N° 4533

# ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958
QUATORZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 21 février 2017.

# RAPPORT D'INFORMATION

DÉPOSÉ

*en application de l'article 145 du Règlement*

PAR LA COMMISSION DES AFFAIRES SOCIALES

*en conclusion des travaux de la* **mission d'évaluation et de contrôle des lois de financement de la sécurité sociale**
*sur* **les données médicales personnelles inter-régimes détenues par l'assurance maladie, versées au SNIIRAM puis au Système national des données de santé (SNDS)**,

ET PRÉSENTÉ PAR

M. Pierre MORANGE,

Député.

**SOMMAIRE**

Pages

# INTRODUCTION

Soucieux de moderniser l'action publique, le Gouvernement a décidé en février 2013 l'ouverture des données publiques. Connue sous l'expression d'*open data*, cette politique vise à mettre en ligne des données dans des formats ouverts et à permettre à toute personne de les réutiliser librement et gratuitement.

Dans ce contexte, il est apparu que les données de santé devaient être plus accessibles afin de faciliter leur utilisation par le plus grand nombre. Un comité interministériel pour la modernisation de l'action publique a confié au ministère des Affaires sociales et de la santé, en juillet 2013, l'animation d'un débat sur l'ouverture de ces données. À cet effet, une commission associant les différents acteurs concernés et ouverte aux contributions citoyennes a été mise en place : la commission *open data*.

Le droit européen définit les données personnelles de santé comme « *des données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins à la santé, qui révèlent des informations sur l'état de santé de cette personne* » [(1)].

Ces données ne sont pas des données comme les autres. C'est pourquoi le Conseil constitutionnel a considéré qu'il appartenait au législateur d'instituer une procédure propre à sauvegarder la vie privée des personnes, lorsqu'est demandée la communication de données de santé susceptibles de permettre leur identification, et a érigé en principe de valeur constitutionnelle le respect de la vie privée [(2)].

Issu des travaux de la commission *open data*, un nouveau dispositif relatif à la mise à disposition de données de santé a été proposé. L'article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé tente de concilier ces deux principes – ouverture des données et protection de la vie privée – en rénovant et en simplifiant les procédures d'accès aux bases médico-administratives tout en encadrant l'utilisation de ces données.

Le nouveau dispositif définit des droits d'accès différenciés selon les données, étant entendu que lorsque ces données peuvent être directement ou indirectement identifiantes, l'accès est restreint et contrôlé en fonction des opérateurs, les organismes publics ayant un accès privilégié.

---

*(1) Article 4 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.*

*(2) Décision 99-416 DC du 23 juillet1999 relative à la loi portant création d'une couverture maladie universelle. En l'espèce, le respect de la vie privée a été assuré par la subordination de la communication des données à l'autorisation de la Commission nationale informatique et libertés.*

Par ailleurs, un nouveau système d'information, dénommé « Système national des données de santé » (SNDS), rassemblera des données médicales et médico-sociales, en intégrant notamment les deux grandes bases existantes, le Programme de médicalisation des systèmes d'information (PMSI) et le Système national d'information inter-régimes de l'assurance maladie (SNIIRAM), mais aussi le CépiDc et, plus tard, les données médico-sociales et des données provenant des organismes complémentaires santé.

Dans ce contexte, la Mission d'évaluation et de contrôle des lois de financement de la sécurité sociale (MECSS) a choisi de se pencher sur la question de l'accès aux données personnelles de santé gérées par l'assurance maladie. La Cour des comptes a remis à la mission un rapport sur ce sujet en mars 2016 (1) et lui a, comme toujours, apporté une précieuse expertise.

La mission a ensuite procédé à l'audition de responsables de l'assurance maladie obligatoire et des complémentaires santé, de responsables de l'administration, de représentants des professionnels de santé et de l'industrie de la santé, des responsables en sécurité informatique ainsi que la Commission nationale de l'informatique et des libertés (CNIL).

Le présent rapport d'étape clôt une première phase des travaux de la mission et vise en premier lieu à faire le point sur le dispositif mis en place pour faciliter l'ouverture des données de santé. Celui-ci n'est pas encore totalement opérationnel puisque plusieurs décrets d'application sont en cours d'élaboration et que la convention constitutive du groupement d'intérêt public (GIP) du futur Institut national des données de santé (INDS) n'a pas encore été arrêtée. En second lieu, le présent rapport s'efforce d'exposer de façon exhaustive les questions abordées par les personnes entendues par la mission, notamment la gouvernance du dispositif, son articulation avec le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, les questions de sécurité et le modèle économique du nouveau dispositif.

*(1) Cour des comptes*, Les données personnelles de santé gérées par l'assurance maladie, *mars 2016.*

# I. UN PROJET AMBITIEUX D'OUVERTURE DES BASES DE DONNÉES MÉDICO-ADMINISTRATIVES INFORMATISÉES

## A. UN PROJET QUI, PAR-DELÀ SES FINALITÉS MÉDICALES ET GESTIONNAIRES, AMBITIONNE D'APPROFONDIR LA DÉMOCRATIE SANITAIRE

Toutes les réflexions menées depuis 2009 (1) s'accordent sur un point : la France peut s'enorgueillir de disposer de bases de données médico-administratives exhaustives couvrant l'ensemble de la population et permettant un chaînage du parcours de soins du patient durant toute sa vie. Cependant, ces bases ne sont pas suffisamment exploitées par les organismes publics, comme le relève la Cour des comptes dans son rapport (2).

Selon le docteur Dominique Blum, praticien hospitalier, la complexité de l'accès à ces bases et la difficulté à les exploiter sans formation spécifique expliquent en partie cette sous-utilisation (3). La Direction de la recherche, des études, de l'évaluation et des statistiques (DREES) a indiqué qu'il fallait compter au moins deux ans pour maîtriser les données du SNIIRAM. M. Philippe Burnel, délégué à la stratégie des systèmes d'information de santé (DSSIS) au secrétariat général du ministère des affaires sociales et de la santé, a, de son côté, relevé que « *le Système national d'information inter-régimes de l'assurance maladie (SNIIRAM) est d'une telle complexité qu'il est nécessaire d'être statisticien pour en comprendre les données – pour bien faire, il faut donc être à la fois médecin et statisticien.* » (4) Il a ajouté que les informations contenues dans cette base sont des données de remboursement brutes avec des codes de modulations tarifaires, dont la bonne compréhension et la maîtrise nécessitent une formation appropriée.

C'est pourquoi l'ouverture, l'accès et l'utilisation de ces données de santé issues de bases médico-administratives ont été repensés. À l'issue de plusieurs réflexions (5) et d'une concertation dans le cadre de la commission *open data* (6), l'article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé a introduit un nouveau chapitre dans le code de la santé publique, intitulé « *Mise à disposition des données de santé* », qui met en place un nouveau dispositif.

---

*(1) Haut Conseil de la santé publique,* Les systèmes d'information pour la santé publique, *décembre 2009.*

*(2) Cour des comptes,* op. cit.

*(3) Audition du 13 décembre 2016.*

*(4) Audition du 13 décembre 2016.*

*(5) Haut Conseil de la santé publique,* Pour une meilleure utilisation des bases de données nationales pour la santé publique et la recherche, *mars 2012, et M. Pierre-Louis Bras,* Rapport sur la gouvernance et l'utilisation des données de santé, *Ministère des affaires sociales et de la santé, septembre 2013.*

*(6) Commission open data en santé,* Rapport remis à Madame Marisol Touraine, ministre des Affaires sociales et de la santé, *juillet 2014.*

### 1. Des bases médico-administratives informatisées qui avaient déjà vu leurs objectifs évoluer

Les deux grandes bases de données médico-administratives – le Programme de médicalisation des systèmes d'information (PMSI) et le Système national d'information inter-régimes de l'assurance maladie (SNIIRAM) – répondaient, à l'origine, à des objectifs de gestion et d'aide à l'optimisation de l'offre de soins dans une logique d'efficience et de rationalisation.

Le PMSI a été conçu pour mesurer l'activité des établissements hospitaliers et permettre l'application de la tarification à l'activité, la T2A. L'article L. 6113-7 du code de la santé publique fixe comme finalité aux systèmes d'information mis en place dans les établissements de santé l'amélioration de la connaissance et l'évaluation de leur activité et de leurs coûts. Il est également précisé que ces systèmes devront favoriser l'optimisation de l'offre de soins. Il s'agit bien d'une logique d'efficience et non de recherche en santé publique.

Cependant, depuis 2006-2007, son chaînage avec la base du SNIIRAM permet de suivre le parcours de soins d'un individu tant en ville qu'à l'hôpital et renforce l'intérêt de son usage pour des études menées par des chercheurs.

Le SNIIRAM a été conçu comme un outil de contrôle et de maîtrise des dépenses de l'assurance maladie obligatoire.

Lorsqu'un dispositif de régulation des actes et des prescriptions des médecins ainsi que des objectifs opposables ont été mis en place en 1996 [(1)], la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS) a eu besoin de disposer d'un système d'information lui permettant de documenter cette régulation. C'est pourquoi les finalités du SNIIRAM fixées en 1999 [(2)] par l'article L. 161-28-1 du code de la sécurité sociale précisent que cette base doit permettre le relevé des dépenses de l'ensemble des régimes d'assurance maladie selon plusieurs critères : circonscription géographique ; nature des dépenses ; professionnels ou établissements à l'initiative de ces dépenses. Les données d'activité, de recettes et éventuellement de prescriptions relatives aux professionnels de santé leur sont transmises en retour.

La CNAMTS utilise le SNIIRAM pour suivre l'évolution des dépenses au sein de l'Objectif national de dépenses d'assurance maladie (ONDAM) ou mener les négociations conventionnelles avec les professionnels de santé. En 2015, les données du SNIIRAM ont ainsi permis d'établir une cartographie de 56 catégories de pathologies et de leurs remboursements.

En 2004, il est apparu que cette base pouvait être mise à contribution pour l'élaboration des politiques de santé publique. En conséquence, l'article 24 de la loi n° 2004-806 du 9 août 2004 relative à la politique de santé publique a assigné

*(1) Ordonnance n° 96-345 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins.*

*(2) Article 21 de la loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale pour 1999.*

une nouvelle mission au SNIIRAM : « *la définition, la mise en œuvre et l'évaluation des politiques de santé publique* » et a complété en ce sens l'article L. 161-28-1 précité.

L'arrêté du 19 juillet 2013 modifié relatif à la mise en œuvre du SNIIRAM détaille ces finalités. S'agissant d'une meilleure gestion des politiques de santé, la base doit permettre :

– d'identifier le parcours de soins des patients ;

– de suivre et d'évaluer l'état de santé des patients et leurs conséquences sur la consommation des soins ;

– d'analyser la couverture sociale des patients ;

– de surveiller la consommation de soins en fonction d'indicateurs de santé publique ou de risque.

L'arrêté prévoit également que la base SNIIRAM doit participer à améliorer la qualité des soins :

– en favorisant la comparaison des pratiques aux référentiels ;

– en évaluant les comportements de consommation de soins ;

– en analysant les caractéristiques et les déterminants de la qualité des soins.

Lors de son audition, M. Antoine Durrleman, président de la sixième chambre de la Cour des comptes, a résumé ainsi cette évolution : « *La force de cette base est d'abord d'être un produit dérivé. Elle n'a pas été conçue à partir de rien : c'est un sous-produit du dispositif de liquidation des prestations d'assurance maladie. Le dispositif de feuilles de soins électroniques, mis en place au tournant des années 1995 avec la carte Sésame-Vitale et pensé pour améliorer les délais de remboursement des assurés, s'est révélé à même de nourrir un entrepôt de données d'une importance majeure.* » (1)

M. Philippe Burnel a également rappelé que la base SNIIRAM, créée par l'assurance maladie, sous le pilotage de l'État, pour ses finalités propres de gestion du risque, est progressivement devenue un outil de recherche : « *À l'époque, les partenaires de l'assurance maladie ne manifestaient à l'égard d'une telle base de données qu'une assez grande indifférence, voire un certain scepticisme. Le programme de médicalisation des systèmes d'information (PMSI) a connu le même parcours.* […] *Avec le temps, les chercheurs ont pris conscience du grand intérêt de ces données pour la recherche médicale, parfois même pour la recherche clinique, et pour le pilotage de la santé publique.* » (2)

*(1) Audition du 3 mai 2016.*

*(2) Audition du 13 décembre 2016.*

### 2. Des finalités nouvelles pour des enjeux majeurs

La loi du 26 janvier 2016 de modernisation de notre système de santé traduit cette évolution en assignant de nouvelles missions aux bases de données médico-administratives [(1)]. Celles-ci sont réunies dans un nouveau système d'information, le système national des données de santé (SNDS), dont la présentation sera développée *infra.*

Désormais, l'accès aux données de santé répond à six finalités que l'on peut regrouper sous quatre enjeux : un enjeu démocratique – conforter la démocratie sanitaire ; un enjeu épidémiologique – une meilleure vigilance sanitaire ; un enjeu économique – l'efficience du pilotage de la santé publique ; un enjeu scientifique – contribuer au progrès de la recherche.

