entendu déroger aux dispositions de l'article 21 de la loi du 6 janvier 1978 susvisée relatives aux pouvoirs de surveillance et de contrôle de la Commission nationale de l'informatique et des libertés ;

47. Considérant que l'ensemble des garanties dont est assortie la mise en œuvre des dispositions de l'article 36 de la loi, au nombre desquelles il convient de ranger les caractéristiques assurant la sécurité du système, sont de nature à sauvegarder le respect de la vie privée ;

En ce qui concerne l'article 41 :

48. Considérant que cet article insère dans la loi susvisée du 6 janvier 1978 un chapitre V ter intitulé « Traitement des données personnelles de santé à des fins d'évaluation ou d'analyse des activités de soins et de prévention » comportant les articles 40-11 à 40-15 ; que ces articles définissent les modalités de communication, y compris à des personnes extérieures à l'administration, des données de santé en vue de permettre l'évaluation ou l'analyse des activités de soins et de prévention ; que l'article 40-12 établit en principe que « *les données issues des systèmes d'information visés à l'article L. 710-6 du code de la santé publique, celles issues des dossiers médicaux détenus dans le cadre de l'exercice libéral des professions de santé, ainsi que celles 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 » ; qu'il prévoit qu'il ne peut être dérogé à cette règle que sur autorisation de la Commission nationale de l'informatique et des libertés, les données utilisées ne pouvant, dans ce cas, comporter ni le nom, ni le prénom des personnes, ni leur numéro d'inscription au répertoire national d'identification des personnes physiques ; que les articles 40-13 à 40-15 déterminent les pouvoirs de contrôle de la Commission nationale de l'informatique et des libertés ; qu'en particulier, celle-ci doit s'assurer de la « *nécessité de recourir à des données personnelles 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* » ; que, dans l'hypothèse où le demandeur n'apporte pas d'éléments suffisants pour attester la nécessité de disposer de certaines informations parmi celles 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* » ; qu'elle dispose, à compter de sa saisine par le demandeur, d'un délai de deux mois, renouvelable une seule fois, pour se prononcer, son silence valant décision de rejet ;

49. Considérant que les requérants soutiennent qu'en subordonnant la communication de « *données statistiques anonymes* » à un « *avis conforme de la Commission nationale de l'informatique et des libertés* », l'article 41 porte atteinte à la liberté de communication énoncée à l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 ; qu'au surplus, cette formalité ne constitue pas, selon eux, « *une garantie suffisante pour éviter la rupture de l'anonymat* » ;

50. Considérant, en premier lieu, qu'il résulte des termes de la loi que les données de santé, si elles ne sont ni directement ni indirectement nominatives, peuvent être librement communiquées ; que manque donc en fait le moyen tiré de ce que la loi subordonne à autorisation de la Commission nationale de l'informatique et des libertés la communication de données ne permettant pas l'identification des personnes ;

51. Considérant, en second lieu, qu'il appartenait au législateur d'instituer une procédure propre à sauvegarder le respect de la vie privée des personnes, lorsqu'est demandée la communication de données de santé susceptibles de permettre l'identification de ces personnes ; qu'en subordonnant cette communication à autorisation de la Commission nationale de l'informatique et des libertés, le législateur, sans méconnaître l'article 11 de la Déclaration des droits de l'homme et du citoyen, a fixé en l'espèce des modalités assurant le respect de la vie privée ; (…)

Décision n° 2004-504 DC du 12 août 2004, *loi relative à l'assurance maladie*.

(…) - Sur l'article 3 :

2. Considérant que le I de l'article 3 de la loi déférée insère dans le code de la sécurité sociale les articles L. 161-36-1 à L. 161-36-4 ; que ces articles prévoient la création d'un dossier médical contenant des données à caractère personnel ; qu'ils précisent que le niveau de prise en charge des actes et prestations de soins par l'assurance maladie est subordonné à l'autorisation donnée par le patient

aux professionnels de santé d'accéder à son dossier et de le compléter ; qu'ils définissent les cas dans lesquels cet accès est autorisé ;

3. Considérant que les auteurs de la saisine soutiennent que ces articles méconnaissent le droit au respect de la vie privée ; qu'ils leur reprochent également de subordonner l'exercice du droit du patient à refuser l'accès à son dossier personnel à une réduction du remboursement des soins ; que, ce faisant, le législateur aurait porté atteinte « *au droit à la protection sociale garanti au titre du onzième alinéa du Préambule de la Constitution de 1946* » ;

4. Considérant qu'aux termes du onzième alinéa du Préambule de la Constitution de 1946, la Nation « *garantit à tous, notamment à l'enfant, à la mère et aux vieux travailleurs, la protection de la santé (...)* » ;

5. Considérant que 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 ce droit requiert que soit observée une particulière vigilance dans la collecte et le traitement de données à caractère personnel de nature médicale ; qu'il appartient toutefois au législateur de concilier, d'une part, le droit au respect de la vie privée et, d'autre part, les exigences de valeur constitutionnelle qui s'attachent tant à la protection de la santé, qui implique la coordination des soins et la prévention des prescriptions inutiles ou dangereuses, qu'à l'équilibre financier de la sécurité sociale ;

6. Considérant, en premier lieu, qu'aux termes du nouvel article L. 161-36-1 du code de la sécurité sociale, le dossier médical personnel est institué « afin de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé » et qu'il comportera notamment « des informations qui permettent le suivi des actes et prestations de soins » ainsi qu'un « volet spécialement destiné à la prévention » ; que, pour atteindre cet objectif, le nouvel article L. 161-36-2 prévoit que chaque professionnel de santé inscrira au dossier « les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge » ; qu'afin de favoriser la continuité de cette mise à jour, le législateur a subordonné le niveau de prise en charge des soins à l'autorisation donnée par le patient aux professionnels de santé d'accéder à son dossier et de le compléter ;

7. Considérant, en second lieu, que le dossier médical personnel sera élaboré « *dans le respect du secret médical* » ; qu'il résulte du renvoi à l'article L. 1111-8 du code de la santé publique que l'hébergement des données et la possibilité d'y accéder seront subordonnés au consentement de la personne concernée ; que le traitement des données sera soumis au respect des dispositions de la loi du 6 janvier 1978 susvisée ; que l'hébergeur devra faire l'objet d'un agrément ; que l'accès au dossier par un professionnel de santé sera soumis à l'observation des règles déontologiques ainsi que des dispositions des articles L. 1110-4 et L. 1111-2 du code de la santé publique, qui imposent notamment le respect de la vie privée et du secret des informations concernant le patient ; que l'accès au dossier médical en dehors des cas prévus par la loi sera puni des peines prévues à l'article 226-13 du code pénal ; que ces sanctions s'appliqueront sans préjudice des dispositions du code pénal relatives aux « atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques » ;

8. Considérant qu'eu égard aux finalités des dispositions contestées, qui sont, d'une part, d'améliorer la qualité des soins, d'autre part, de réduire le déséquilibre financier de l'assurance maladie, et compte tenu de l'ensemble des garanties qui viennent d'être rappelées, le législateur a opéré, entre les exigences constitutionnelles en cause, une conciliation qui n'apparaît pas manifestement déséquilibrée ; que, dès lors, les griefs invoqués doivent être rejetés ; (…)

2.3. – Jurisprudence du Conseil d'État

CE, ssr, 26 mai 2014, *Société IMS Health*, n° 354903.