#### *a. L'enjeu démocratique : conforter la démocratie sanitaire*

La démocratie sanitaire est une démarche qui vise à associer l'ensemble des acteurs du système de santé dans l'élaboration et la mise en œuvre de la politique de santé, dans un esprit de dialogue et de concertation. Pour y parvenir, le développement de l'information des usagers du système de santé est nécessaire. C'est pourquoi les associations de patients ont œuvré à une plus grande ouverture des bases de données de santé afin de bénéficier d'une véritable information transparente sur l'offre de soins. Dans le dispositif actuel, les usagers sont représentés au sein de l'Institut des données de santé par le Collectif interassociatif sur la santé (CISS) qui regroupe une quarantaine d'associations de patients. Ces dernières ont participé aux travaux de la commission *open data*.

Le nouveau dispositif prévoit que le SNDS contribue à l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité [(2)]. En outre, l'article R. 1461-1 du code de la santé publique dispose que le SNDS permet de contribuer à « *l'orientation des usagers dans le système de santé, en permettant la comparaison des pratiques de soins, des équipements et des tarifs des établissements et des professionnels de santé.* »

Tout assuré pourra être informé de l'offre des professionnels de santé et notamment consulter utilement les pratiques de dépassement d'honoraires. Si l'annuaire santé disponible sur le site internet ameli.fr de la CNAMTS met d'ores et déjà à la disposition du public les données d'activité des professionnels libéraux telles que leur secteur de conventionnement, l'utilisation de la carte vitale et leur tarification, il reste méconnu. Le docteur Jacques Lucas, vice-président du Conseil national de l'Ordre des Médecins, délégué général aux systèmes d'information en santé, s'est montré réservé sur une évaluation individuelle des médecins et a plaidé plutôt pour une évaluation des pratiques professionnelles par territoire ou par équipes de soins [(3)]. Cette position est totalement partagée par le rapporteur.

---

*(1) Paragraphe III de l'article L. 1461-1 du code de la santé publique.*

*(2) Paragraphe III de l'article L. 1461-1 du code de la santé publique.*

*(3) Audition du 31 janvier 2017.*

Lors de son audition, M. Philippe Burnel a évoqué la multiplication des palmarès d'établissements de santé et a souligné qu'il convenait d'interpréter avec prudence certaines statistiques, les indicateurs retenus n'étant pas exempts de défauts : « *Je me souviens ainsi d'un indicateur d'attractivité des hôpitaux selon la proportion de patients venus d'un autre département : il offrait une prime extraordinaire aux hôpitaux frontaliers, fussent-ils de qualité médiocre.* » (1) Il s'est dit partisan d'une plus grande ouverture des données, qui permettra « *aussi de disposer d'une pluralité d'indicateurs et de diagnostics et c'est en ce sens qu'il faut aller.* » Mme Chantal Cases, présidente de l'Institut des données de santé (IDS), a livré une analyse similaire : « *Nous soutenons le principe de l'ouverture des données, considérant que le fait qu'un grand nombre d'usagers potentiels puissent les utiliser est la meilleure garantie que se forgent des analyses soumises à contre-expertise.* » (2)

Une plus grande transparence des données de santé contribuera aussi à documenter les disparités territoriales de l'offre de soins.

***b. L'enjeu épidémiologique : améliorer la vigilance sanitaire***

L'utilisation des bases de données de santé permet d'améliorer la vigilance sanitaire, que ce soit en pharmacovigilance, en pharmaco-épidémiologie ou dans les procédures de réévaluation des médicaments.

Par exemple, l'Agence nationale de santé publique (ANSP) utilise la base SNIIRAM pour suivre la couverture vaccinale. Le docteur Jean-Claude Desenclos, représentant l'ANSP, a indiqué : « *les données de remboursement permettent de connaître la couverture vaccinale avec une grande réactivité, à six mois près, ainsi que son évolution par cohorte de naissance. Cette dernière donnée s'est révélée très utile, nous permettant de mesurer que le niveau de couverture vaccinale avait atteint près de 90 % s'agissant de la première injection du vaccin contre l'hépatite B, et,* a contrario*, nous montrant très tôt l'effondrement de la couverture vaccinale des jeunes filles par le vaccin anti-HPV.* » (3)

L'ANSP utilise également les autres bases médico-administratives pour établir une surveillance lors d'épisodes de canicule ou d'épidémies de grippe.

S'agissant de la pharmacovigilance, l'article R. 1461-1 du code de la santé publique précise que le SNDS permet de contribuer à « *la détection d'événements de santé inhabituels pouvant représenter une menace pour la santé publique et l'évaluation de leurs liens éventuels avec des facteurs d'exposition et l'évaluation d'actions de santé publique.* »

La Cour des comptes a d'ailleurs souligné le rôle majeur de la base SNIIRAM pour documenter les effets des médicaments sur la santé des patients, à

*(1) Audition du 13 décembre 2016.*

*(2) Audition du 20 décembre 2016.*

*(3) Audition du 31 janvier 2017.*

la suite d'alertes de pharmacovigilance, en citant trois exemples : le Médiator, la Depakine et la pilule de troisième génération [(1)]. Ainsi, la base SNIIRAM a servi à une étude de santé publique menée en 2009 par la CNAMTS qui confirmait le lien entre la consommation du Médiator et le développement de valvulopathies et d'hypertension artérielle pulmonaire. De même, une étude a été conduite en 2015 sur les effets de la Depakine chez les femmes enceintes. Enfin, M. Mahmoud Zureik, directeur scientifique et de la stratégie européenne au sein de l'Agence nationale de sécurité du médicament et des produits de santé (ANSM), a retracé comment le croisement de données issues de plusieurs bases médico-administratives a permis de documenter les effets secondaires de la pilule de troisième génération : « *L'agence a, sur ces bases, préconisé la prescription de pilules de deuxième génération. Puis elle a pu mesurer un ou deux ans plus tard un effet certain sur la morbidité : le nombre d'embolies pulmonaires chez les femmes en âge de procréer a baissé de 10 %, diminution qui correspond au changement de médicament.* » [(2)]

Par ailleurs, l'usage des médicaments remboursés, leurs effets et le respect des indications d'autorisation de mise sur le marché (AMM) par les prescripteurs sont documentés dans la base SNIIRAM et peuvent ainsi être analysés.

L'ANSM a d'ailleurs conclu une convention de partenariat avec la CNAMTS en 2011. Depuis 2012, l'ANSM s'est dotée d'un pôle de pharmaco-épidémiologie dont les 13 agents se consacrent exclusivement à l'exploitation des données de santé. M. Dominique Martin, directeur général de l'ANSM, a précisé : « *Nous conduisons des études ensemble et nous nous en répartissons d'autres, selon un plan de travail précis, de manière extrêmement organisée et productive. Nous avons ainsi pu développer récemment deux plateformes de pharmaco-épidémiologie, l'une à Rennes, l'autre à Bordeaux.* » [(3)]

La Cour des comptes cite dans son rapport un exemple d'utilisation par l'ANSM des données du SNIIRAM pour renforcer les conditions de prescription d'un médicament, l'isotrétinoide, présentant des risques en cas d'usage lors d'une grossesse. L'analyse des données avait, en effet, démontré un respect insuffisant des conditions de prescription.

Quant aux procédures de réévaluation d'un médicament, notamment de l'amélioration du service médical rendu, la nouvelle base permettra de servir aux études post inscription demandées par l'ANSM. La Cour des comptes déplore d'ailleurs que la Haute Autorité de santé ne se livre pas suffisamment à des études à partir du SNIIRAM afin de vérifier celles fournies par les laboratoires pharmaceutiques [(4)].

---

*(1) Cour des comptes,* op.cit.

*(2) Audition du 31 janvier 2017.*

*(3) Audition du 31 janvier 2017.*

*(4) Cour des comptes,* op.cit.

Les représentants des industries du médicament se sont montrés particulièrement intéressés par la richesse du SNIIRAM pour des études post inscription qui, selon eux, permettraient de suivre un médicament en conditions réelles d'utilisation et de documenter ainsi son rapport bénéfice-risque à partir d'un échantillon de patients large et diversifié [(1)]. Ce point est particulièrement sensible pour la mise sur le marché de traitements innovants. M. Thomas Borel, président du groupe de travail post-AMM des données de santé au LEEM (Les entreprises du médicament), a ainsi précisé : « *les études cliniques – aussi importantes soient-elles, notamment quand elles portent sur plusieurs milliers de patients – ne permettent pas d'apprécier certains éléments relatifs au produit lorsqu'il est utilisé dans les conditions réelles par des patients qui souffrent de comorbidités qui n'avaient pas nécessairement été étudiées de façon complète pendant la phase clinique ou dont les traitements complémentaires peuvent interagir avec le traitement mis sur le marché.* » M. Vincent Bildstein, président de IMS Health France, a pour sa part insisté sur l'intérêt du nouveau dispositif d'accès aux bases de données en raison de la réduction des délais : « *Il a beaucoup été question du suivi des conditions d'utilisation des médicaments et produits de santé "en vie réelle", mais qui dit "vie réelle" dit aussi temps réel : il nous faut accéder à ces données de la manière la plus fluide possible pour répondre à des enjeux de santé publique qui demandent des réponses immédiates.* » [(2)]

Ces préoccupations sont partagées par les représentants de l'industrie des dispositifs médicaux, qui sont demandeurs de l'accès aux bases de données afin de pouvoir évaluer en vie réelle le parcours de soins, l'usage du dispositif médical et ses conséquences en termes d'organisation des soins. M. François-Régis Moulines, directeur des affaires gouvernementales et de la communication au SNITEM (Syndicat national de l'industrie des technologies médicales), a insisté sur le fait que ce secteur est organisé autour de multiples marchés de niche : « *les populations cibles de patients sont restreintes, et les populations d'étude doivent par conséquent être importantes pour pouvoir observer un nombre suffisant d'événements.* » [(3)]

Enfin, la nouvelle base permettra aussi d'étudier les problématiques de santé environnementale.

### *c. L'enjeu économique : rendre plus efficient le pilotage de la santé publique et du système de soins*

Dans un contexte budgétaire contraint, le nouveau système pourrait être un outil pertinent pour documenter l'organisation et la performance du système de soins. Dans ce domaine, le Rapporteur est convaincu que des marges de progrès substantielles existent.

---

*(1) Audition du 24 janvier 2017.*

*(2) Audition du 24 janvier 2017.*

*(3) Audition du 24 janvier 2017.*

D'ailleurs, lors de son audition, M. Antoine Durrleman a regretté que le SNIIRAM, « *d'une grande richesse et d'une grande finesse, offre des usages potentiels considérables, mais que son usage réel soit "précautionneux" au regard des enjeux en termes de santé publique et d'efficience organisationnelle du système de soins.* » (1)

En premier lieu, il faut pouvoir suivre la qualité et le coût d'un parcours de soins. L'article R. 1461-1 du code de la santé publique prévoit que le SNDS permet de favoriser « *l'identification des parcours de soins des patients, le suivi et l'évaluation de leur état de santé et de leur consommation de soins et de services d'accompagnement social* ». Le croisement de données peut contribuer à améliorer l'organisation de l'offre ambulatoire, comme l'atteste l'utilisation du SNIIRAM dans le cadre des programmes d'accompagnement des retours à domicile après hospitalisation (PRADO). La Cour des comptes indique que les données du SNIIRAM permettent de cibler les motifs d'hospitalisation prioritaires, d'identifier les sources d'économies et de contrôler le suivi de ces parcours de soins, 840 millions d'euros d'économies pouvant en être escomptés. M. Pascal Perrot, médecin-conseil national et directeur de la gestion des risques et de l'action sociale à la caisse nationale du régime social des indépendants (RSI), a abondé en ce sens et a manifesté son intérêt pour cette nouvelle base qui devrait permettre d'effectuer un suivi du parcours ambulatoire des assurés du RSI (2).

En deuxième lieu, les indicateurs de qualité et d'efficience qui figurent dans les lois de financement de la sécurité sociale pourraient être documentés par ces bases de données. Les études relatives au suivi de cohortes ou aux consommations de soins publiées dans les rapports Charges et produits de la CNAMTS remis au Parlement préfigurent ce type d'analyse, comme l'a souligné M. Nicolas Revel, directeur général de la CNAMTS (3).

Enfin, une utilisation optimale des données permet une meilleure gestion du risque. L'utilisation des données agrégées du SNIIRAM permet d'identifier des catégories de prescriptions ou d'actes médicaux atypiques qui nécessitent des actions de régulation. Un exemple, étudié par la MECSS lors de son étude sur les arrêts de travail, est l'établissement de profils de médecins hyperprescripteurs par le service médical de la CNAMTS (4). Dans le code de la sécurité sociale, il est fait référence au prescripteur dont l'activité de prescription d'arrêt de travail apparaît anormalement élevée au regard de la pratique constatée chez les professionnels de santé appartenant à la même profession (5). Afin de dissuader ces praticiens identifiés comme « hyperprescripteurs » de délivrer des arrêts maladie de complaisance, l'assurance maladie a mis en place des dispositifs plus

---

*(1) Audition du 3 mai 2016.*

*(2) Audition du 17 janvier 2017.*

*(3) Audition du 17 janvier 2017.*

*(4) Mme Bérengère Poletti,* Rapport d'information en conclusion des travaux de la MECSS sur les arrêts de travail et les indemnités journalières, *Assemblée nationale, XIVe Législature, n° 986, 24 avril 2013.*

*(5) Article L. 315-1 du code de la sécurité sociale.*

contraignants : l'entretien d'alerte, l'accord préalable et la mise sous objectifs quantifiés. M. Pascal Perrot a, pour sa part, cité l'utilisation du SNIIRAM pour détecter des remboursements de frais de taxi alors que leurs chauffeurs étaient en arrêt maladie [(1)].