1. Considérant que par une délibération du 8 septembre 2011, dont la société IMS Health demande l'annulation pour excès de pouvoir, la Commission nationale de l'informatique et des libertés (CNIL) a autorisé la société Celtipharm à mettre en œuvre un traitement de données issues des feuilles de soins anonymisées à bref délai, sur le fondement du III de l'article 8 et de l'article 25 de la loi du 6 janvier 1978 relative à l'informatique et aux libertés, ayant pour but la réalisation d'études statistiques relatives à la consommation de produits de santé ; qu'en vertu de cette délibération, les organismes concentrateurs techniques, qui assurent le routage des feuilles de soins électroniques vers les caisses d'assurance-maladie pour le compte et sur instruction des pharmaciens d'officine, transmettent également ces données à la société Celtipharm, après les avoir anonymisées par un processus de « hachage » irréversible, s'agissant des données identifiant les patients et sous forme cryptée, s'agissant de celles qui identifient les professionnels de santé ; que la société Celtipharm procède ensuite à une seconde anonymisation des données relatives aux patients, qui demeurent toutefois rattachables à un même individu anonyme via un identifiant unique ; qu'elle procède par ailleurs au décryptage puis à l'anonymisation des données identifiant les professionnels de santé ; que ce n'est qu'à l'issue de ce processus que la société Celtipharm procède au traitement des données contenues dans les feuilles de soins électroniques à des fins statistiques et de recherche scientifique ; (…)

Sur la légalité interne :

En ce qui concerne le moyen tiré de la violation du secret professionnel et de la vie privée des patients :

9. Considérant qu'aux termes de l'article 226-13 du code pénal : « *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende* » ; que, par ailleurs, les articles L. 161-36-1-A du code de la sécurité sociale et 1er de la loi du 6 janvier 1978 garantissent le droit au respect de la vie privée, qui implique le secret des données contenues dans les feuilles de soins électroniques ; que toutefois, dès lors que ces données font l'objet d'une anonymisation irréversible, le traitement autorisé par la délibération attaquée ne saurait avoir pour effet de porter atteinte au secret professionnel et au respect de la vie privée des patients ;

En ce qui concerne le moyen tiré du détournement du traitement des données issues des feuilles de soins électroniques à des fins purement commerciales :

10. Considérant qu'aux termes de l'article 226-21 du code pénal : « *Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte règlementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende* » ; que, selon le 2° de l'article 6 de la loi du 6 janvier 1978, les données à caractère personnel « *sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées* » ; qu'il résulte de ces dispositions que les traitements de données initialement collectées pour d'autre finalités à des fins statistiques ou de recherche scientifique sont réputés compatibles avec ces finalités initiales, sous les réserves énoncées au 2° de l'article 6 de la loi du 6 janvier 1978 ;

11. Considérant que le traitement autorisé par la délibération attaquée a pour but, ainsi qu'il a été dit au point 1, le traitement de données issues des feuilles de soins électroniques à des fins statistiques et de recherche scientifique en vue de la réalisation d'études relatives à la consommation de médicaments ; que, dès lors, un tel traitement doit être regardé comme compatible avec les finalités initiales de la collecte des données figurant dans les feuilles de soins électroniques en vertu des dispositions du 2° de l'article 6 de la loi du 6 janvier 1978 ; qu'au demeurant, dès lors que le traitement litigieux a été autorisé par délibération de la CNIL, l'utilisation, dans ce cadre, de données issues des feuilles des soins électroniques ne saurait relever du champ des infractions réprimées par l'article 226-21 du code pénal ; que, dans ces conditions, il ne saurait être reproché au traitement autorisé par la délibération attaquée d'organiser le détournement de leur finalité des informations figurant dans les feuilles de soins électroniques ; qu'il suit de là que le moyen tiré de la méconnaissance des dispositions de l'article 226-21 du code pénal doit être écarté ;

En ce qui concerne le moyen tiré de la méconnaissance, par la délibération attaquée, des dispositions de l'article 6 de la loi du 6 janvier 1978 :

12. Considérant qu'il résulte des motifs énoncés au point précédent que les finalités du traitement autorisé par la délibération attaquée, au demeurant conformes à la volonté du législateur, doivent être regardées comme légitimes eu égard à leur

objet, qui tend à l'amélioration de la connaissance relative à la consommation de produits de santé ; que les données collectées, dès lors qu'elle font l'objet d'un processus d'anonymisation, sont également adéquates, pertinentes et non excessives au regard des finalités poursuivies ; qu'il suit de là que le moyen tiré de la méconnaissance de l'article 6 de la loi de 1978 ne peut qu'être écarté ;

En ce qui concerne le moyen tiré de la méconnaissance de l'article 35 de la loi du 6 janvier 1978 :

13. Considérant qu'aux termes de l'article 35 de la loi du 6 janvier 1978 : « *les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable de traitement ou de celle du sous-traitant que sur instruction du responsable de traitement. / Toute personne traitant des données à caractère personnel pour le compte du responsable de traitement est considérée comme un sous-traitant au sens de la présente loi* » ; que, selon l'article 45-3 de la convention nationale organisant les rapports entre les pharmaciens titulaires d'officine et l'assurance-maladie, approuvée par arrêté du 11 juillet 2006 et adopté sur le fondement de l'article L. 161-34 du code de la sécurité sociale, « *le pharmacien peut recourir à un service informatique notamment par un contrat avec un organisme concentrateur technique (OCT). Cet organisme tiers agit pour le compte et sous la responsabilité du pharmacien dans le respect : / - des dispositions légales et règlementaires ayant trait plus particulièrement à l'informatique et aux libertés, ainsi qu'à la confidentialité et à l'intégrité des feuilles de soins électroniques ; / - des dispositions du cahier des charges OCT publié par le GIE SESAM-Vitale* » ;

14. Considérant que si la société requérante soutient que le traitement autorisé par la délibération qu'elle attaque est illégal en ce qu'il permettrait aux organismes concentrateurs techniques d'agir pour le compte de la société Celtipharm, l'anonymisation des données identifiant les patients et la transmission de ces données anonymisées ne peuvent être faites que sur instruction des pharmaciens d'officine participants, de même que la transmission des données cryptées identifiant les professionnels de santé aux fins d'anonymisation à bref délai par la société Celtipharm ; qu'il suit de là que le moyen tiré de la méconnaissance de l'article 35 de la loi de 1978 ne peut qu'être écarté ;

En ce qui concerne le moyen tiré du caractère illégal de la collecte et du traitement du numéro d'inscription au répertoire des personnes physiques par une entreprise privée :

15. Considérant que la délibération attaquée précise que les organismes concentrateurs techniques, qui collectent les données issues des feuilles de soins électroniques, procèdent ensuite à une première anonymisation de celles de ces données qui sont susceptibles d'identifier les patients, au nombre desquelles figure le numéro d'inscription au répertoire national des personnes physiques, avant de les transmettre à la société Celtipharm ;

16. Considérant que l'article R. 115-1 du code de la sécurité sociale énumère les personnes et organismes autorisés à utiliser le numéro d'inscription au répertoire national des personnes physiques ; qu'en vertu de l'article R. 115-2 de ce même code, cette autorisation vaut exclusivement pour les traitements énumérés à cet article, au nombre desquels ne figurent pas les traitements à des fins statistiques ou de recherche scientifique ;

17. Considérant, toutefois, que la loi du 6 janvier 1978, dans sa version issue de la loi du 6 août 2004, ne subordonne plus systématiquement la mise en œuvre de traitements de données à caractère personnel incluant le numéro d'inscription au répertoire national des personnes physiques à une autorisation par décret en Conseil d'État ; qu'en effet, certains d'entre eux peuvent désormais être autorisés par délibération de la CNIL, y compris en dehors des cas prévus par les dispositions du code de la sécurité sociale mentionnées au point 16 ; que tel est notamment le cas du traitement de données à caractère personnel à des fins statistiques et de recherche scientifique en litige, dont les finalités doivent, ainsi qu'il a été dit au point 10, être regardées comme compatibles avec les finalités initiales de la collecte des données qu'il contient, qui a été autorisé par la CNIL sur le fondement des dispositions combinées du III de l'article 8 de la loi du 6 janvier 1978 et de l'article 25 de cette même loi, auquel il renvoie ; qu'il suit de là que le moyen tiré de ce que la délibération attaquée autoriserait la collecte et le traitement du numéro d'inscription au répertoire national des personnes physiques dans des conditions illégales doit être écarté ; (…)

CE, ssr, 30 décembre 2015, *Société Les Laboratoires Servier*, n° 372230.

(…)1. Considérant qu'il ressort des pièces du dossier soumis aux juges du fond que la société Les Laboratoires Servier a demandé à la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS) la communication des données sources, issues du « système national d'information inter-régimes de l'assurance maladie », de deux études réalisées sous son égide, l'une intitulée « Benfluorex et valvulopathies cardiaques : une étude de cohorte sur un million de personnes traitées pour diabète » et publiée le 13 octobre 2010 sur *Wiley online library*, l'autre intitulée « Benfluorex, valvulopathies cardiaques et décès », et adressée le 28 septembre 2010 à l'Agence française de sécurité sanitaire des produits de santé ; que, par une décision du 2 février 2012, la CNAMTS a refusé la communication de ces données ; qu'à la suite de la saisine de la Commission d'accès aux documents administratifs et de l'avis défavorable émis par celle-ci le 19 avril 2012, la CNAMTS a confirmé son refus de communication par une décision implicite de rejet ; que, par le jugement attaqué du 15 juillet 2013, le tribunal administratif de Paris a rejeté la demande de la société Les Laboratoires Servier tendant à l'annulation de cette décision et à ce qu'il soit enjoint à la CNAMTS de lui communiquer ces données ;

2. Considérant qu'il résulte de l'article 37 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés que les dispositions de cette loi ne font, en principe, pas obstacle à l'application, au bénéfice de tiers, des dispositions du titre I^{er} de la loi du 17 juillet 1978, relatif à la liberté d'accès aux documents

administratifs et à la réutilisation des informations publiques ; que lorsque des données à caractère personnel ont également le caractère de documents administratifs, elles ne sont communicables aux tiers, en vertu du III de l'article 6 de la loi du 17 juillet 1978, que s'il est possible d'occulter ou de disjoindre les mentions portant atteinte, notamment, à la protection de la vie privée ou au secret médical ; qu'il ne peut être accédé à une demande de communication sur le fondement de la loi du 17 juillet 1978 que si le traitement nécessaire pour rendre impossible, s'agissant de données de santé, toute identification, directe ou indirecte, de l'une quelconque des personnes concernées, y compris par recoupement avec d'autres données, n'excède pas l'occultation ou la disjonction des mentions non communicables, seule envisagée par cette loi ; que, dans le cas contraire, sont seules applicables les dispositions de la loi du 6 janvier 1978 et des lois spéciales applicables au traitement de certaines catégories de données, notamment, en ce qui concerne les données de santé à caractère personnel, les chapitres IX et X de la loi du 6 janvier 1978 ; qu'il suit de là que, contrairement à ce que soutient la CNAMTS, la seule circonstance que les données en cause soient issues du système national d'information inter-régimes de l'assurance maladie ne faisait pas, par elle-même, obstacle à ce qu'elles soient communiquées sur le fondement de la loi du 17 juillet 1978, si les conditions posées par cette loi étaient réunies ;

3. Considérant qu'il résulte des articles 1er et 2 de la loi du 17 juillet 1978 que l'État, les collectivités territoriales ainsi que les autres personnes de droit public et les personnes de droit privé chargées d'une mission de service public sont tenues de communiquer aux personnes qui en font la demande les documents administratifs qu'elles détiennent, définis comme les documents produits ou reçus dans le cadre de leur mission de service public, quels qu'en soient la forme et le support, sous réserve des dispositions de l'article 6 de cette loi ; qu'aux termes du I de l'article 6 de la même loi : « *Ne sont pas communicables : (...) 2° Les autres documents administratifs dont la consultation ou la communication porterait atteinte : (...) f) Au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, sauf autorisation donnée par l'autorité compétente* » ;

4. Considérant qu'il résulte de ces dernières dispositions que la seule circonstance que la communication d'un document administratif soit de nature à affecter les intérêts d'une partie à une procédure juridictionnelle ou qu'un document ait été transmis à une juridiction dans le cadre d'une instance engagée devant elle ne fait pas obstacle à sa communication ; que, toutefois, il revient à la personne chargée d'une mission de service public qui est sollicitée pour communiquer des documents qu'elle détient de vérifier notamment, au cas par cas et selon les circonstances de l'espèce, si leur communication risquerait d'empiéter sur les compétences et prérogatives d'une autorité judiciaire ou d'une juridiction, auxquelles il appartient seules, dans le cadre des procédures engagées devant elles et en vertu des principes et des textes qui leur sont applicables, d'assurer le respect des droits de la défense et le caractère contradictoire de la procédure ;

5. Considérant qu'il ressort des pièces du dossier soumis aux juges du fond que les études en cause avaient été produites dans le cadre de l'information judicaire ouverte contre la société Les Laboratoires Servier, mise en examen, et qu'elles faisaient l'objet d'une expertise judiciaire en cours dans le cadre de cette information judiciaire ; qu'en outre, l'identification des effets secondaires du Mediator, spécialité pharmaceutique contenant du benfluorex que la société Les Laboratoires Servier avait commercialisée avant son retrait du marché, constituait un élément essentiel de la caractérisation des éléments matériels de l'infraction pour laquelle elle était ainsi poursuivie ; qu'en jugeant que la communication demandée était de nature à porter atteinte au déroulement d'une procédure juridictionnelle, au sens du f) du 2° du I de l'article 6 de la loi du 17 juillet 1978, le tribunal administratif de Paris, qui a suffisamment motivé son jugement, n'a pas commis d'erreur de droit (…) ;

CE, cr, 20 mai 2016, *Société Celtipharm*, n° 385305.

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 œuvre du Système national d'information inter-régimes 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 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 inter-régimes 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 inter-régimes 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 œuvre 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 œuvre, 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 règlementaire, 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 (…) ;

CE, cr, 17 novembre 2017, *Fondation Jérôme Lejeune et autres*, n° 401212.

(…)

1. Aux termes de l'article L. 2131-1 du code de la santé publique : « *I. - Le diagnostic prénatal s'entend des pratiques médicales, y compris l'échographie obstétricale et fœtale, ayant pour but de détecter in utero chez l'embryon ou le fœtus une affection d'une particulière gravité. / II. - Toute femme enceinte reçoit, lors d'une consultation médicale, une information loyale, claire et adaptée à sa situation sur la possibilité de recourir, à sa demande, à des examens de biologie médicale et d'imagerie permettant d'évaluer le risque que l'embryon ou le fœtus présente une affection susceptible de modifier le déroulement ou le suivi de sa grossesse. (…)* ». Aux termes de l'article L. 2131-5 du même code : « *Sauf disposition contraire, les modalités d'application du présent chapitre sont déterminées par décret en Conseil d'État et notamment : (…) 2° La*

nature des examens de biologie médicale destinés à établir un diagnostic prénatal et les conditions dans lesquelles ils peuvent être pratiqués dans les établissements publics de santé et les laboratoires de biologie médicale autorisés (…) ». Enfin, aux termes de l'article L. 1418-1 du même code : « *L'Agence de la biomédecine (…) est compétente dans les domaines de la greffe, de la reproduction, de l'embryologie et de la génétique humaines. Elle a notamment pour missions : (…) 4° De suivre, d'évaluer et, le cas échéant, de contrôler les activités médicales et biologiques (…) relevant de sa compétence et de veiller à la transparence de ces activités (…)* ».

2. Par un décret du 3 mai 2016, le Premier ministre a introduit dans le code de la santé publique un article R. 2131-2-3 renvoyant à un arrêté du ministre chargé de la santé le soin de préciser, notamment, les conditions dans lesquelles, à des fins de contrôle de qualité des mesures échographiques dont les résultats sont combinés avec ceux des marqueurs sériques maternels et d'évaluation de leurs résultats, sont transmises, par les praticiens effectuant les examens de cytogénétique, aux biologistes médicaux effectuant les examens de biochimie portant sur les marqueurs sériques maternels les données utiles à l'évaluation et au contrôle de qualité, ces derniers transmettant à l'Agence de la biomédecine les données anonymisées dont ils sont détenteurs ou destinataires, en vue de l'exercice par l'agence de sa mission d'évaluation du diagnostic prénatal, et cette agence transmettant, d'une part, ces données aux organismes intervenant dans le processus de contrôle de qualité et, d'autre part, des données agrégées issues de l'évaluation qu'elle réalise aux autorités sanitaires compétentes et aux organismes intervenant dans le processus de contrôle de qualité. Par un arrêté du 11 mai 2016, pris sur le fondement des dispositions de cet article, le ministre des affaires sociales et de la santé a notamment précisé les données transmises par les biologistes médicaux et leurs destinataires, ainsi que les données transmises par l'Agence de la biomédecine et leurs destinataires. La fondation Jérôme Lejeune et les autres requérants demandent l'annulation pour excès de pouvoir de ce décret et de cet arrêté. (…)

9. En premier lieu, les dispositions critiquées du décret et de l'arrêté attaqués se bornent à prévoir la transmission de données aux fins du contrôle de qualité et de l'évaluation des résultats d'examens de dépistage utilisant les marqueurs sériques maternels. De telles dispositions, qui répondent à l'objectif d'intérêt général tenant à l'amélioration des pratiques des professionnels concernés et à la recherche d'une plus grande fiabilité des tests de dépistage, en vue notamment du moindre recours aux méthodes invasives de diagnostic telles que les amniocentèses, ne portent, par elles-mêmes, aucune atteinte au principe constitutionnel du respect de la dignité de la personne humaine ni aux principes de droit à la vie ou de non-discrimination protégés notamment par les stipulations des articles 2 et 14 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales

10. En deuxième lieu, 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, tout comme les stipulations de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. 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, ainsi que le rappelle d'ailleurs l'article 6 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