La Cour des comptes relève cependant que l'exploitation des bases médico-administratives par la CNAMTS est restée limitée en matière de contrôles et de lutte contre la fraude [(2)]. Si l'utilisation du SNIIRAM progresse au niveau national, le nombre de requêtes annuelles étant passé de 146 en 2012 à 392 en 2014, elle reste très inégale au niveau des caisses primaires d'assurance maladie et des directions régionales du service médical. C'est pourquoi la Cour recommande d'exploiter le potentiel du SNIIRAM à des fins de gestion du risque, notamment pour sanctionner plus systématiquement les comportements abusifs, fautifs et frauduleux. Le rapporteur est extrêmement favorable à cette recommandation.

S'agissant de l'organisation de l'offre de soins, l'utilisation des données du SNIIRAM contribue, dès à présent, à l'organisation de la permanence des soins ambulatoires. La CNAMTS transmet aux agences régionales de santé (ARS) les données relatives aux astreintes et aux actes réalisés afin de leur permettre de définir le découpage territorial le plus approprié et le nombre de professionnels de santé nécessaire.

En permettant une étude territoriale des données de santé, le SNDS pourrait également servir à réduire les inégalités territoriales en réorientant l'organisation de l'offre de soins. La Cour des comptes relève qu'une exploitation directe des données du SNIIRAM permettrait d'améliorer l'élaboration des schémas régionaux d'organisation des soins des agences régionales de santé.

### *d. L'enjeu scientifique : contribuer aux progrès de la recherche*

Les chercheurs en sciences médicales ont besoin de disposer de masses d'informations – particulièrement de mesures tirées de la vie réelle. L'ouverture des bases de données peut faciliter la reproductibilité de la preuve et permettre la constitution de cohortes significatives. D'ores et déjà, les organismes de recherche forment la deuxième catégorie utilisatrice de la base SNIIRAM, avec 93 comptes actifs à la fin du mois de septembre 2016. [(3)]

Ainsi, un programme dénommé Epidemium [(4)] – lancé conjointement en 2015 par un laboratoire pharmaceutique majeur des traitements anticancéreux, et La Paillasse, laboratoire « ouvert et communautaire » [(5)] – utilise de façon

*(1) Audition du 17 janvier 2017.*

*(2) Cour des comptes, op. cit.*

*(3) Les ARS comptent 84 utilisateurs actifs et l'IDS 83 comptes actifs fin septembre 2016.*

*(4) Voir « Cédric Villani : "Le big data va booster la recherche contre le cancer" », Journal du dimanche, 5 février 2017.*

*(5) Le laboratoire La Paillasse se définit comme « un réseau de laboratoires interdisciplinaires offrant sans discrimination d'âge, de diplôme ou de revenu, le cadre technique, juridique et éthique nécessaire à la mise en œuvre de projets collaboratifs et open-source. »*

systématique les données statistiques des grandes bases de données afin de les croiser pour détecter des situations à risque dans le domaine de la cancérologie.

M. Alain Pelc, directeur chargé des études, des répertoires et des statistiques à la Caisse centrale de la Mutualité sociale agricole (CCMSA), a fait part de l'intérêt de celle-ci pour le SNDS, qui devrait faciliter le développement de la recherche sur des maladies à caractère professionnel, et plus particulièrement sur des maladies émergentes dans le champ agro-environnemental. Il s'est aussi félicité de l'intégration dans le SNDS de la base CepiDC, qui indique les causes de décès, ce qui permettra à la CCMSA de mener des études sur le suicide chez les exploitants agricoles et de travailler à leur prévention [(1)].

La commission *open data* a souligné que l'accès à cette base de données élargie et enrichie donnera à la recherche française un réel avantage. Ce point a été confirmé par les représentants des entreprises du médicament. Néanmoins des progrès restent à faire pour que les instituts de recherche et les chercheurs s'approprient ce système. M. Antoine Durrleman a d'ailleurs relevé que le SNIIRAM n'était pas vu comme un outil de recherche par le ministère de la recherche [(2)].

### *e. Les finalités interdites : éviter la marchandisation de la santé*

L'ouverture des données personnelles de santé a suscité des craintes, particulièrement celle de leur utilisation par les assureurs et les industriels de la santé à des fins mercantiles. C'est pourquoi l'article L. 1461-1 du code de la santé publique interdit expressément, d'une part, aux assureurs d'utiliser ces données à des fins d'exclusion de garanties ou de modification de cotisations ou primes d'assurance et, d'autre part, aux industriels de la santé de s'en servir pour un démarchage commercial des professionnels de santé.

Le rapporteur tient à rappeler que cette clarification bienvenue est issue du travail parlementaire. En effet, l'exploitation des données de santé ne doit pas être dévoyée vers une marchandisation qui aboutirait à rompre le principe républicain d'égalité devant la santé porté depuis l'origine par la Sécurité sociale.

Répondant à une question du rapporteur, M. Philippe Burnel a confirmé qu'était prohibée pour les assureurs la logique de sélection du risque et d'adaptation de la tarification ; il en est de même pour le ciblage territorial ou professionnel du démarchage commercial des prescripteurs de médicaments [(3)]. M. Franck von Lennep, directeur de la DREES, a également souligné que les assureurs ne pourraient pas utiliser les données du SNDS pour élaborer une tarification fondée sur l'état de santé des assurés [(4)].

---

*(1) Audition du 17 janvier 2017.*

*(2) Audition du 3 mai 2016.*

*(3) Audition du 13 décembre 2016.*

*(4) Audition du 20 décembre 2016.*

Néanmoins, ces catégories d'opérateurs pourront commanditer des recherches si leur finalité inclut un motif d'intérêt public, selon certaines conditions développées *infra*. M. Franck von Lennep a ainsi souligné : « *il nous semble également important de permettre aux acteurs privés, y compris les assureurs ou les industriels de santé, de soumettre les données aux usages autorisés.* »

## B. UNE OUVERTURE CONTRÔLÉE DES BASES DE DONNÉES

L'ouverture plus large des bases de données doit s'accompagner d'un dispositif d'accès rénové. La loi a suivi les recommandations de la commission *open data* qui « *considère qu'il convient de donner accès sans restrictions* (open data) *aux données de santé, y compris la possibilité de les réutiliser, dès lors qu'elles ne sont pas porteuses de risque de réidentification.* […] *La préservation du secret des données personnelles de santé justifie en revanche des précautions pour l'accès aux données de santé dès lors qu'elles sont porteuses de risque de réidentification du patient* » [(1)].

### 1. Des données regroupées dans un nouveau système d'information

Le SNDS a vocation à transformer un ensemble de bases de données médico-administratives conçues pour piloter le système de soins en un système permettant de réaliser des études et des recherches. Son insertion dans le code de la santé publique [(2)] est significative de l'évolution des finalités assignées à cet outil, à savoir une logique globale de pilotage de la santé publique et de soutien à la recherche, alors que le SNIIRAM, conçu à l'origine comme outil de pilotage des dépenses de santé, est prévu par le code de la sécurité sociale [(3)].

L'article L. 1461-1 du code de la santé publique définit le périmètre du SNDS : il comprendra les bases existantes du SNIIRAM, du PMSI et du CépiDC. Seront ensuite introduites les données médico-sociales et les données de remboursement des organismes d'assurance maladie complémentaire, qui figureront dans de nouveaux systèmes d'information à mettre en place.

Un décret en Conseil d'État fixe la liste des catégories de données qui figureront au sein du SNDS et leurs modalités d'alimentation, étant entendu que la gestion de ces bases continue de relever des opérateurs producteurs de données [(4)].

Six catégories de données seront réunies :

– les informations relatives aux bénéficiaires de soins et de prestations médico-sociales ;

---

*(1) Commission open data en santé, op. cit.*

*(2) Articles L. 1461-1 à L. 1461-7 du code de la santé publique.*

*(3) Article L. 161-28-1 du code de la sécurité sociale.*

*(4) Articles L. 1461-7 et R. 1461-4 du code de la santé publique.*

– les informations relatives aux organismes d'assurance maladie obligatoire et, s'il y a lieu, aux organismes d'assurance maladie complémentaire intervenant dans la prise en charge financière du bénéficiaire des soins et des prestations ;

– les informations relatives à la prise en charge sanitaire, médico-sociale et financière associée à chaque bénéficiaire ;

– les informations relatives aux professionnels et services de santé intervenant dans la prise en charge des bénéficiaires ;

– les informations médico-sociales relatives à la situation des personnes en situation de handicap ;

– les informations relatives aux arrêts de travail et aux prestations en espèces.

Combinant des données médicales et médico-sociales, le système a vocation à être très riche, mais il n'en demeure pas moins que dans l'immédiat, seules trois bases – le SNIIRAM, le PMSI et le CépiDC – sont opérationnelles.

Une première version du SNDS, comprenant le SNIIRAM et le PMSI, doit entrer en fonction le 1er avril 2017 (1).

- *Le SNIIRAM*

Le Système national d'information inter-régimes de l'assurance maladie (SNIIRAM) (2) recueille des informations individuelles sur les patients issues des feuilles de soins transmises aux organismes d'assurance maladie obligatoire à des fins de liquidation. La CNAMTS en assure la gestion. Depuis septembre 2009, cette base a été alimentée par tous les régimes d'assurance maladie obligatoire, y compris les régimes spéciaux, et est devenue véritablement inter-régime. En 2010, son chaînage avec le PMSI a permis un suivi des consommations individuelles de soins pour un même patient, à la fois en ville et à l'hôpital.

Plusieurs types de données figurent dans la base :

– données sur le bénéficiaire ;

– données sur la prestation ;

– période des soins ;

– date d'effet des prestations permanentes ;

---

*(1) Article 2 du décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».*

*(2) Créé par l'article 21 de la loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale pour 1999.*

– mode de prise en charge lié au bénéficiaire ;

– informations médicalisées du bénéficiaire ;

– mode de prise en charge lié à la prestation ;

– données sur le professionnel de santé.

La richesse de la base ne doit pas occulter l'absence de données qui pourraient être précieuses. La Cour des comptes a recensé ces limites [(1)].

En premier lieu, la nature même des données – des informations administratives liées à la liquidation de soins du régime obligatoire – ne donne aucune information sur les soins non remboursés ou pris en charge par une complémentaire santé. Il n'est donc pas possible d'étudier des pratiques d'automédication ou de connaître les restes à charge. Par ailleurs, M. Dominique Martin a cité l'exemple des prothèses mammaires PIP, non remboursées, qui ont soulevé des problèmes de sécurité sanitaire [(2)].

En deuxième lieu, la qualité des informations médicales est insuffisante. La Cour des comptes relève qu'en soins de ville, seules les affections de longue durée et les maladies professionnelles y figurent. Il manque à ce jour le codage des pathologies en soins de ville chez les médecins généralistes selon la classification internationale des actes médicaux (CIM-10) de l'Organisation mondiale de la santé, bien que cette obligation figure à l'article L. 161-29 du code de sécurité sociale. C'est ce qui a amené M. Philippe Burnel à affirmer que les données cliniques en médecine de ville sont le plus gros manque du SNIIRAM [(3)]. Ce constat est partagé par M. Thomas Borel, qui souhaiterait une amélioration de la médicalisation de l'information. Néanmoins, le docteur Jacques Lucas a émis des réserves sur ce codage : « *toute cotation spécifique étant parfaitement identifiante, cela peut, en fonction des pathologies, avoir un effet stigmatisant et discriminant pour les patients.* » [(4)]

À cet égard, M. Nicolas Revel a rappelé que la CNAMTS a introduit un nouvel élément de rémunération dans le forfait structure des médecins afin de les encourager à coder les données cliniques de leurs patients et à participer à la définition ou à la mise en place de registres permettant le suivi de malades atteints d'une pathologie donnée. L'enjeu est de pouvoir, à terme, étudier les relations entre la pathologie et les actes et soins prescrits [(5)].

Ne figurent pas non plus dans le SNIIRAM les examens biologiques, les facteurs de risques (antécédents familiaux) ou les données socio-économiques, à

*(1) Cour des comptes,* op. cit.

*(2) Audition du 31 janvier 2017.*

*(3) Audition du 13 décembre 2016.*

*(4) Audition du 31 janvier 2017.*

*(5) Audition du 17 janvier 2017.*

l'exception du bénéfice de la couverture maladie universelle complémentaire (CMU-C). M. Dominique Martin a également plaidé pour une intégration de données sociodémographiques qui permettraient de disposer d'éléments de contexte dans l'analyse du risque [(1)].

C'est pourquoi les rapports de la commission *open data* et de la Cour des comptes recommandent d'accroître le périmètre descriptif des patients et de rendre accessibles des variables socio-économiques. La Cour des comptes préconise plus particulièrement d'enrichir le SNIIRAM par le codage médical des soins de ville afin d'améliorer les données médicales et de faciliter leur rapprochement avec les données socio-économiques [(2)]. Le rapporteur est favorable à cette évolution.