11. Les dispositions de l'arrêté litigieux prévoient, en modifiant le point 4.3 de l'annexe de l'arrêté du 23 juin 2009 fixant les règles de bonnes pratiques en matière de dépistage et de diagnostic prénatals avec utilisation des marqueurs sériques maternels de la trisomie 21, la transmission à l'Agence de la biomédecine, par les biologistes médicaux chargés du calcul de risque de la trisomie 21, de données portant sur l'identification du laboratoire autorisé à effectuer les examens en cause, le code d'anonymisation attribué par ce laboratoire aux résultats individuels des examens de dépistage et, le cas échéant, de diagnostic, le numéro identifiant de l'échographiste, la date de naissance de la femme enceinte examinée, cet élément étant nécessaire au calcul du risque, enfin les différents résultats obtenus à la suite de ces examens ainsi que leurs dates de réalisation. D'une part, l'arrêté, qui ne dispense pas le responsable des traitements de données à caractère personnel qu'il implique du respect des formalités prévues par la loi du 6 janvier 1978, rappelle la nécessité de prendre les mesures nécessaires pour garantir, dans le respect des dispositions de cette loi, la confidentialité et la sécurité des données recueillies, conservées et mises à disposition. D'autre part, le recueil des données considérées, en vue de leur analyse et de leur agrégation par l'Agence de la biomédecine, prévues au point 7 de l'arrêté, dans le cadre de sa mission d'évaluation du dépistage de la trisomie 21, répond, de manière adéquate et proportionnée, à l'objectif d'intérêt général mentionné au point 9. En particulier, contrairement à ce qui est soutenu, ces données ne portent pas sur l'issue des grossesses et la durée de leur conservation ne doit pas, en toute hypothèse, excéder le délai nécessaire à la poursuite de cet objectif. De même, en ce qu'il prévoit, aux points 7.3 et 7.4 qu'il ajoute à l'annexe de l'arrêté du 23 juin 2009, que chaque réseau de périnatalité et chaque organisme agréé par la Haute Autorité de santé pour l'accréditation de la qualité de la pratique professionnelle pour les spécialités concernées par le dépistage et le diagnostic prénatal de la trisomie 21 se voit communiquer par l'Agence de la biomédecine les données transmises par les biologistes médicaux chargés du calcul de risque portant sur la population suivie par les professionnels adhérant au réseau ou concernant les échographistes ayant adhéré au programme d'assurance qualité de cet organisme, en complément des résultats obtenus par l'Agence, l'arrêté met en œuvre de manière adéquate et proportionnée l'objectif d'intérêt général poursuivi.

12. En revanche, alors que l'arrêté attaqué prévoit également, au point 4.3 de l'annexe à l'arrêté du 23 juin 2009 qu'il modifie, la mise à disposition de la Fédération française des réseaux de périnatalité et de tous les organismes agréés par la Haute Autorité de santé de l'ensemble des données recueillies sur le territoire national, transmises par les biologistes médicaux, le ministre chargé de la santé n'a apporté aucun élément, en dépit de la mesure supplémentaire d'instruction diligentée par la 1re chambre de la section du contentieux, mettant le Conseil d'État en mesure de vérifier qu'une telle mise à dispositions de l'ensemble des données à caractère personnel en cause serait nécessaire à la poursuite de l'objectif poursuivi, et qu'ainsi

les obligations découlant du droit des personnes au respect de leur vie privée auraient été respectées. Par suite, en l'absence de toute justification apportée en défense sur ce point, les requérants sont fondés à demander l'annulation des dispositions du point 4.3 de l'annexe à l'arrêté du 23 juin 2009 modifié prévoyant cette mise à disposition, lesquelles sont divisibles du reste de l'arrêté attaqué.

13. En troisième lieu, aux termes de l'article 7 de la loi du 6 janvier 1978 : « *Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes : (…) / 3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ; / (…) / 5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée* ». D'une part, les traitements de l'ensemble des données qu'impliquent les dispositions de l'arrêté attaqué autres que celles annulées au point 12, qui doivent être mis en œuvre dans le respect des dispositions de la loi du 6 janvier 1978, modifiée notamment par la loi du 26 janvier 2016 de modernisation de notre système de santé, relatives aux conditions de l'information des personnes auprès desquelles sont recueillies des données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, sont nécessaires à l'exécution de la mission de service public confiée par la loi à l'Agence de la biomédecine. D'autre part, et alors qu'il résulte de ce qui a été dit ci-dessus qu'ils ne méconnaissent pas l'intérêt et les droits et libertés fondamentaux des personnes concernées, ces traitements sont également nécessaires à la mission d'intérêt général poursuivie par les réseaux de santé en périnatalité et les organismes agréés par la Haute Autorité de santé pour l'accréditation de la qualité de la pratique professionnelle pour les spécialités concernées. Par suite, les requérants ne sont pas fondés à soutenir que, faute d'avoir subordonné la transmission des données considérées au consentement des personnes concernées, le décret et l'arrêté attaqué méconnaîtraient l'article 7 de la loi du 6 janvier 1978. (…)

CE, ssr, 22 octobre 2014, *Section française de l'observatoire international des prisons*, n° 362681.

(…) 5. Considérant qu'aux termes de l'article L. 1110-4 du code de la santé publique : « *Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant. / Excepté dans les cas de dérogation, expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé (…)* » ; qu'en vertu des articles 226-13 et 226-14 du code pénal, la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire est pénalement sanctionnée, sauf dans les cas où la loi impose ou autorise la révélation du secret ; qu'aux termes de l'article 45 de la loi du 24 novembre 2009 pénitentiaire : « *L'administration pénitentiaire respecte le droit au secret médical des personnes détenues ainsi que le secret de la consultation, dans le respect des troisième et quatrième alinéas de l'article L. 6141-5 du code de la santé publique* » ;

6. Considérant, en premier lieu, qu'en vertu de l'article 22 de la loi du 24 novembre 2009 pénitentiaire, l'état de santé des détenus doit être pris en compte dans les restrictions apportées à l'exercice de leurs droits du fait des contraintes inhérentes à la détention, du maintien de la sécurité et du bon ordre des établissements, de la prévention de la récidive et de la protection de l'intérêt des victimes ; que l'article 46 de la même loi dispose que : « *(…) L'état psychologique des personnes détenues est pris en compte lors de leur incarcération et pendant leur détention. L'administration pénitentiaire favorise la coordination des différents intervenants agissant pour la prévention et l'éducation sanitaires. Elle assure un hébergement, un accès à l'hygiène, une alimentation et une cohabitation propices à la prévention des affections physiologiques ou psychologiques* » ; qu'en vertu de l'article 717-1 du code de procédure pénale, les personnes détenues font l'objet d'une période d'observation pluridisciplinaire à leur accueil dans l'établissement pénitentiaire et leur état de santé est pris en compte pour leur répartition dans les prisons pour peines et pour leur régime de détention ;

7. Considérant que la circulaire attaquée prévoit que les professionnels de santé peuvent informer les professionnels de l'administration pénitentiaire et de la protection judiciaire de la jeunesse de la réalisation des visites médicales règlementaires, des handicaps et incapacités du détenu nécessitant une adaptation de ses conditions de détention, de la nécessité de lui remettre des médicaments et documents médicaux avant sa libération et de l'existence d'un projet de soins, en vue de le mettre en cohérence avec le projet de sortie ; qu'elle prévoit également une information systématique sur les cas de maladie contagieuse, en vue de prendre des mesures préventives, sur les matériels médicaux nécessaires à la vie quotidienne du détenu en cas de pathologie chronique, sur la nécessité d'un hébergement et sur sa nature en cas de demande de suspension de peine pour raison médicale et sur l'existence d'une ordonnance justifiant la présence de médicaments en cellules ; que, dans cette mesure, la circulaire se borne à mentionner les informations qui doivent être communiquées aux professionnels de l'administration pénitentiaire ou de la protection judiciaire de la jeunesse pour permettre la prise en compte de l'état de santé du détenu majeur ou mineur lors de sa détention et pour la préparation de sa libération ainsi que le maintien de conditions de détention propices à la prévention des affections physiologiques ; que la communication de telles informations est la conséquence nécessaire des dispositions législatives mentionnées au point 6 ; qu'il appartient au chef d'établissement, spontanément ou à la demande du professionnel de santé, de veiller, lorsque ces questions sont évoquées au cours d'une réunion de la commission pluridisciplinaire unique ou de l'équipe pluridisciplinaire, à ce que n'y participent que les professionnels ayant besoin de disposer de ces informations dans l'accomplissement de leurs missions ; que, par suite, l'association requérante n'est pas fondée à soutenir que la circulaire attaquée apporterait sur ces points une restriction illégale au secret médical ;

8. Considérant, en deuxième lieu, qu'aux termes du premier alinéa de l'article 44 de la loi du 24 novembre 2009 : « *L'administration pénitentiaire doit assurer à chaque personne détenue une protection effective de son intégrité physique en tous lieux collectifs et individuels* » ; qu'en vertu des troisième et quatrième

alinéas de l'article L. 6141-5 du code de la santé publique, « *dès lors qu'il existe un risque sérieux pour la sécurité des personnes* » dans un établissement public de santé destiné à l'accueil des personnes incarcérées, « *les personnels soignants intervenant au sein de ces établissements et ayant connaissance de ce risque sont tenus de le signaler dans les plus brefs délais au directeur de l'établissement en lui transmettant, dans le respect des dispositions relatives au secret médical, les informations utiles à la mise en œuvre de mesures de protection* » et « *les mêmes obligations sont applicables aux personnels soignants intervenant au sein des établissements pénitentiaires* » ;

9. Considérant que la circulaire attaquée prévoit que les professionnels de santé peuvent informer les personnels de l'administration pénitentiaire et de la protection judiciaire de la jeunesse, sans donner d'indication sur le diagnostic, de l'existence d'un risque sérieux pour le détenu ou pour autrui et des principaux signes d'alerte à surveiller en vue d'obtenir une demande de surveillance renforcée ponctuelle pour un patient présentant un problème psychiatrique ou somatique ; qu'elle prévoit également que les professionnels de l'administration pénitentiaire et de la protection judiciaire de la jeunesse ont besoin d'être informés, pour accomplir leurs missions, d'un risque suicidaire, en vue de mettre en œuvre un suivi spécifique, et d'un risque de dangerosité, en vue de prévenir des agressions ; que doivent être ainsi communiquées les seules informations utiles à la mise en œuvre de mesures de protection ; qu'une telle communication est la conséquence nécessaire de l'obligation incombant au service public pénitentiaire en vertu de la loi d'assurer la protection effective de l'intégrité physique des personnes détenues ; qu'il appartient au directeur de l'établissement, destinataire de l'information en vertu de l'article L. 6141-5 du code de la santé publique, de veiller à ce qu'elle soit communiquée, si elle est évoquée au cours d'une réunion de la commission pluridisciplinaire unique ou de l'équipe pluridisciplinaire, aux seuls professionnels ayant besoin d'en disposer pour l'accomplissement de leurs missions ; que, dans ces conditions, la circulaire n'apporte pas sur ces points une restriction illégale au secret médical ;

10. Considérant, en troisième lieu, qu'aux termes de l'article 226-14 du code pénal : « *L'article 226-13 (…) n'est pas applicable : / 1° À celui qui informe les autorités judiciaires, médicales ou administratives de privations ou de sévices (…) dont il a eu connaissance et qui ont été infligées à un mineur ou à une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son incapacité physique ou psychique ; / 2° Au médecin qui, avec l'accord de la victime, porte à la connaissance du procureur de la République les sévices ou privations qu'il a constatés, sur le plan physique ou psychique, dans l'exercice de sa profession et qui lui permettent de présumer que des violences physiques, sexuelles ou psychiques de toute nature ont été commises. Lorsque la victime est un mineur ou une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son incapacité physique ou psychique, son accord n'est pas nécessaire (…)* » ; qu'aux termes du premier alinéa de l'article R. 4127-44 du code de la santé publique : « *Lorsqu'un médecin discerne qu'une personne auprès de laquelle il est appelé est victime de sévices ou de privations, il doit mettre en œuvre les moyens les plus adéquats pour la protéger en faisant preuve de prudence et de circonspection* » ; qu'aux termes du premier

alinéa de l'article R. 4127-10 du même code : « *Un médecin amené à examiner une personne privée de liberté ou à lui donner des soins ne peut, directement ou indirectement, serait-ce par sa seule présence, favoriser ou cautionner une atteinte à l'intégrité physique ou mentale de cette personne ou à sa dignité* » ; que les deuxième et troisième alinéas du même article imposent au médecin d'informer l'autorité judiciaire dans l'hypothèse prévue par le 2° de l'article 226-14 du code pénal ;

11. Considérant que, sans préjudice de l'obligation qui incombe, en vertu de l'article L. 6141-5 du code de la santé publique cité au point 8, aux personnels soignants intervenant au sein d'un établissement public de santé destiné à l'accueil des personnes incarcérées ayant connaissance d'un risque sérieux pour la sécurité des personnes d'en avertir dans les plus brefs délais le directeur de l'établissement, la circulaire attaquée mentionne, au titre des informations qui peuvent être communiquées par les professionnels de santé aux personnels de l'administration pénitentiaire et de la protection judiciaire de la jeunesse, les informations sur « *les personnes détenues victimes de maltraitance* », en rappelant l'obligation déontologique découlant de l'article R. 4127-10 du code de la santé publique ; que, d'une part, la circulaire n'impose pas la communication de telles informations mais se borne à mentionner qu'elle est possible ; que, d'autre part, il appartient aux médecins d'apprécier dans chaque situation les moyens les plus adéquats pour protéger le détenu victime de mauvais traitements et les informations devant, à cette fin, être communiquées en vue, notamment, d'une modification ou d'un aménagement de ses conditions de détention, ainsi que les personnes auxquelles elles doivent être communiquées ; que, par suite, l'association requérante n'est pas fondée à soutenir que la circulaire apporterait, sur ce point, une restriction illégale au secret médical et méconnaîtrait les dispositions de l'article R. 4127-10 du code de la santé publique ;

3. Rapports

3.1. – P.-L. Bras, Rapport sur la gouvernance et l'utilisation des données de santé, septembre 2013

(…) Synthèse

La première partie du rapport est un constat :

En premier lieu, elle rappelle (1.1) les finalités initiales des bases SNIIRAM et PMSI, décrit leur réunion en une grande base – appelée Système d'information (SI) dans la suite du rapport –, détaille son contenu et son organisation (1.2), sa richesse exceptionnelle et ses limitations (1.3).

En second lieu, elle expose les difficultés actuelles, juridiques et pratiques, d'accès aux données :

- comment, dans une base supposée anonyme, il peut exister un risque de réidentification indirecte des personnes (2.1) ;
- ce qu'est le régime actuel des droits d'accès aux SI, ce que sont ses origines, sa complexité et ses défauts (2.2) ;
- pourquoi les contraintes actuelles sur l'emploi du NIR (numéro de sécurité sociale) protègent moins les données personnelles qu'elles n'entravent les recherches (2.3) ;
- pourquoi enfin la difficulté d'accéder aux données n'est pas seulement juridique mais liée aussi à leur complexité et à l'insuffisance des services de mise à disposition et de mise en forme des données (2.4).

La seconde partie du rapport présente les enjeux et les propositions :

Les enjeux (1) sont, d'une part, le risque de réidentification et le risque de mésusage et, d'autre part, les grands bénéfices démocratiques, sanitaires et économiques dont est porteur le SI.

Au terme d'une revue critique des arguments, les principes proposés (2) sont les suivants :

- le SI a des finalités très larges et constitue donc un bien public qui ne peut être approprié par aucun des acteurs du système. Il doit être administré dans l'intérêt commun par une autorité légitime en concertation avec l'ensemble des parties prenantes ;
- dès lors que les données présentent un risque de réidentification des patients, l'accès doit en être restreint ;

- les lots de données qui ne présentent pas un tel risque de réidentification doivent être communicables à tous ou rendus publics ;
- la diffusion des tarifs moyens des professionnels de santé ne devra plus être réservée à l'assurance maladie mais le débat sur la transparence des données nominatives relatives à l'activité des professionnels mérite d'être ouvert dans un cadre concerté avec les intéressés.