- *Le PMSI*

Le Programme de médicalisation des systèmes d'information (PMSI) rassemble les informations sur les séjours hospitaliers, en médecine-chirurgie-obstétrique (MCO), en soins de suite et de réadaptation (SSR), en hospitalisation à domicile (HAD) ou en psychiatrie. Le PMSI est géré par l'Agence technique de l'information sur l'hospitalisation (ATIH).

L'article L. 6113-7 du code de la santé publique précise que les établissements de santé, publics et privés, doivent mettre en œuvre des systèmes d'information qui tiennent compte des pathologies et des modes de prise en charge du patient. Ils comprennent ainsi des données relatives à :

– l'identification du patient ;

– des informations médicales, y compris le codage des diagnostics ;

– la gestion du séjour ;

– la facturation ou la tarification.

- *La base CépiDC*

L'article L. 2223-42 du code général des collectivités territoriales dispose que l'autorisation de fermeture d'un cercueil ne peut être délivrée qu'au vu d'un certificat établi par un médecin qui atteste le décès. Ce certificat doit mentionner la ou les causes de décès et permet d'alimenter la base gérée par le Centre d'épidémiologie de l'Institut national de la santé et de la recherche médicale (INSERM). Celle-ci a pour finalité l'établissement de statistiques nationales des causes de décès et contribue à faciliter la recherche publique de l'INSERM.

Selon M. Nicolas Revel, l'intégration de cette base au SNDS est prévue dans un délai d'un an.

---

*(1) Audition du 31 janvier 2017.*

*(2) Cour des comptes,* op. cit.

- *Les données médico-sociales des maisons départementales de personnes handicapées (MDPH)*

L'un des avantages du SNDS est qu'il a vocation à regrouper des données médicales et médico-sociales. Néanmoins, l'intégration de ces données est rendue difficile par les problèmes rencontrés pour la mise en place de systèmes d'information dans les établissements médico-sociaux.

Un système d'information unique, dénommé RESID-EHPAD, a été mis en place dans les établissements d'hébergement pour personnes âgées dépendantes.

Ce n'est pas encore le cas pour les MDPH, bien que l'article R. 146-38 du code de l'action sociale et des familles prévoit qu'elles doivent mettent en œuvre un système de gestion et d'information. Il est expressément indiqué que ce traitement automatisé a notamment pour but la production de statistiques relatives au suivi des personnes et à l'activité des structures. La Caisse nationale de solidarité pour l'autonomie sera chargée de centraliser ces données.

Selon Mme Chantal Cases, le fichier national des MDPH n'est pas fondé jusqu'à présent sur le numéro d'inscription au répertoire (NIR), ce qui suppose un travail d'identification pour pouvoir l'apparier au SNDS ; cette difficulté technique retarde d'autant l'intégration du fichier national dans le SNDS [(1)]. La DREES a indiqué que les premiers flux ne remonteraient pas avant 2019.

- *Un échantillon représentatif des remboursements des organismes d'assurance maladie complémentaire*

Le cinquième alinéa de l'article L. 1461-1 du code de la santé publique prévoit que sera constitué un échantillon représentatif des remboursements des organismes d'assurance maladie complémentaire, qui recueillera des données de remboursement par bénéficiaire et sera défini en concertation avec les représentants des organismes d'assurance maladie complémentaire.

Une première expérimentation a eu lieu sous la forme d'un appariement d'échantillons de données du régime général obligatoire (CNAMTS, CCMSA, RSI) et des complémentaires santé (institutions de prévoyance, mutuelles et assureurs) en 2010. Ce projet, dénommé MONACO (Méthodes, outils et normes pour la mise en commun des données des assurances complémentaire et obligatoire), devait permettre d'analyser le reste à charge des patients. Un système d'information dédié a été créé, piloté par l'Institut des données de santé.

Bien que cette expérimentation ait été considérée comme encourageante par l'Institut de recherche et documentation en économie de la santé (IRDES), qui a réalisé une étude sur les perspectives du projet, il convient de relever qu'elle a été conduite sur un échantillon restreint (2440 individus) et n'a touché que le quart du marché des complémentaires. Le test technique a permis de démontrer la

*(1) Audition du 20 décembre 2016.*

possibilité d'apparier des données du régime obligatoire et des données des organismes de couverture complémentaire, mais il reste nécessaire de définir un cahier des charges technique pour une mise en œuvre opérationnelle à plus grande échelle. Mme Chantal Cases a estimé qu'« *Il faut mettre en place un système susceptible de rendre compte d'un échantillon représentatif d'assurés, et donc réaliser un échantillon aléatoire et en faire un tirage en accord avec les familles de complémentaires santé. Toutes les complémentaires qui figurent dans cet échantillon doivent pouvoir techniquement envoyer des données.* » (1) La DREES a indiqué qu'un cadrage en ce sens était en cours.

Cependant, M. Christian Babusiaux, ancien président de l'Institut des données de santé, a fait part de ses doutes sur la transmission de ces données au SNDS par les organismes d'assurance maladie complémentaire. Cet apport doit se faire en concertation avec leurs principaux représentants : « *je m'interroge sur les données qui devraient provenir des complémentaires de santé : certes, le texte législatif en fait mention mais qui, en France, pourrait contraindre des entreprises privées et des mutuelles à fournir des données alors même qu'on essaie de les exclure de la gouvernance du système ?* » (2)

### 2. Un accès encadré et un partage maîtrisé

Le dispositif définit un droit d'accès aux bases de données différencié selon la nature des données et la nature du demandeur.

#### *a. La nature des données*

Les conditions de mise à disposition des données diffèrent selon la nature de ces données.

Les données agrégées qui ne présentent aucun risque de réidentification, définies comme des statistiques présentées par groupes d'individus qui sont constitués de patients présentant tous des critères identiques ou de données individuelles appauvries, seront ouvertes à tous de manière gratuite.

Les données relatives à l'activité des professionnels de santé – notamment leurs tarifs – seront également ouvertes à tous.

Par contre, les données qui correspondent à un seul individu et sont potentiellement identifiantes seront ouvertes sous conditions pour des recherches, évaluations et études présentant un intérêt public.

#### *b. La nature du demandeur*

Parallèlement, l'accès sera différent selon la nature du demandeur, les organismes publics bénéficiant d'un dispositif simplifié.

---

*(1) Audition du 20 décembre 2016.*

*(2) Audition du 17 janvier 2017.*

- *Les opérateurs publics*

Les services publics – services de l'État, établissements publics et organismes chargés d'une mission de service public – bénéficieront d'un accès permanent, nommément accordé à des personnes habilitées [(1)] ; ainsi, dans le cadre de leurs missions, ces opérateurs n'auront pas besoin de demander d'autorisation de traitement chaque fois qu'ils souhaiteront utiliser le SNDS.

Une liste des opérateurs concernés est établie par décret en Conseil d'État [(2)]. Y figurent, notamment, la DREES, la direction générale de la santé, la direction générale de l'offre de soins, la direction de la sécurité sociale, la direction du budget et le service de santé des armées, les caisses nationales de régime de l'assurance maladie obligatoire, certaines agences sanitaires, l'Institut national des données de santé (INDS), l'IRDES ainsi que des équipes de recherche de l'INSERM, des centres hospitaliers universitaires ou de l'École des hautes études en santé publique.

Les agences régionales de santé disposent de nouvelles modalités d'accès au SNDS [(3)]. L'évolution la plus importante consiste à habiliter l'ensemble des personnels, et non plus les seuls médecins, à consulter les données du SNDS.

L'étendue de cet accès permanent est néanmoins encadrée, comme l'a souligné M. Franck von Lennep [(4)], selon des critères tels que le périmètre ou la profondeur des données et le type de variables qui pourront être croisées [(5)]. L'article R. 1461-11 du code de la santé publique prévoit ainsi que l'étendue de cette autorisation sera limitée selon deux critères :

« *1° Par la profondeur historique des données utilisées, l'aire géographique ou les caractéristiques d'une population déterminée au regard des finalités sanitaires ou sociales du traitement ;*

« *2° Par la possibilité ou non d'utiliser de manière simultanée dans un même traitement, en sus des autres informations relatives aux soins et à la prise en charge, plusieurs variables, dénommées identifiants potentiels, dont la combinaison accroît le risque de réidentification. Ces identifiants potentiels sont la période de naissance exprimée en mois et année, le code de la commune de résidence et les données infracommunales de localisation, la date des soins, la date du décès et le code de la commune de décès.* »

Par ailleurs, dans ce cadre d'accès permanent, les opérateurs publics désigneront en leur sein un correspondant informatique et libertés qui dressera une liste des traitements mis en œuvre et de leurs caractéristiques ; cette liste sera

*(1) Les responsables des opérateurs publics nommeront ces personnes habilitées.*

*(2) Article R. 1461-12 du code de la santé publique.*

*(3) Article L. 1435-6 du code de la santé publique.*

*(4) Audition du 20 décembre 2016.*

*(5) Article R. 1461-11 du code de la santé publique.*

transmise annuellement à la CNIL et au comité stratégique chargé de fixer les orientations de développement du SNDS [(1)].

La liste des opérateurs publics au sens du SNDS est plus restrictive que celle figurant dans l'arrêté du 19 juillet 2013 modifié relatif à la mise en œuvre du SNIIRAM. Ainsi, l'Union nationale des professionnels de santé (UNPS) a regretté de ne pouvoir accéder au SNDS au titre des « organismes publics », alors même que les unions régionales de professionnels de santé sont habilitées [(2)]. Elle déplore un accès plus restrictif que celui dont elle dispose actuellement. En effet, selon l'arrêté du 19 juillet 2013 précité, l'UNPS a accès aux données de la base SNIIRAM sous forme de statistiques agrégées ou sous une forme individualisée de l'échantillon généraliste. L'UNPS souhaite conserver un accès facilité à la base SNDS pour pouvoir disposer du même niveau d'information que ses interlocuteurs dans les négociations conventionnelles. La Cour des comptes relève, cependant, que son accès actuel au SNIIRAM ne l'a pas conduite à effectuer des analyses des pratiques des professionnels de santé, sous l'angle de la qualité des soins.

- *Les opérateurs privés*

Les opérateurs privés – entreprises produisant ou commercialisant des produits à finalité sanitaire [(3)], banques, sociétés d'assurances, mutuelles ou institutions de prévoyance – pourront disposer d'un accès ponctuel soumis au respect de trois conditions [(4)].

En premier lieu, les recherches, études ou évaluations devront avoir une finalité d'intérêt public et contribuer aux finalités fixées à l'article L. 1461-3 du code de la santé publique. M. Philippe Burnel a précisé que l'intérêt privé « porteur » d'un intérêt public pourrait voir autoriser sa requête : « *Après de nombreux débats, nous avons considéré que cet intérêt public n'interdisait pas l'existence, en parallèle, d'un intérêt privé, mais que ce dernier ne pouvait constituer la seule finalité pour accéder aux données médicales.* » [(5)] La notion d'intérêt public reste encore imprécise, ce que n'a pas manqué de soulever M. Christian Babusiaux, qui aurait préféré une formulation différente, comme celle d'« intérêt pour plusieurs types d'acteurs » : l'accès aux données « *peut correspondre à l'intérêt des patients et des professionnels de santé, ou à celui de l'assurance maladie, des hôpitaux ou encore des complémentaires de santé – en clair, à "plusieurs groupes d'acteurs".* » [(6)] Il en est de même pour le docteur Jacques Lucas, qui juge cette notion d'intérêt public floue et préconise la mise en place d'un comité d'éthique auprès du futur INDS, qui serait composé de

*(1) Article R. 1461-10 du code de la santé publique.*

*(2) Audition du 20 décembre 2016.*

*(3) L'article L. 5311-1 du code de la santé publique liste aussi bien les médicaments, les dispositifs médicaux, les logiciels médicaux que les produits cosmétiques.*

*(4) Article L. 1461-3 du code de la santé publique.*

*(5) Audition du 13 décembre 2016.*

*(6) Audition du 17 janvier 2017.*

personnalités qualifiées chargées de se prononcer sur le caractère d'intérêt public des requêtes [1].

En deuxième lieu, pour les opérateurs privés, ces recherches, études ou évaluations devront être réalisées par un intermédiaire, un laboratoire de recherche ou un bureau d'études public ou privé, à moins qu'ils ne démontrent que leur méthodologie garantit qu'ils n'enfreignent pas les interdictions relatives aux usages prohibés. Ces prestataires devront présenter à la CNIL un engagement de conformité à un référentiel arrêté par le ministre chargé de la santé qui inclura des critères de confidentialité, d'expertise et d'indépendance.

Enfin, des informations devront être fournies, au préalable, au futur INDS, à savoir l'autorisation de la CNIL, une déclaration des intérêts du demandeur et le protocole d'analyse. En fin de traitement, le demandeur communiquera à l'INDS la méthode utilisée, les résultats et les moyens d'en évaluer la validité. L'INDS se chargera de publier les résultats et la méthode.