Pour mettre en œuvre ces principes, il est proposé (3) :

- de distinguer autant que possible les lots de données clairement anonymes des lots de données indirectement nominatifs. À partir d'une expertise publique sur les risques de réidentification, les lots de données qui peuvent sans risques être communiqués ou rendus publics seront définis sous le contrôle de la CNIL ;
- d'ouvrir l'accès aux lots de données anonymes en distinguant la publication (gratuite) et des extractions ou des tableaux de bord à façon (payants) ;
- de limiter l'accès aux données indirectement nominatives du SI, avec pour critères la finalité d'intérêt public, la qualité du protocole, le besoin d'accéder aux données, la sécurité des procédures et la qualité du demandeur :
  - les droits d'accès permanents seront accordés par le ministre de la santé sous le contrôle de la CNIL aux organismes publics, à partir d'une appréciation de l'équilibre entre les risques (réidentification) et les bénéfices (vigilance sanitaire, connaissance médico-économique) ;
  - les organismes de vigilance sanitaire (ANSM, INVS, HAS) doivent se donner les moyens d'exploiter pleinement le potentiel du SI ;
  - les droits d'accès ponctuels seront accordés, par un dispositif unique qui permettra de vérifier que le « bénéfice » collectif potentiel attendu de la recherche envisagée justifie la mise à disposition des données, avec des moyens accrus, pour un contrôle a priori des risques de mésusage ;
  - les appariements autorisés dans le cadre cette procédure ne nécessiteront pas de décret en Conseil d'État ;
  - les données seront hébergées dans des conditions sûres et les procédures d'accès seront sécurisées ;
- si ces orientations sont retenues, à l'issue de la concertation avec les parties prenantes, leur mise en œuvre impliquera des modifications législatives concernant notamment :
  - les dispositions relatives au SNIIRAM et au PMSI dans les codes de la sécurité sociale et de la santé ;
  - les dispositions de la loi « informatique et libertés » relatives à la recherche en santé, à l'analyse et à l'évaluation des activités de soins et de prévention ainsi qu'à l'emploi du NIR ;
- l'exploitation du potentiel exceptionnel de la base et le développement des usages, spécialement pour les chercheurs, passent par un plan d'urbanisation du SI et la mise en place d'une grande plateforme de services aux utilisateurs ;

- les besoins et les priorités pour l'élargissement du périmètre du SI seront déterminés en concertation avec les parties prenantes.

Enfin sont proposées (4) les grandes lignes d'un modèle économique et institutionnel :

- pour couvrir les coûts de fonctionnement, les accès à la base sécurisée, les extractions et les travaux à façon donneront lieu à paiement par l'organisme commanditaire de l'étude. Cela s'appliquera aussi aux laboratoires pharmaceutiques ;
- trois solutions institutionnelles alternatives sont proposées à la discussion pour l'organisation de la base et du guichet associé :
  - une structure autonome,
  - une structure adossée à la CNAMTS mais disposant de moyens dédiés,
  - Une structure adossée à la direction statistique du ministère des affaires sociales, la DREES ;
- Une gouvernance qui relèvera en dernière instance des ministres chargés de la santé et de la sécurité sociale, s'appuyant sur un Haut Conseil des données de santé réunissant les parties prenantes et doté d'un Conseil scientifique.

3.2. - Rapport de la commission « Open data en santé », 9 juillet 2014

(…) Conclusion

Les travaux de la Commission ont permis de mesurer le consensus existant sur les impacts positifs d'une plus grande ouverture et d'une meilleure utilisation des différents types de données produites par le système de santé, qui permettent d'attendre de nombreux bénéfices en termes de démocratie sanitaire, de renforcement de l'autonomie des patients, de développement de la recherche et de l'innovation, d'efficacité de l'action publique et d'amélioration des pratiques professionnelles.

La principale limite à cette ouverture étant la nécessité de garantir la protection de la vie privée des patients, la Commission a cherché les principes permettant de garantir ces deux objectifs.

La nécessité de protéger la vie privée des personnes est d'autant plus partagée que les données de santé constituent des données particulièrement sensibles. Même en supprimant tout identifiant direct dans ces données, il faut se prémunir contre les risques de réidentification des personnes dans les bases médico-administratives, qui peut survenir dès lors qu'un tiers se trouverait avoir par ailleurs connaissance de certains traits spécifiques du parcours de soins de ces personnes.

La Commission considère qu'il est nécessaire d'adopter des attitudes différentes en fonction du niveau de risque objectivement mesuré, qui constitue le seul critère pouvant justifier les différences de procédure d'accès. Il est proposé, au sein de chaque classe de risque, d'unifier et de simplifier les procédures d'accès. Pour les données strictement anonymes, c'est-à-dire, à risque nul d'identification, l'accès doit être totalement libre, sans restriction de réutilisation des données publiques. Le champ de la santé doit ainsi résolument s'engager dans la voie de l'open data. À ce titre, la Commission prône le principe d'ouverture par défaut des données publiques anonymes de santé, sauf exception motivée.

La Commission rappelle que la qualité des données, leur complétude ou leur complexité ne constituent pas des critères devant déterminer l'ouverture ou non des données de santé anonymes. L'ouverture des données granulaires doit être privilégiée et les enquêtes et recherches menées sur fonds publics devront dès leur conception prévoir l'ouverture des données granulaires anonymisées.

Les réunions plénières de la Commission, et plus encore les rencontres et ateliers thématiques organisés en parallèle, ont permis de lancer un mouvement dynamique autour de l'« *open data* » (données ouvertes) en santé, concrétisé par l'ouverture d'un certain nombre de jeux de données. La définition d'une liste de jeux de données dont la commission demande l'ouverture dans les plus brefs délais, et l'identification d'actions préalables nécessaires à mettre en œuvre, à court terme, pour l'ouverture d'un certain nombre de jeux de données supplémentaires, sont listés dans le rapport.

La commission recommande de continuer ces travaux à travers la constitution d'un groupe de travail, pour renforcer l'ouverture des données médico-administratives et élaborer une « offre *open data* » ambitieuse dépassant les freins actuels n'ayant pas de justification légale.

Des problématiques spécifiques ayant été soulignées pour les données d'enquêtes et de recherche, la Commission recommande qu'un groupe de travail soit également constitué afin de définir des solutions au niveau législatif, technique et économique pour ouvrir ces données à tout public.

Enfin, la Commission recommande que les directions générales des établissements publics et des opérateurs renforcent leurs actions concernant l'*open data* à travers la définition d'une feuille de route et d'un échéancier pour l'ouverture des données. Cette feuille de route pourrait être élaborée avec l'appui de correspondants open data dans les organisations concernées. À ce titre, des travaux techniques ont été menés pour constituer des jeux de données anonymes à partir du PMSI. Ces travaux devront se poursuivre et être étendus à l'ensemble du SNIIRAM.

Pour les données présentant un très faible risque de réidentification du fait de la granularité limitée des informations mises à disposition ou de la non exhaustivité de la population décrite (échantillon), une procédure simplifiée pourrait être retenue dès lors que la CNIL, après avis d'un comité technique, en aura validé

les caractéristiques. L'autorisation d'accès à tel ou tel organisme pourrait relever d'un arrêté ministériel, après avis de la même instance, pour ce qui concerne les acteurs autres que les services de l'État et ses opérateurs. Des propositions ont été formulées pour créer de nouveaux jeux de données répondant à cet objectif.

Enfin, pour les données détaillées, emportant de ce fait un risque plus important de réidentification, il est proposé de simplifier le circuit des demandes d'accès des organismes privés ou publics en créant un canal unique d'autorisation délivrée par la CNIL :

- après avis d'un comité technique pour ce qui concerne la recherche académique ;

- après avis d'un comité technique et d'un comité d'orientation s'il ne s'agit pas de recherche académique.

Enfin, s'agissant de l'autorisation d'accès à ces données par les administrations, les opérateurs de l'État, les ARS ainsi que d'autres utilisateurs permanents des données, il est recommandé de confier cette décision au ministre en charge de la santé après avis de la CNIL.

L'étape d'instruction technique n'aurait pas lieu d'être lorsqu'une recherche est réalisée à la demande d'une autorité publique et qu'elle a validé le protocole d'étude, la CNIL restant naturellement le décisionnaire ultime. D'autres procédures simplifiées visant à rendre la procédure plus rapide pourront être mises en place sur le modèle déjà existant des méthodologies de référence notamment, ou pour l'accès à des ensembles de données à faible risque de réidentification. Seraient également concernées par cette procédure, les demandes d'industriels visant à alimenter un dossier type requis par l'administration.

Une attention particulière a été portée aux données relatives aux professionnels et établissements de santé. L'exigence de transparence sur des sujets aussi importants pour les patients que le reste à charge et la qualité des soins délivrés justifie la mise à disposition de données individuelles. Si cette mise à disposition est maintenant bien acquise dans le champ des établissements de santé, elle pose plus de difficultés s'agissant des professionnels de santé rendus ainsi directement et personnellement exposés. La Commission propose donc une approche graduelle et concertée permettant des avancées immédiates, par exemple sur la réutilisation des données tarifaires ou sur les données permettant d'identifier le profil d'activité d'un professionnel et confiant à la concertation entre les parties prenantes la responsabilité de faire émerger progressivement des indicateurs rendant compte de façon fiable et pertinente de la qualité des soins délivrés. La Commission appelle de ses vœux un lancement rapide de cette concertation. Les représentants des professionnels appellent néanmoins à la prudence sur ce sujet, la constitution et la publication d'indicateurs individuels nécessitant, dans certains cas, une certaine pédagogie pour leur interprétation ou leur appropriation.