***c. Les procédures***

L'objectif du nouveau dispositif est de simplifier la procédure d'accès aux bases de données en instaurant un guichet unique pour toutes les demandes : le futur Institut national des données de santé (INDS). Mme Chantal Cases a déclaré que « *le futur INDS sera le lien entre tous les utilisateurs des données, publics et privés.* » [2] L'article 20 du décret n° 2016-1872 du 26 décembre 2016 prévoit que, dès réception d'une demande d'autorisation de traitement de données, le secrétariat de l'INDS la transmettra pour avis dans un délai maximal de 7 jours au comité compétent [3] :

– pour des recherches biomédicales, auprès du comité de protection des personnes (CPP) ;

– pour des recherches sur des données n'impliquant pas la personne humaine, auprès du comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (CEREES).

L'article 25 du décret n° 2016-1872 du 26 décembre 2016 détaille la composition et le fonctionnement du CEREES. 21 membres seront nommés par arrêté conjoint des ministres chargés de la santé et de la recherche, sur proposition d'un comité de sélection [4]. Au moins 3 membres devront être experts en données de santé et seront proposés par la CNAMTS, l'Agence nationale de santé publique et l'INSERM. Le mandat indemnisé de ces membres sera de 3 ans, renouvelable une fois. Ces dispositions correspondent aux recommandations de M. Franck

*(1) Audition du 31 janvier 2017.*

*(2) Audition du 20 décembre 2016.*

*(3) Décret n° 2016-1872 du 26 décembre 2016 modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

*(4) La composition de ce comité sera fixée par arrêté. Un appel à candidatures a été lancé en janvier 2017.*

von Lennep, qui avait souhaité que le comité soit suffisamment étoffé et comprenne une vingtaine d'experts indemnisés [(1)]. Le CEREES se réunira au moins 12 fois par an et pourra fixer des réunions supplémentaires. Les réunions ne seront pas publiques mais ses avis seront publiés par l'INDS.

Le CEREES devra se prononcer notamment sur la qualité scientifique du projet, la méthodologie retenue et la nécessité de disposer de données personnelles au regard de la finalité et de la méthode proposée. À défaut d'avis dans le délai d'un mois, celui-ci sera réputé favorable. En cas d'urgence, le délai pourra être ramené à quinze jours.

Enfin, lorsque le comité aura rendu un avis favorable, la CNIL accordera ou non l'autorisation d'effectuer le traitement. Son secrétaire général, M. Édouard Geffray, a rappelé son champ de compétences : « *la CNIL définira, en tenant compte de l'appréciation portée par le CEREES, les conditions de traitement des données* » [(2)]. Elle statuera sur la durée de conservation des données nécessaires au traitement et appréciera les dispositions prises pour assurer leur sécurité vis-à-vis du risque d'atteinte à la vie privée [(3)]. Elle vérifiera également les garanties présentées par le demandeur et la conformité de sa demande à ses missions ou à son objet social.

Par ailleurs, la CNIL sera sollicitée si le CEREES émet un avis avec recommandations, réservé ou défavorable, et si le demandeur en fait part au secrétariat de l'INDS [(4)].

En outre, il est prévu la possibilité d'une saisine parallèle du futur INDS soit par lui-même, soit par la CNIL ou le ministre de la santé, pour examiner si la demande de recherche, d'étude ou d'évaluation présente un caractère d'intérêt public. L'INDS devra rendre un avis motivé dans un délai d'un mois à compter de sa saisine. Cette modalité risque de compliquer le processus [(5)].

Si ce dispositif vise à fluidifier l'accès aux bases de données, le Rapporteur n'est pas persuadé que l'intervention de plusieurs organismes publics et comités simplifie les procédures. Par ailleurs, l'amélioration de l'accès aux bases de données passe avant tout par des moyens humains à la hauteur des enjeux ; ce point sera développé *infra*.

L'enjeu principal est, en effet, de raccourcir les délais nécessaires pour obtenir l'autorisation d'effectuer un traitement des données contenues dans ces bases. Il s'agit d'un des points les plus critiqués du dispositif antérieur. La Cour des comptes a insisté sur cette appétence des équipes de recherche et d'évaluation, qui, confrontées à de longs délais, de l'ordre de 18 mois, se découragent. M. Alain

*(1) Audition du 20 décembre 2016.*

*(2) Audition du 24 janvier 2017.*

*(3) Article 54 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

*(4) Article 23 du décret n° 2016-1872 du 26 décembre 2016.*

*(5) Article 24 du décret n° 2016-1872 du 26 décembre 2016.*

Pelc a d'ailleurs rapporté que ses équipes attendaient depuis plus de 8 mois l'autorisation de la CNIL pour mener une recherche sur les maladies à caractère professionnel émergentes dans le champ agro-environnemental [(1)].

Selon Mme Valérie Edel, directrice adjointe de l'IDS, ces délais qui, fin 2015, étaient de l'ordre de 15 mois, ont été ramenés à 3 ou 4 mois en 2016 [(2)].

M. Franck von Lennep a souligné que la mise en place de méthodologies de référence pour l'utilisation des catégories les plus usuelles de traitements de données permettrait aussi de raccourcir de façon substantielle les délais d'instruction des demandes d'accès : « *Nous avons également pour objectif de multiplier les méthodologies de référence qui sont des procédures standardisées définies par la CNIL. Si un utilisateur s'engage à respecter l'une de ces méthodologies, alors il n'a plus besoin de demander l'autorisation de la CNIL. L'utilisateur se déclare conforme, et des audits seront réalisés* ex post. » [(3)] Trois méthodologies sont applicables actuellement : la MR-001 encadre des recherches interventionnelles ou biomédicales, des essais cliniques de médicaments et des recherches nécessitant la réalisation d'un examen des caractéristiques génétiques ; la MR-002 concerne les études non interventionnelles de performances menées sur les dispositifs médicaux *in vitro* ; la MR-003 encadre des recherches en soins courants, des recherches non interventionnelles et des essais cliniques de médicaments par grappe.

La CNIL peut aussi accorder des autorisations cadres, dont bénéficient déjà l'ANSM et l'ANSP. M. Mahmoud Zureik s'est félicité de ce dispositif : « *L'autorisation cadre a été délivrée en 2013. Nous n'avons pas à solliciter d'autres autorisations lorsque nous voulons mener des études. C'est une avancée majeure car nous avons parfois besoin de réponses extrêmement rapides*. » [(4)]

Des procédures simplifiées seront également élaborées, en particulier pour l'accès à l'échantillon généraliste de bénéficiaires (EGB), très demandé. L'autorisation d'accès à des jeux de données agrégées ou à des échantillons pourra être déléguée par la CNIL au futur INDS, dans le cadre d'une procédure homologuée et publiée par la CNIL [(5)].

M. Franck von Lennep a aussi insisté sur la nécessité de mieux structurer les projets et les demandes en amont. L'une des explications à la longueur actuelle de l'instruction des demandes tient, selon lui, « *au fait que des demandes relatives aux données médico-administratives parviennent à la CNIL sans avoir été assez normées et étudiées en amont, ce qui oblige à une interaction avec le demandeur*. » Dans la nouvelle procédure, l'échange avec l'utilisateur s'opèrera avec le CEREES, en amont de l'intervention de la CNIL.

---

*(1) Audition du 17 janvier 2017.*

*(2) Audition du 20 décembre 2016.*

*(3) Audition du 20 décembre 2016.*

*(4) Audition du 31 janvier 2017.*

*(5) Article 54 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

***d. Un partage maîtrisé***

Si le rapport de la commission *open data* recommande « *de donner accès sans restriction (open data) aux données de santé, y compris la possibilité de les réutiliser, dès lors qu'elles ne sont pas porteuses de risque de réidentification* » [(1)], elle porte un jugement plus nuancé sur les données pseudonymisées du SNIIRAM et du PMSI : « *Il ne s'agit pas de fermer l'accès aux données mais de l'organiser en se fondant sur une évaluation objective et explicite des risques de réidentification mis en regard des bénéfices attendus.* » C'est pourquoi la commission préconisait d'« *organiser l'accès* [à ces dernières] *de telle sorte que les risques soient évalués et mis en regard des bénéfices attendus* ».

Afin de limiter le risque d'atteinte à la liberté de la vie privée, le respect de deux principes sera affirmé dans le référentiel de sécurité relatif aux règles de la gestion sécurisée, en instance de publication.

En premier lieu, le partage de ces données est soumis à un dispositif de pseudonymisation. L'article L. 1461-4 du code de la santé publique précise que « *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.* » L'article R. 1461-7 du même code indique les modalités pratiques de mise en œuvre de cette pseudonymisation : « *Un pseudonyme, constitué d'un code non signifiant obtenu par un procédé cryptographique irréversible du numéro d'inscription au Répertoire national d'identification des personnes physiques est associé aux données se rapportant à chaque personne.* » M. Franck von Lennep a insisté sur la confidentialité du dispositif en relevant que cette procédure est organisée de façon que nul ne dispose à la fois de l'identité des personnes et du pseudonyme.

En deuxième lieu, une obligation de traçabilité est introduite afin de réduire les risques de dissémination des données : « *Les modalités de conservation et d'utilisation des données permettent d'en contrôler les usages et de fournir des preuves en cas d'usage non autorisé.* » [(2)]

Par ailleurs l'article L. 1461-1 du code de la santé publique dispose que « *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* » et que les personnes responsables de ces traitements et celles qui les utilisent sont soumises au secret professionnel.

Le rapporteur tient cependant à souligner que les traitements de pseudonymisation appliqués aux données versées au SNDS ne permettent pas de garantir que les bénéficiaires des soins restent anonymes. Les autorités publiques à l'origine du SNIIRAM et du PMSI n'en avaient d'ailleurs pas pris immédiatement conscience. Comme l'a rappelé M. Philippe Burnel, « *Lorsque j'étais en charge*

*(1) Commission open data en santé*, op. cit., *page 43.*

*(2) Article R. 1461-7 du code de la santé publique.*

*du PSMI, nous avions créé le résumé de sortie anonyme (RSA) de l'hôpital qui tronquait certaines informations : au lieu des dates d'entrée et de sortie, c'est la durée du séjour qui était mentionnée, l'âge remplaçait la date de naissance… À l'époque, nous étions persuadés d'avoir "anonymisé" le RSA. En 1994, la Commission nationale de l'informatique et des libertés (CNIL), saisie de l'arrêté de création de ce dispositif, avait même considéré qu'elle n'avait pas à se prononcer, s'agissant de données anonymes. Cependant, progressivement, nous avons pris conscience, et la CNIL avec nous, que ces données n'étaient pas "anonymisées" mais seulement "pseudonymisées". Dans certaines conditions, il était possible d'identifier le patient, et si l'on "repérait son voisin de palier", on pouvait accéder à l'ensemble de ses données.* » (1)

Lors de son audition (2), le docteur Dominique Blum – qui appartenait à la mission PMSI et qui s'est intéressé, depuis 2009, aux problèmes d'anonymat et de ré-identification que soulevait ce programme – a également déclaré : « *Le résumé de sortie anonymisé (RSA) à l'hôpital est une de mes inventions. Elle est due à ce que la Commission nationale de l'informatique et des libertés (CNIL) nous avait informés que le résumé de sortie standardisé, que tous les hôpitaux et toutes les cliniques produisaient, avait un caractère indirectement nominatif.*

« *J'ai alors proposé un dispositif d'appauvrissement du contenu qui a consisté à remplacer la date de naissance du patient par son âge et les dates d'entrée et de sortie d'hospitalisation par le mois de sortie et la durée du séjour, et quelques autres modifications de cette nature.*

« *Nous étions persuadés, à l'époque, que les bases étaient ainsi véritablement anonymisées. Mais, en 1997, pensant qu'il fallait être précautionneux, j'ai repris la base nationale et je me suis rendu compte qu'en combinant les informations, même appauvries, on aboutissait à des combinaisons uniques dans la base de données nationales.*

« *La note interne que j'ai alors publiée a amené le ministère à consulter la CNIL, laquelle a demandé que l'on procède à des adaptations pour les informations placées dans les fichiers distribués à l'extérieur – à l'époque, à la demande des journalistes en particulier, les bases de données étaient diffusées sous forme de cédérom.*

« *À partir de 2002, je me suis éloigné du PMSI jusqu'en 2009, année de mon retour à la direction de la recherche, des études, de l'évaluation et des statistiques (DREES). J'ai alors constaté que le résumé de sortie anonymisé avait été extraordinairement enrichi et contenait de très nombreuses informations supplémentaires mais, par ailleurs, qu'aucune disposition n'avait été prise pour éviter les risques de ré-identification.*

---

*(1) Audition du 13 décembre 2016.*

*(2) Audition du 13 décembre 2016.*

« *Aussi ai-je conduit, en 2010, de nouveaux travaux, cette fois sur les données collectées en 2008, et j'ai démontré que si l'on connaît quelqu'un - j'entends par cela que si l'on connaît son âge, son sexe, le code postal de son lieu de résidence et la date de son entrée dans un établissement donné, ce qui est le cas d'un employeur, par exemple – on a 89 % de chances de le retrouver dans la base nationale, pourtant considérée comme anonyme ; la proportion passe à 100 % si la personne concernée a été hospitalisée au moins deux fois dans l'année. En effet, les combinaisons de données de la base nationale sont uniques si l'on dispose des informations que j'ai citées et quand on sait si le patient est sorti de l'établissement vivant ou mort.*