L'effectivité des mesures proposées dépend de la qualité de l'organisation qui sera mise en place pour leur donner une réalité : modalités d'accès aux données, traçabilité des accès, mais aussi respect des données d'instruction des demandes, degré d'ouverture réelle en fonction des réponses apportées aux demandes d'accès, capacité à prendre en compte des questions nouvelles, etc.

Ceci doit conduire à prêter une attention particulière aux moyens qui seront attribués tant pour l'instruction des demandes d'accès que pour la mise à disposition effective des données. Dans un contexte de contrainte économique forte pour l'ensemble des acteurs, le choix du modèle économique est un sujet sur lequel la Commission souhaite insister même s'il n'était pas inclus dans sa saisine.

La question de la gouvernance, garante de la mise en œuvre effective des principes posés, a fait l'objet de longs débats. Les propositions qui sont formulées visent à répondre aux préoccupations légitiment exprimées par les différentes parties prenantes. De façon résumée : garantir au chercheur un accès réel aux données au nom des exigences de la seule recherche, mais aussi garantir aux parties prenantes (patients et usagers, professionnels de santé, industriels, assureurs, etc.) un examen ouvert et loyal de leur demande d'accès au vu des seules règles posées.

Ces préoccupations conduisent la commission à recommander une organisation sous la forme de deux comités disposant de compétences propres, fonctionnellement articulés autour d'un guichet unique constituant *a minima* un secrétariat commun aux deux instances, et de préférence regroupés au sein d'une même structure :

- un comité technique composé d'experts et de scientifiques dont la diversité et l'indépendance doivent être assurées, désignés par les responsables d'autorités compétentes telles que l'INSERM, le HCSP, l'ANSM, la HAS, etc. Cette instance étudie les demandes d'accès au regard des critères mis en avant par la Commission (bénéfice collectif, pertinence des traitements, références de l'équipes, etc.). Son avis est ensuite transmis à la CNIL ;

- un comité d'orientation, réunissant l'ensemble des parties prenantes, constituant le lieu de supervision du dispositif et d'animation des débats qui doivent se poursuivre au-delà des travaux de la Commission, notamment pour ce qui concerne l'accès aux données nominatives d'activité ou de tarification des professionnels de santé. La Commission recommande que ce comité puisse être également saisi, à l'initiative de son président ou de son représentant, de l'évaluation du bénéfice collectif attendu des projets soumis par d'autres acteurs que ceux de la recherche académique, afin de garantir une meilleure prise en compte des enjeux collectifs et sociétaux induits par la demande. Son avis est ensuite transmis à la CNIL, l'avis du comité technique étant joint pour ce qui concerne l'évaluation des autres critères.

La mise en œuvre de ces recommandations suppose diverses mesures législatives et règlementaires dont les premières devront pouvoir trouver leur place dans la loi de santé publique en cours de préparation.

3.3. - Cour des comptes. Les données personnelles de santé gérées par l'assurance maladie. Une utilisation à développer, une sécurité à renforcer. Communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale, mars 2016

Synthèse

Le système national inter-régimes de l'assurance maladie, une base sans équivalent en Europe adossée à un système informatique puissant, réalisée par la CNAMTS en dépit d'un pilotage éloigné de l'État.

Conçu pour doter les pouvoirs publics d'un outil unifié de pilotage des dépenses de santé et créé par la loi de financement de la sécurité sociale pour 1999, le Système national d'information inter-régimes de l'assurance maladie (SNIIRAM) enregistre, dans une base unique, les données de liquidation des bénéficiaires des régimes d'assurance maladie obligatoire. Entre sa création législative et sa mise en service opérationnelle, trois années se sont écoulées en raison de l'ampleur des migrations à opérer depuis les systèmes préexistants, et de la complexité du cadre règlementaire à définir.

Le SNIIRAM a connu des évolutions successives pour enrichir son contenu et améliorer sa structuration, jusqu'à devenir aujourd'hui une base de données médico-administratives, sans équivalent en Europe au regard du nombre de personnes concernées et de la diversité des données disponibles. À cet égard, le chaînage des données de ville avec les données de paiement hospitalières issues du programme de médicalisation des systèmes d'information depuis 2009 a constitué une avancée majeure. La CNAMTS, maître d'ouvrage dont il convient de souligner l'implication et les résultats obtenus, a développé des outils de structuration des données, en créant en particulier un échantillon généraliste des bénéficiaires en 2005, qui ont contribué à l'exploitation du SNIIRAM en dehors de l'assurance maladie. Ces efforts de structuration doivent encore être poursuivis dans une logique d'offre de service à des utilisateurs plus nombreux.

Le potentiel de ces outils est très important, mais il reste à parfaire. La qualité de la base peut être améliorée en réduisant certaines fragilités de codage et des remontées d'informations encore parfois incomplètes.

La gouvernance du SNIIRAM, projet majeur, a été partagée entre deux instances partiellement concurrentes – le comité de pilotage inter-régimes, associant notamment les administrations et le maître d'ouvrage, et l'Institut des données de santé, faisant pour sa part place aux utilisateurs potentiels En l'absence d'investissements et de moyens de la tutelle, le pilotage du SNIIRAM, les choix en matière d'orientations stratégiques, de gestion des évolutions techniques et de détermination des droits d'accès, ont été de fait délégués à la CNAMTS, impliquée dans la gestion technique pour améliorer la base, à petit pas et souvent empiriquement. Dès lors, de maître d'ouvrage, la CNAMTS s'est comportée en propriétaire du SNIIRAM ce qui, conjugué à une approche restrictive des demandes

par la CNIL, a conduit à la forte limitation des accès permanents au SNIIRAM et à des freins au développement des utilisations ponctuelles par les acteurs du monde de la santé publique.

Après une période marquée par un attentisme certain, la mise à niveau technique du SNIIRAM et de sa sécurité informatique est, depuis 2013, conduite diligemment, et l'absence de tout incident de fuite de données est à souligner. Un renforcement des audits techniques et de la documentation relative aux applications s'impose néanmoins, d'autant que si la mise en conformité technique avec les normes et bonnes pratiques de gestion de mégadonnées apparait satisfaisante, plusieurs risques et défaillances de sécurité identifiés par la CNAMTS subsistent. D'autres problèmes concernent les dispositifs de cryptage, obsolescents même si leur changement ne s'avèrera indispensable qu'à horizon de quelques années. L'ampleur des enjeux appelle la plus grande anticipation dans la programmation des chantiers, l'estimation de leurs coûts et la mise en œuvre des actions de réduction des risques. Une attention suffisante n'y a pas été apportée par la tutelle. La CNAMTS doit se doter sans plus attendre d'un calendrier et d'un plan d'actions adapté, et définir l'échéancier financier correspondant ; des moyens devant impérativement être dégagés à hauteur du nécessaire compte tenu du caractère stratégique des enjeux de sécurisation.

Notons une diversification progressive des utilisations du SNIIRAM, malgré une gestion prudente à l'extrême des accès, mais nettement insuffisantes au regard des enjeux financiers et sanitaires du pays

Alors que la France a réussi à constituer une base exceptionnelle par son exhaustivité, sa richesse et sa finesse d'informations, qui n'a pas d'exemple dans le monde, et aux potentialités considérables en matière de santé publique, de recherche, d'efficience du système de soins et de maîtrise des dépenses, elle s'interdit paradoxalement de l'exploiter pleinement.

En effet, le cadre juridique est particulièrement complexe et l'approche des différentes parties prenantes restrictive à l'extrême. Les difficultés de gouvernance du SNIIRAM n'ont pas permis de traiter convenablement ces enjeux d'accès aux données du SNIIRAM. La définition des droits d'accès, accordés au cas par cas aux termes de procédures aux délais excessifs, mobilisent de nombreux acteurs, mal coordonnés, tels l'IDS, le COPIIR, la CNAMTS et la CNIL. Cette situation, dans un contexte de montée des demandes au cours des dernières années, a conduit à une paralysie des accès permanents depuis près de trois années et à une asphyxie des instances chargées des demandes d'accès ponctuels. De surcroît, les protocoles de recherche peuvent faire l'objet de modifications des variables utilisées à la demande de la CNIL, afin de limiter, selon elle, la réidentification des personnes mais qui, de fait, au nom du principe de précaution, peuvent entraver ou démotiver la recherche. S'il appartient sans conteste à la CNIL de veiller au respect de l'anonymat des personnes concernées et de la sécurité des données, ses procédures d'instructions techniques et juridiques sont marquées par de multiples exigences *a priori* qui contrastent fortement avec l'absence de tout contrôle *a posteriori*.