« *J'avais mis en évidence, en 1998, que le mode de sortie "décès" est un élément extrêmement discriminant ; aussi la CNIL avait-elle demandé que cette information soit supprimée des fichiers. Malgré cela, les éléments contenus dans le résumé de sortie anonymisé sont restés tout aussi ciblants.*

« *D'ailleurs, ayant renouvelé l'étude en 2015 sur les données collectées en 2013, je suis parvenu à des conclusions identiques : si on les connaît, neuf patients sur dix peuvent être ré-identifiés à coup sûr, et tous peuvent l'être s'ils ont été hospitalisés au moins deux fois dans l'année.*

« *De plus, le programme est un chaînage longitudinal et transversal, géographique et chronologique ; il résulte de ces caractéristiques que, quelle que soit la date de son hospitalisation depuis 2006 et quels que soient le secteur et l'établissement dans lequel le patient a été hospitalisé, on peut retrouver tous ces éléments si l'on en a trouvé un seul.*

« *J'ai appelé l'attention des pouvoirs publics à ce sujet en 2011, car je tiens à ce que la base de données puisse continuer d'être utilisée dans de bonnes conditions selon les finalités pour lesquelles elle a été créée, et aussi que les chercheurs puissent continuer à travailler sur ces données.*

« *Or chacun comprend que si une fuite se produisait qui permettait la divulgation d'éléments de santé d'une célébrité ou, pire encore peut-être, d'un citoyen quelconque qui aurait été identifié à son insu par son employeur ou par son assureur, et que cette intrusion était révélée, le grand public remettrait en cause le principe même de la base de données.* »

Le docteur Jacques Lucas a fait part, de son côté, de ses préoccupations quant à l'atteinte possible à la vie privée de ses patients : « *Ce n'est pas tant l'organisation du SNDS, récemment précisée par décret, qui nous préoccupe que les conditions d'accès aux données. L'ouverture de l'accès est nécessaire, mais vous ne serez pas surpris de m'entendre dire que le Conseil national de l'Ordre des médecins, particulièrement soucieux de la protection des libertés individuelles, souhaite que l'on ne puisse redescendre à un degré de granularité qui permettrait de reconnaître les personnes.* » [(1)]

*(1) Audition du 31 janvier 2017.*

C'est pourquoi le contrôle de l'utilisation de ces bases de données doit être renforcé et réorienté vers un contrôle *a posteriori* dans lequel la CNIL jouerait un rôle déterminant, ce que préconise la Cour des comptes. Celle-ci recommande, en premier lieu, de surveiller le nombre et la nature des requêtes réalisées et, en deuxième lieu, de mener des contrôles inopinés sur les utilisateurs [(1)].

M. Dominique Martin s'est dit favorable à ce type de contrôle, qui offrirait plus de souplesse aux utilisateurs : « *À mes yeux, les contrôles* a posteriori *assortis de sanctions sévères sont souvent aussi efficaces et plus efficients que des contrôles* a priori *qui peuvent entraver le déroulement du processus et sont souvent lourds à mettre en place.* » [(2)]

Les contours d'un contrôle *a posteriori* ne sont pas encore définis. Un comité d'audit et de contrôle devrait être mis en place et piloté par le Haut fonctionnaire de défense et de sécurité auprès des ministres chargés des affaires sociales.

M. Édouard Geffray a souligné que la CNIL devrait développer ses contrôles en aval sur les opérateurs bénéficiant d'un accès permanent. Il a aussi indiqué que le SNIIRAM faisait partie du programme de contrôle de la CNIL pour 2016 [(3)]. Le site internet de la CNIL précise que « *Les contrôles permettront de vérifier la conformité des traitements de données mis en œuvre avec l'ensemble des dispositions de la loi informatique et libertés, notamment la sécurité des données et la réalité de la pseudonymisation de ces dernières.* »

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a d'ores et déjà renforcé les pouvoirs de la CNIL en matière de contrôle et a durci les procédures de sanction. Son article 64 dispose que *« Lorsque le responsable d'un traitement ne respecte pas les obligations découlant de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut le mettre en demeure de faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'extrême urgence, ce délai peut être ramené à vingt-quatre heures.* »

Les sanctions pécuniaires sont également aggravées. Leur montant est proportionné à la gravité du manquement et aux avantages qui en sont tirés ; il peut atteindre 3 millions d'euros. La CNIL pourra également prononcer des sanctions financières sans mise en demeure préalable des organismes lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité [(4)].

Le Rapporteur estime que la question des moyens humains de la CNIL affectés à ce contrôle doit être posée. Le secrétaire général de la CNIL a indiqué que le service des contrôles compte 22 équivalents temps plein dont huit consacrés au service de la santé, pour environ 550 contrôles par an. Il a d'ailleurs indiqué

---

*(1) Cour des comptes,* op. cit.

*(2) Audition du 31 janvier 2017.*

*(3) Audition du 24 janvier 2017.*

*(4) Article 65 de la loi n 2016-1321 du 7 octobre 2016 pour une République numérique.*

que, bien que les contrôles *a posteriori* offrent plus de souplesse, « *si nous voulons atteindre un niveau d'exigence suffisamment élevé et universel, il est évident que nous aurons besoin de renforcer ces équipes*. » [(1)]

*(1) Audition du 24 janvier 2017.*

## II. LES QUESTIONS EN SUSPENS POUR LA CONSTRUCTION DU FUTUR SNDS

### A. DES TEXTES CONFUS OU INCOMPLETS QUI FRAGILISENT LE SOCLE JURIDIQUE DU SNDS

#### 1. Un règlement européen s'appliquera en 2018 aux données personnelles informatisées

##### *a. Un règlement européen renforce la protection juridique des données personnelles contre leur traitement informatique sans consentement*

Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données renforce la protection juridique des personnes physiques contre le traitement informatique de données qui les concernent et auquel elles n'auraient pas consenti.

L'article 5 de ce règlement exige qu'un tel traitement informatique soit subordonné à une finalité. Il suggère, mais n'exige pas, la conclusion préalable d'un contrat. Il ajoute à des exigences de licéité et de loyauté, caractéristiques du droit des contrats, une exigence de transparence, étrangère à ce droit. Le considérant 58 et l'article 12 caractérisent cette transparence par l'intelligibilité des obligations convenues et des informations dues, et non par leur publicité.

Le principe qui exige qu'un traitement informatique de données à caractère personnel soit consenti, explicitement, par les personnes concernées, est assorti d'exceptions.

L'article 5 considère que quiconque publie ses données personnelles consent à leur collecte et à leur traitement. L'article 6 autorise des traitements sans consentement préalable. Il les qualifie de nécessaires pour des finalités mais il ne sépare pas nettement les traitements licites par consentement de ceux qui le sont par nécessité.

Un intérêt vital, public ou légitime [(1)] suffit à rendre nécessaire un traitement informatique. Une obligation légale le peut aussi. Le considérant 44 dit même qu'un traitement peut être nécessaire dans le cadre d'un contrat ou de l'intention de conclure un contrat.

L'article 6 ne précise pas si la nécessité d'un traitement doit faire l'objet d'une déclaration ou d'une autorisation préalable. L'appréciation de cette nécessité pourrait relever de l'autorité de contrôle, organe spécifique de l'appareil

*(1) Il s'agit, en l'espèce, des «* intérêts légitimes poursuivis par le responsable du traitement ou par un tiers *», notion particulièrement floue que le considérant 47 s'efforce de cerner.*

administratif des États – relevant néanmoins de la catégorie des « autorités publiques indépendantes » – auquel le règlement soumet les traitements.

La saisine de cette autorité est d'ailleurs la principale mesure que le règlement suggère aux États pour sauvegarder les droits fondamentaux et protéger les intérêts des personnes concernées. L'autorité de contrôle peut connaître d'un traitement nécessaire. Elle peut aussi connaître d'un traitement convenu, avant que le juge du contrat soit saisi.

Pour que cette saisine soit possible et pour que les personnes concernées par un traitement de données puissent les rectifier, faire valoir leur droit à l'oubli ou à la portabilité et s'opposer à ce traitement, elles doivent recevoir du responsable du traitement des informations définies par les articles 13 et 14, dans le cas où les données à caractère personnel sont collectées auprès des personnes concernées (article 13) ou bien lorsque les données à caractère personnel n'ont pas été collectées auprès des personnes concernées (article 14), et indépendamment du caractère convenu ou nécessaire du traitement.

Dans le deuxième cas, l'opérateur d'un traitement est dispensé de les informer de ce traitement et de leur droit à s'y opposer lorsque « *la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés* » ou dans la mesure où cette information serait « *susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement.* » Le règlement prévoit qu'en pareille situation, « *le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles.* »

***b. Le règlement n'autorise que par exception le traitement de catégories particulières de données à caractère personnel, dont celles de santé***

L'article 9 protège davantage les données personnelles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ainsi que les données génétiques, biométriques ou concernant la santé, la vie sexuelle et l'orientation sexuelle d'une personne physique.

Il les fait bénéficier d'une interdiction de principe des traitements informatiques, assortie de dix exceptions. Parmi ces exceptions, on retrouve celles provoquées par le consentement de la personne concernée, qu'il soit explicite (cas *a*), présumé parce que la personne a manifestement rendu publiques les données traitées (cas *e*) ou lié à son adhésion à l'organisation à but non lucratif qui exécute le traitement (cas *d*).

Sept autres exceptions, déclarées nécessaires à une finalité, autorisent un traitement sans le consentement des personnes concernées et ce, pour les finalités suivantes :

– les droits et obligations du travail, de la sécurité sociale et de la protection sociale (cas *b*) ;

– les procédures juridictionnelles (cas *f*) ;

– un motif d'intérêt public important (cas *g*) ;

– la médecine préventive ou la médecine du travail, l'appréciation de la capacité de travail du travailleur, les diagnostics médicaux, la prise en charge sanitaire ou sociale, ou la gestion des systèmes et des services de soins de santé ou de protection sociale (cas *h*) ;

– 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 (cas *i*) ;

– une finalité archivistique dans l'intérêt public, une finalité de recherche scientifique ou historique ou une finalité statistique (cas *j*).

Dans les cas *b* et *g*, des mesures appropriées et spécifiques doivent être prises pour sauvegarder les droits et libertés de la personne concernée ainsi que ses intérêts.

Dans le cas *h*, les droits, libertés et intérêts des personnes concernées ne sont pas explicitement mentionnés. En revanche, le traitement doit s'opérer 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 soumis au secret professionnel ; l'opérateur du traitement agissant sous la responsabilité de ce professionnel doit également être tenu au secret.

Dans le cas *i*, seuls les droits et libertés doivent être protégés, non les intérêts des personnes, mais parmi les mesures appropriées à cette protection, le règlement cite le secret professionnel, sans l'imposer.

### *c. Les articles 5 et 9 admettent que des données collectées à certaines fins soient soumises à des traitements nécessaires à d'autres fins*

L'article 5 du règlement européen n'interdit pas que les données collectées soient traitées ultérieurement à une fin autre que celle qui a justifié leur collecte ; il exige cependant que le traitement ultérieur ne soit pas « *incompatible* » avec cette fin initiale. Il définit quatre catégories de traitements considérés comme compatibles avec les finalités initiales d'une collecte de données personnelles.

Ces catégories fondent quatre exceptions – une exception d'archivage d'intérêt public et trois exceptions d'exploitation savante : la recherche scientifique, la recherche historique et la statistique – au principe de limitation de la conservation des données posé par l'alinéa *e* de l'article 5. Celui-ci stipule que

les données à caractère personnel doivent être « *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*) ».

Ces quatre exceptions sont exprimées dans des termes analogues par l'article 9 du règlement. Cet article ne rappelle pas l'interdiction de traiter les données d'une manière incompatible avec les finalités initialement déclarées, peut-être parce que cette interdiction particulière serait incluses dans l'interdiction générale de traitement dont il fait un principe.

Selon l'alinéa *j* de l'article 9, le traitement portant sur des catégories particulières de données à caractère personnel n'est pas interdit lorsque « *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*. »

Ces alinéas inventent une finalité appelée archivistique alors que la finalité visée serait plutôt la conservation d'enregistrements informatiques. L'archivage d'intérêt public pourrait servir les fins de preuve juridictionnelle mentionnées par l'alinéa *f* de l'article 9 du règlement.

Il pourrait également servir d'autres fins nécessaires, partageant le même intérêt public, en particulier celle de mission de service public mentionnée par l'alinéa *e* de l'article 6 ou celle d'intérêt public important mentionnée par l'alinéa *g* de l'article 9.

Ainsi unie à d'autres finalités, l'exception d'archivage d'intérêt public – ainsi, d'ailleurs, que les trois exceptions d'exploitation savante – affaiblit la séparation de principe dressée par le règlement entre traitement initial et traitement ultérieur des données.

Elle l'affaiblit d'autant plus qu'elle n'est pas assortie de cette restriction, pourtant commune en droit public de l'archivage, qui interdit aux tiers de consulter, du vivant des personnes qu'elles concernent ou pendant plusieurs décennies après leur versement ou après le décès de l'intéressé, des archives privées ou couvertes par un secret mais soumises à une obligation de dépôt public.

***d. Le règlement n'impose pas de délai de rétention avant l'ouverture de l'archivage d'intérêt public***

L'exception d'archivage d'intérêt public prévue par le règlement européen n'exige pas que les archives soient déposées auprès d'un tiers de confiance ni qu'un délai minimal soit imposé avant l'ouverture de ces archives à la consultation des tiers. Ces mesures de protection des droits et intérêts des déposants et des personnes concernées sont renvoyées au droit de l'Union ou des États.