Dans ces circonstances, il n'est pas étonnant que le degré d'utilisation du SNIIRAM soit très variable suivant le type d'acteurs sans compter le fait que, même en cas d'accès permanent, les procédures d'interrogation sont complexes et nécessitent le soutien ou l'entremise de la CNAMTS.

Malgré une utilisation devenue régulière, la CNAMTS n'exploite pas encore le SNIIRAM au maximum de ses potentialités, en particulier en matière de gestion du risque et de lutte contre les abus et la fraude des professionnels de santé. Or, il s'agit d'un outil puissant à mettre au service d'une stratégie d'ensemble d'amélioration de l'efficience des prises en charge et de maîtrise des dépenses.

Par son manque d'investissement et d'expertise, renforcé par des droits d'accès parfois trop restreints, l'État s'est, quant à lui, privé au niveau national comme déconcentré, d'un instrument précieux pour le pilotage du système de santé et la recherche d'efficience des dépenses d'assurance maladie.

Si l'utilisation du SNIIRAM à des fins de veille sanitaire est en pleine expansion grâce au chaînage avec le PMSI, les agences et autorités sanitaires sont inégalement impliquées, et la contribution du SNIIRAM aux analyses portant sur l'amélioration de la qualité des soins est insuffisante. Des efforts rapides doivent être consentis pour améliorer encore le contenu du SNIIRAM, notamment par sa médicalisation.

Des transformations importantes ont été introduites par la loi du 26 janvier 2016 de modernisation de notre système de santé, dont la portée reste conditionnée par les textes d'application et l'évolution des principaux acteurs.

La loi « santé » de 2016, en son article 193, crée le système national des données de santé (SNDS), au périmètre élargi par rapport au SNIIRAM. Ce dernier constitue toutefois et pour longtemps le cœur du système de données de santé. Les priorités restent donc les enjeux d'amélioration et de sécurisation de l'existant, de gouvernance et d'ouverture fluide des accès pour encourager leur utilisation à des fins d'intérêt général.

La nouvelle gouvernance prévue par la loi devra résoudre l'éclatement du pilotage du SNIIRAM et l'actuelle dilution des responsabilités en distinguant clairement entre gestion technique du SNDS, gestion des droits d'accès et définition des orientations stratégiques. Il importe donc que les textes d'application soient suffisamment ambitieux et précis, notamment dans la définition des procédures d'instruction des demandes d'accès à la base, ce qui suppose une implication forte et convergente du ministère de la santé, de l'assurance maladie et de la CNIL. La rénovation du cadre juridique d'accès ne suffira pas à résoudre l'ensemble des difficultés rencontrées. Face à l'augmentation prévisible, et souhaitable, des demandes d'accès, la CNIL devra faire évoluer sa doctrine et ses méthodes de travail afin d'accompagner une ouverture sécurisée des données et non plus de la freiner.

Dans ce contexte l'accent doit être mis moins sur le contrôle *a priori* qui doit être radicalement allégé que sur une politique de contrôle *a posteriori* aujourd'hui inexistante, reposant tout d'abord sur la responsabilisation des utilisateurs. La CNIL, autorité indépendante de régulation, doit faire du SNDS un de ses axes prioritaires de contrôle dans le champ de la santé et ne pas hésiter, si nécessaire, à sanctionner les mésusages.

Le système national des données de santé, par son périmètre plus large que les seules données du SNIIRAM, nécessite des efforts particuliers. Il importe de faire preuve de pragmatisme et de réalisme, comme les promoteurs du SNIIRAM ; la CNAMTS, au premier chef, ont su le faire en construisant en marchant ce système reconnu, et en ne cédant pas à la tentation d'une construction *ex nihilo* alors que les appariements entre bases de données sont désormais facilités. En tout état de cause, le SNIIRAM constituera, pour quelques temps encore, l'essentiel du SNDS. Dans ce contexte, il convient de continuer sans relâche à enrichir et à sécuriser son contenu, et à améliorer sa structuration pour faciliter son appropriation par le plus grand nombre.

À cet égard, la question de la valorisation de l'exploitation du SNIIRAM, et demain du SNDS, se pose au regard de la soutenabilité financière de ces projets. Même si les gestionnaires et les administrations de tutelle n'ont pas été en mesure de produire des documents prévisionnels sur les coûts potentiels du SNDS pour l'étude d'impact de la loi, ou pour répondre aux demandes de la Cour, les principaux postes de dépenses liés tant au SNIIRAM, et aux autres bases de données qui vont s'intégrer dans le SNDS, qu'au développement, à la sécurité et à la gestion de ce dernier, devront être identifiés et rigoureusement suivis. Il importe donc de mettre en place un modèle économique qui permette de dégager les ressources nécessaires pour contribuer à la prise en charge des investissements humains et financiers prioritaires et coûteux qui doivent être réalisés pour la sécurisation du SNIIRAM, son enrichissement et les développements nécessaires à la création du SNDS.

Recommandations

1. Poursuivre, en les hiérarchisant, les efforts d'amélioration de la complétude et de la qualité des données, en particulier des informations issues du PMSI.

2. Mettre en place rapidement un suivi analytique des coûts d'alimentation, de sécurisation, de gestion et d'utilisation du SNIIRAM.

3. Reconnaître à la CNAMTS le statut d'opérateur d'importance vitale et la soumettre aux règles et contrôles périodiques externes de sécurité y afférant.

4. Anticiper en vue de la prochaine COG la programmation financière et le calendrier des travaux additionnels de mise en conformité du SNIIRAM et de son environnement informatique avec les exigences de renforcement de sa sécurité rendues indispensables par l'obsolescence progressive de certains dispositifs.

5. Exploiter, au sein des régimes d'assurance maladie obligatoire, les potentialités

du SNIIRAM à des fins de gestion du risque, notamment pour sanctionner plus systématiquement les comportements abusifs, fautifs et frauduleux.

6. Développer l'exploitation du SNIIRAM par les pouvoirs publics en définissant les besoins de chaque direction d'administration centrale et en mutualisant les compétences au sein de la DREES, selon des priorités concertées.

7. Intensifier l'utilisation des bases médico-administratives par l'introduction systématique d'objectifs ambitieux et d'indicateurs de performance dans les conventions passées entre le ministère et les opérateurs.

8. Enrichir le SNIIRAM en améliorant la qualité des informations médicales contenues, notamment par le codage médical des soins de ville et en facilitant son rapprochement avec les données socio-économiques ou d'habitude de vie.

9. Hiérarchiser, dans le prolongement de la loi « santé » de 2016, les finalités poursuivies par le SNDS, afin de définir les investissements à consentir et les accès permanents et ponctuels à autoriser.

10. Simplifier les procédures relevant de la CNIL pour l'accès ponctuel aux données du SNDS par l'élaboration, dans les meilleurs délais, de méthodologies de référence et d'autorisations cadres selon des priorités concertées avec l'État et l'INDS.

11. Articuler précisément et explicitement le rôle des différents acteurs dans la gestion du pilotage et des accès au SNDS.

12. Mettre en œuvre une politique systématique et rigoureuse de contrôle *a posteriori* des règles relatives à l'utilisation du SNIIRAM et du SNDS, s'appuyant sur des sanctions renforcées et faisant notamment l'objet d'un rapport annuel au Parlement de la CNIL.

13. Assurer la soutenabilité financière du SNDS, en articulant gratuité d'une offre de base et tarification adaptée des services spécifiques apportés de manière à contribuer au financement des dépenses de développement, de sécurisation, de mise à disposition des données et d'accompagnement.

Comité de rédaction

Responsable de la publication :

Martine de Boisdeffre, présidente de la section du rapport et des études.

Conception et réalisation :

François Seners, président adjoint et rapporteur général de la section du rapport et des études.

Corinne Mathey, secrétaire de la section du rapport et des études.

Avec l'appui de Laure Marcus, premier conseiller de tribunal administratif et de cour administrative d'appel, chargée de mission auprès de la présidente de la section du rapport et des études.

La documentation juridique du colloque a été préparée par Clément Malverti, rapporteur à la section sociale et à la section du contentieux du Conseil d'État.

Secrétaire de rédaction

Frédéric Navas Alonso de Castaneda, chargé de mission à la section du rapport et des études.

Avec la contribution de Ava Farzin Pour, stagiaire à la section du rapport et des études.

Coordination du colloque

Caroline Lafeuille, chargée de mission pour les relations extérieures.

Crédits photos, conseil graphique

Direction de la communication.

Retrouvez la vidéo du colloque à partir de www.conseil-etat.fr, rubrique « colloques ».