À titre de comparaison, l'article 6 de la loi française n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques dispose que les renseignements individuels et personnels figurant dans les questionnaires de l'INSEE « *ne peuvent, sauf décision de l'administration des archives, prise après avis du comité du secret statistique et relative à une demande effectuée à des fins de statistique publique ou de recherche scientifique ou historique, faire l'objet d'aucune communication de la part du service dépositaire avant l'expiration d'un délai de soixante-quinze ans suivant la date de réalisation de l'enquête ou d'un délai de vingt-cinq ans à compter de la date du décès de l'intéressé, si ce dernier délai est plus bref.* »

Dans sa réponse écrite aux questions du rapporteur, M. Kamel Gadouche, directeur du Centre d'accès sécurisé aux données (CASD) du groupe des écoles nationales d'économie et statistiques rappelle que « *Jusqu'en 2008, la loi du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques interdisait toute communication de "renseignements individuels* […] *ayant trait à la vie personnelle et familiale et d'une manière générale, aux faits et comportement d'ordre privé". Les chercheurs et datascientists étrangers aux services statistiques de l'État ne pouvaient donc pas accéder à des informations confidentielles issues des enquêtes ou des documents administratifs relatifs aux individus et aux ménages. En juillet 2008, la loi dite "des archives" a modifié la loi de 1951 (loi 51-711) pour autoriser l'accès aux données confidentielles relatives aux individus et aux ménages sous réserve d'une "décision de l'administration des archives, prise après avis du comité du secret statistique et relative à une demande effectuée à des fins de statistique publique ou de recherche scientifique ou historique" ».

De la même façon, le 2° du paragraphe I de l'article L. 213-2 du code du patrimoine prévoit que les archives publiques ne sont communicables de plein droit qu'à l'expiration d'un délai de « *vingt-cinq ans à compter de la date du décès de l'intéressé, pour les documents dont la communication porte atteinte au secret médical. Si la date du décès n'est pas connue, le délai est de cent vingt ans à compter de la date de naissance de la personne en cause* ».

Enfin, l'article 30 du décret n° 2016-1872 du 26 décembre 2016 prévoit que les dossiers, rapports, délibérations et avis sont conservés par le CEREES « *pour les recherches, les études et les évaluations dans le domaine de la santé*

*dans des conditions assurant leur confidentialité, pendant une durée maximale de dix ans, avant leur versement aux Archives nationales.* »

***e. L'alinéa qui autorise les traitements savants ultérieurs sans consentement ne les définit pas, les limite peu et prête à interprétation***

Les alinéas des articles 5 et 9 qui autorisent un archivage d'intérêt public, sans le consentement des personnes concernées, autorisent aussi le traitement de données personnelles à d'autres fins que celles pour lesquelles elles ont été collectées. Ce traitement ultérieur peut servir trois finalités distinctes, qui ne sont définies ni par le règlement, ni par ses considérants 156 à 163 :

– la recherche scientifique ;

– la recherche historique ;

– la statistique.

Les traitements nécessaires à ces finalités sont admis sur des données en cours de traitement, auprès de l'opérateur de leur collecte initiale. Ils sont aussi admis sur les dépôts d'archives autorisés par les mêmes alinéas.

Le règlement ne prévoit ni n'exige l'accord du dépositaire ou du déposant et renvoie, comme pour l'exception archivistique d'intérêt public, au droit des États ou de l'Union le soin de sauvegarder, par des mesures appropriées, les droits fondamentaux et les intérêts des personnes concernées.

En définitive, le règlement fait de la recherche scientifique et historique comme de l'exploitation statistique des données personnelles un droit supérieur à celui du dépositaire des données et des personnes qu'elles concernent, puisqu'il peut s'exercer sans leur accord. Un traitement scientifique, historique ou statistique pourrait même s'exercer sans avoir à justifier l'intérêt public requis pour rendre obligatoire l'archivage des données, ensuite soumises au traitement.

***f. Le chapitre IX du règlement admet encore d'autres exceptions***

Ces exceptions fragilisent le montage juridique élevé par le règlement pour protéger les droits et intérêts des personnes physiques contre l'exploitation, sans leur consentement, de données informatiques qui les concernent.

Elles permettent en effet au dépositaire des données de les conserver autant qu'il lui plaît dès lors qu'il allègue un intérêt public, sachant qu'un intérêt de recherche ou de statistique futur et indéfini pourrait en tenir lieu.

Bien sûr, le règlement européen exige que cette exception soit permise par le droit de l'Union ou d'un État membre, qu'elle soit proportionnée à l'objectif poursuivi, qu'elle respecte l'essence du droit à la protection des données et qu'elle prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

Mais cette protection ne s'étend pas aux intérêts des personnes morales ni aux intérêts collectifs des personnes physiques, même lorsqu'elles sont réidentifiées par des caractéristiques communes qui réclament, selon l'article 9, une vigilance particulière des autorités de contrôle.

Aux exceptions précitées s'ajoute celle de traitement journalistique, évoquée plutôt que définie par le chapitre IX du règlement et laissée à l'appréciation des États.

L'article 85 stipule que « *Les États membres concilient, par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire*. » Pour ce traitement, « *les États membres prévoient des exemptions ou des dérogations* » aux dispositions des chapitres précédents, y compris le chapitre II (principes) et le chapitre III (droits de la personne concernée), si elles sont « *nécessaires pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information* ».

On notera que les traitements à des fins d'expression universitaire sont distingués des traitements à des fins de recherche scientifique ou historique. De la même façon, indépendamment des traitements à des fins archivistiques d'intérêt public, l'article 86 stipule que « *Les données à caractère personnel figurant dans des documents officiels détenus par une autorité publique ou par un organisme public ou un organisme privé pour l'exécution d'une mission d'intérêt public peuvent être communiquées par ladite autorité ou ledit organisme conformément au droit de l'Union ou au droit de l'État membre auquel est soumis l'autorité publique ou l'organisme public, afin de concilier le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel au titre du présent règlement.* »

L'article 89 précise les garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Il exige des protections techniques et organisationnelles des droits et intérêts des personnes concernées et veut les protéger par la minimisation des données traitées et par la pseudonymisation de ces données. Pour que ces protections opèrent, il faut que les intéressés soient informés des dépôts de données qui les concernent et des traitements mis en œuvre.

Or, comme indiqué précédemment, l'article 14 du règlement dispense l'opérateur d'un traitement, en particulier pour des fins archivistiques dans l'intérêt public, statistiques ou de recherche scientifique ou historique, d'informer individuellement les personnes concernées lorsque cette information exigerait des efforts disproportionnés ou compromettrait gravement le traitement.

La pseudonymisation censée protéger les personnes contre le ciblage ou le risque de réidentification devient alors un obstacle à leur information, surtout si l'opérateur estime qu'elle inciterait les personnes concernées à s'opposer au traitement qu'il envisage, pour protéger leurs intérêts individuels ou collectifs.

L'article 14 lui enjoint alors de substituer à l'information individuelle des personnes concernées la publication des informations qu'il cite, qui décrivent le traitement et garantissent qu'il soit équitable et transparent.

Cette publicité, étendue aux résultats du traitement, pourrait causer un préjudice aux personnes concernées, qui ne pourront que demander, *ex post*, la sanction administrative par l'autorité de contrôle, nantie par l'article 83 d'amendes dissuasives, de l'abus éventuellement commis – à moins qu'elle ne l'ait autorisé –, une indemnisation conventionnelle ou juridictionnelle du préjudice subi, voire une sanction pénale.

### 2. L'article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé offre un cas exemplaire d'interprétation de ce règlement

L'article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé met le règlement européen à l'épreuve d'une interprétation qui soutient qu'une liberté publique d'exploitation d'archives publiques de données personnelles de santé peut s'affranchir des distinctions que le règlement européen fait entre plusieurs finalités de traitement licite de ces données.

En effet, l'article L. 1460-1 érige en liberté publique la consultation des archives de santé collectées auprès des services ou des établissements publics de l'État, des collectivités territoriales ou des organismes de sécurité sociale, mais cette liberté publique ne s'accorde pas aisément au règlement européen.

#### *a. L'archivage public de données personnelles de santé est rendu obligatoire dans un but d'intérêt public*

La loi de modernisation de notre système de santé a été promulguée avant le règlement européen. À la différence de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, son article 193 n'interdit pas, par principe, le traitement des données personnelles de santé. Au contraire, il insère, dans le code de la santé publique, la déclaration d'une liberté publique d'accéder aux archives des données recueillies à titre obligatoire par des personnes publiques. Cette déclaration figure dans un article codifié qui n'était pas dans le projet de loi déposé le 15 octobre 2014 [(1)]. L'article a été ajouté par un amendement du Gouvernement, adopté par la commission des affaires sociales lors de la première lecture du texte à l'Assemblée nationale [(2)].

---

*(1) Article 47 du projet de loi (http://www.assemblee-nationale.fr/14/projets/pl2302.asp).*

*(2) Voir http://www.assemblee-nationale.fr/14/amendements/2302/CION-SOC/AS1373.asp.*

L'amendement greffe d'un chapitre préliminaire de « *Principes relatifs à la mise à disposition des données de santé* » les dispositions législatives insérées dans un titre VI nouveau du livre IV « Administration générale de la santé » du code de la santé publique.

Ce chapitre préliminaire ne contient que l'article L. 1460-1, structuré en deux alinéas. Le premier autorise le traitement informatique, à des fins « *de recherche, d'étude ou d'évaluation présentant un caractère d'intérêt public* », des « *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* ».

Cet alinéa interdit les traitements qui peuvent avoir pour objet ou pour effet de porter atteinte à la vie privée des personnes concernées. Il précise que, sauf disposition législative contraire, ces traitements ne doivent en aucun cas avoir pour fin l'identification directe ou indirecte de ces personnes. Les traitements d'intérêt public ne sont autorisés que dans le respect des garanties posées par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le second alinéa ajoute que « *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.* » Ce droit d'accès – qui inclut de façon implicite un droit d'exploiter – oblige à conserver les données dans un système d'archivage.

Au cours de son audition, M. Christian Babusiaux, ancien président de l'IDS, s'est interrogé sur « *la compatibilité de la distinction qui est faite entre les organismes selon leur nature – publique ou privée – avec les textes européens en matière de concurrence. Dans un arrêt du 20 mai 2016, le Conseil d'État a d'ailleurs jugé que l'une des dispositions de l'arrêté de 2013 relatif aux modalités d'accès SNIIRAM provoquait une distorsion entre organismes publics et privés. Je ne veux pas surestimer la dimension européenne, mais le risque de recours peut exister.*

« *Se pose également la question de l'accès d'opérateurs provenant d'autres pays de l'Union européenne aux données. À titre personnel, j'estime que, pour agir en matière de santé, les bases de données nationales ne suffisent pas car les échantillons sont trop petits – quelques centaines de personnes dans le cas de maladies rares, par exemple.*

« *Il serait donc utile de réunir des données sinon européennes, au moins de plusieurs pays de l'Union pour étoffer les bases dans certains domaines. Cela suppose d'ouvrir l'accès aux bases à des opérateurs non français, et donc de revoir la philosophie et l'articulation du processus.* » (1)

***b. Cet intérêt public serait celui d'une démocratie sanitaire transparente***

i. La liberté publique instaurée semble s'inspirer d'une version préparatoire du règlement européen, et non de sa version définitive

Le rapporteur note tout d'abord que l'article 193 de la loi du 26 janvier 2016 semble s'inspirer d'une version préparatoire du règlement. Le texte de la proposition de règlement présentée par la Commission européenne en janvier 2012 autorisait le traitement des données relatives à la santé lorsque ce traitement est nécessaire à des fins liées à la santé (2) ou pour l'exécution d'une mission effectuée dans l'intérêt général.

Ces deux exceptions figuraient encore dans la version adoptée par le Parlement européen (3) mais ont disparu de celle adoptée par le Conseil européen en navette et de la version définitive de l'article 9 (4) : l'exception liée à la santé a été divisée en deux, l'une pour la médecine du travail et la médecine préventive (cas *h*), l'autre pour la santé publique (cas *i*) ; l'exception de mission effectuée dans l'intérêt général a été remplacée par celle de motif d'intérêt public important (cas *g*) ; le droit de la sécurité sociale et de la protection sociale a été ajouté à l'exception relative au droit du travail (cas *b*).

La loi française n'a pas suivi les péripéties de ce texte. Parmi les données ouvertes à la consultation publique, l'article L. 1460-1 ne sépare pas celles qui ont été collectées au titre d'une convention de droit privé, par exemple d'assurance maladie, avec le consentement des personnes concernées, et celles qui ont été collectées au titre d'une mission de service public, sans ce consentement.

ii. Le critère de l'intérêt public est inspiré à la loi française comme au règlement européen par une jurisprudence du droit à l'information

La liberté publique instaurée par l'article L. 1460-1 peut correspondre à une interprétation des finalités de traitement de données déclarées licites par le règlement européen qui réunirait leurs intérêts public et savant pour justifier l'ouverture immédiate des archives publiques de données de santé à une recherche méthodique visant à verser des preuves scientifiques ou documentées au débat public requis par une démocratie sanitaire.

---

*(1) Audition du 17 janvier 2017.*

*(2) Cf le h) du 2 de l'article 9 de la proposition au Parlement européen et au Conseil du 25 janvier 2012 (http://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1484574349985&uri=CELEX:52012PC0011).*

*(3) Voir http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT%20TA%20P7-TA-2014-0212%200%20DOC%20XML%20V0//fr.*

*(4) Voir http://eur-lex.europa.eu/procedure/FR/2012_11?qid=1484578052643&rid=13.*

L'intérêt public allégué vient de la jurisprudence du droit à l'information du public dans une société démocratique. Dans cette jurisprudence, il justifie une enquête de journalisme, les révélations d'un lanceur d'alerte ou une publication.

Cet intérêt justifierait de porter atteinte aux droits fondamentaux et aux intérêts des personnes concernées par des archives publiques de données de santé, en permettant la communication et l'exploitation de ces archives, par analogie avec l'atteinte licite portée par une publication de presse aux droits et intérêts des personnes physiques et morales que cette publication évoque.

Toutefois, à la différence du droit des publications, ni le règlement européen sur la protection des données personnes, ni les lois françaises de 1978 ou de 2016 sur l'archivage obligatoire et l'exploitation publique des données de santé ne protègent les droits et intérêts des personnes morales dont les personnes physiques concernées sont membres ou ceux des groupes sociaux qu'elles composent. En l'absence d'une protection suffisante de leurs intérêts, personnels ou collectifs, les intéressés pourraient alors être incités à rompre les conventions qui les lient aux opérateurs de collecte ou de traitement initial de leurs données pour s'opposer à leur traitement ultérieur ou conclure avec ces opérateurs des conventions qui excluent la cession des données à des tiers.

Le rapporteur a interrogé les représentants de l'Institut des données de santé dans les termes suivants : « *L'accès élargi aux données de santé, dans la transparence, est voulu pour améliorer la démocratie sanitaire. Outre que les associations de patients aspirent légitimement à avoir accès à certaines informations, les médias s'en servent pour classer les établissements de santé. Ne faut-il pas s'assurer que l'accès aux données anonymisées est fondé sur des critères incontestables, non pour restreindre l'accès à ces informations mais pour être certain de leur qualité et éviter qu'elles ne soient manipulées ?* »

Mme Chantal Cases a répondu : « *Ces questions ont été longuement débattues par la commission dite "open data" à laquelle je participais lorsque je dirigeais l'Institut national d'études démographiques (INED). Dans la recherche, il y a du bon et du mauvais, et l'évaluation est fondée sur la contre-expertise. Nous soutenions le principe de l'ouverture des données, considérant que le fait qu'un grand nombre d'usagers potentiels puissent les utiliser est la meilleure garantie que se forgent des analyses soumises à contre-expertise.*

« *La loi implique la transparence des méthodes et des résultats ; c'est exactement ce qui vaut dans la recherche et ce modèle nous semble être le bon. Certaines études seront peut-être meilleures que d'autres, mais elles pourront être contestées parce qu'il faudra faire savoir comment elles ont été conduites.*

« *La contre-expertise se construit collectivement. C'est le pari de l'ouverture de la consultation des données : on ne pourra plus fonctionner sur des on-dit, des analyses opposables pourront être réalisées, des discussions techniques sur la manière de traiter les données et de les interpréter seront*

*possibles, et c'est la meilleure garantie contre les éventuelles déviances du système. On ne peut empêcher l'accès à des données au motif qu'elles risquent d'être utilisées de manière à en donner une interprétation inappropriée. C'est la clef du choix qui a été fait.* »

iii. L'intérêt public justifiant l'ouverture des archives publiques de données de santé serait celui d'une démocratie sanitaire transparente

L'articulation entre ouverture des données de santé et démocratie sanitaire a été particulièrement explicitée par le rapport de la commission open data en santé, notamment dans sa section 2.1 :

« *Le premier enjeu est de permettre aux citoyens de peser davantage sur les orientations du système de santé, en fondant leurs contributions sur une connaissance renforcée de son fonctionnement. L'accès aux données qui supportent la décision publique constitue une condition nécessaire pour permettre une participation active des parties prenantes aux instances de la démocratie sanitaire.*

« *Ainsi que le souligne le rapport de Pierre-Louis Bras, les données de santé peuvent par exemple servir à documenter des inégalités territoriales de santé ou d'offres de services aussi bien que les pratiques de dépassement d'honoraires. Ces accès constituent aussi un outil de transparence en permettant aux parties prenantes de construire leurs propres évaluations des politiques publiques.*

« *Parties prenantes du dialogue dans le cadre de la démocratie sanitaire, les professionnels et les établissements de santé, par le biais des organisations qui les représentent, doivent pouvoir également accéder aux données les concernant collectivement.*

« *Les associations de patients et d'usagers du système de santé mettent aussi en avant la possibilité de jouer leur rôle de lanceur d'alerte, par exemple sur les questions de sécurité sanitaire, ou encore la possibilité d'aider plus efficacement leurs adhérents en matière d'accès à l'assurance en leur garantissant notamment que les éventuelles exclusions ou surprimes seront évaluées au regard des données actualisées de survie et d'invalidité les concernant.*

« *Enfin, l'accès aux données permet de construire un partage des connaissances entre acteurs du système de santé (Assurance maladie obligatoire, organismes complémentaires et offreurs de soins) et représentants des usagers fondé sur une base d'informations commune qui servira donc de référence et facilitera le dialogue entre les parties prenantes. Ce partage des connaissances est indispensable pour le débat démocratique, l'évaluation de la réponse aux*

*besoins de santé et la recherche collective d'une plus grande efficience de notre système de santé.* » (1)

Le rapport a également posé une doctrine de l'open data en santé :

« *L'ouverture des données de santé anonymes vise quatre objectifs stratégiques : contribuer à la démocratie sanitaire, permettre l'autonomisation du patient, renforcer l'efficacité de l'action publique et stimuler la croissance et l'innovation.*

« *Pour atteindre ces objectifs, l'ouverture des données anonymes de santé au public doit suivre les principes généraux suivants, en cohérence avec la loi CADA, la directive européenne* Public Sector Information *et la politique du gouvernement rappelée dans la première partie du rapport :*

« ● *L'ouverture de toutes les données anonymes relatives à la santé et au système de santé français doit être organisée, sans préjuger de l'utilisation qui sera faite de ces données ;*

« ● *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. Si les données granulaires ne sont pas anonymes, ou sont protégées par un secret prévu par la loi (ex : secret industriel et commercial, secret statistique), l'ouverture des données agrégées doit être organisée (dans la mesure des capacités des organisations à produire ces agrégats s'ils n'existent pas déjà) ;*

« ● *Les enquêtes et recherches menées sur fonds publics devront dès leur conception prévoir l'ouverture des données granulaires ou anonymisées.* » (2)

iv. Le consultant des archives publiques de données de santé est contraint de publier le résultat de ses recherches

Dans une démocratie qui ne serait plus seulement politique mais aussi sanitaire, les principes de transparence et de droit à l'information justifient le versement obligatoire de données personnelles, publiques ou privées, attestant l'exécution de conventions d'assurance maladie ou de protection sociale ou celle d'une politique de santé publique, à un système national d'archives publiques, sous secret professionnel.

La démocratie sanitaire aurait pu privilégier l'exploitation des données personnelles de santé par les seules personnes morales à but non lucratif qui en sont dépositaires, dans l'intérêt de leurs membres et anciens membres, comme le prévoit l'alinéa *d* de l'article 9 du règlement européen. Un débat interne aux ordres

*(1) Commission open data en santé,* op. cit., *pages 37 et 38.*

*(2) Commission open data en santé,* op. cit., *page 44.*

professionnels, aux organismes de soins et aux organismes de sécurité sociale aurait limité le débat public aux scandales sanitaires. L'ouverture à des tiers des archives de leurs travaux et de leurs débats pouvait alors être restreinte aux procédures juridictionnelles engagées à la suite de ces scandales.

Ce n'est pas la logique retenue par la loi du 26 janvier 2016.

En contrepartie du fait qu'il est dispensé de recueillir le consentement des personnes concernées, deux alinéas du paragraphe II de l'article L. 1461-3 du code de la santé publique subordonnent l'accès du consultant aux archives publiques :

« *b) A 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.* »

Cette disposition légale instaure une obligation de publication des résultats de toute recherche savante autorisée, sous contrôle d'un tiers évaluant leur validité, en confondant dans une même procédure le débat démocratique, le débat public, le débat scientifique, académique ou universitaire ou le débat d'experts judiciaires et les preuves journalistique, scientifique, historique et d'expertise juridictionnelle versées à ces débats, que le règlement européen distingue encore.

Dans sa réponse à une question écrite du rapporteur, la DREES explique effectivement que « *l'ouverture permettra également la contradiction raisonnée et factuelle de ce type de publication. Rappelons que l'article L. 1461-3 du code de la santé publique prévoit la publication des méthodes, des résultats des études et des moyens d'en évaluer la validité.* »

Au cours de son audition, le docteur Jean-Claude Desenclos a confirmé l'intérêt majeur qui s'attache à la publication des résultats de toute étude réalisée par traitement des données personnelles de santé : « *cela devrait se faire à l'anglo-saxonne, c'est-à-dire dans un cadre où chaque opérateur, public ou privé, a l'obligation de publier le résultat de ses travaux afin qu'ils puissent être vérifiés. Au Royaume-Uni, ces obligations font partie de l'organisation générale de la* General Practice Research Database, *dont l'utilisation est transparente, les résultats obtenus devant tous être publiés et pas uniquement ceux qui sont favorables à l'opérateur ou au commanditaire de l'opérateur. Il s'agit là de bonnes pratiques, qui, à ce jour, n'ont pas été explicitement intégrées dans nos dispositifs.* » [(1)]

*(1) Audition du 31 janvier 2017.*

L'INDS agirait donc à la manière du comité de lecture d'une revue savante ou scientifique sans toutefois pouvoir s'opposer à la publication d'un article de résultats d'exploitation du SNDS.

Cette publication serait de droit public, voire d'ordre public puisqu'elle conditionne le droit de sonder le SNDS susceptible d'être accordé à tous ceux qui ne disposent pas d'un accès permanent.

*In fine,* le critère de l'intérêt public connaît un certain « glissement » : il fondait jusqu'ici seulement la justification d'un traitement informatique de données personnelles de santé archivées ; il fonde désormais aussi la justification de la publication obligatoire du résultat de ce traitement ; cela fait basculer cette publication dans le domaine du droit des publications, auquel le critère a été emprunté, voire dans celui des publications judiciaires.

Mais en droit des publications, un auteur ou un journaliste ne peuvent être contraints à publier l'un le résultat de sa réflexion, l'autre celui de ses enquêtes. Le journaliste peut aussi invoquer son droit au secret de ses sources, l'auteur d'une publication son droit au silence.

Le glissement du droit de l'informatique au droit de l'information publique et à celui des publications n'est pas explicite dans le règlement européen mais seulement suggéré par le critère de l'intérêt public et la prudence des dispositions du chapitre IX du règlement. Le glissement est cependant manifeste dans la loi française du 26 janvier 2016.

Si un droit à l'information peut justifier l'exploitation d'archives publiques obligatoires, la sauvegarde des droits fondamentaux et des intérêts des personnes physiques concernées se trouve réduite à l'interdiction de la publication ou à l'indemnisation du préjudice causé par elle.

Certes, la loi française soumet les traitements à des fins de recherche publique à l'autorisation de la CNIL, mais c'est à l'INDS d'apprécier le résultat de cette recherche. Il y aurait donc deux autorités de contrôle, voire trois si l'intérêt public est celui d'une preuve scientifique livrée à l'appréciation du CEREES (voir page 27).

### *c. L'intérêt public invoqué par la loi française recouvre néanmoins plusieurs des « intérêts publics » distingués par l'article 9 du règlement européen*

L'article L. 1460-1 limite l'exercice de la liberté publique qu'il instaure en exigeant qu'il soit motivé par un intérêt public. Celui-ci ne correspond ni au « motif d'intérêt public important » de l'alinéa *g* de l'article 9 du règlement européen, ni aux « motifs d'intérêt public » de l'alinéa *i du même article*, qui sont assortis d'une exigence de sauvegarde des droits fondamentaux, libertés et intérêts des personnes concernées, par exemple par le secret professionnel.

Le motif d'intérêt public requis dans le cas *j* de l'article 9 du règlement européen ne l'est que pour collecter des données à des fins archivistiques. À la différence de l'article L. 1460-1, il n'est pas exigé pour les traitements à des fins de recherche scientifique ou historique, à des fins statistiques. Il n'est pas non plus mentionné pour les finalités journalistiques ou universitaires prévues par le chapitre IX du règlement européen mais renvoyées au droit des États.

Un motif d'intérêt public pourrait bien sûr être exigé par un État pour restreindre les traitements admis par l'article 9 du règlement européen en matière de droit du travail, de la sécurité sociale ou de la protection sociales (cas *b*) comme en matière médicale, sanitaire ou sociale (cas *h*).

M. Édouard Geffray a toutefois estimé que « *S'agissant, tout d'abord, du règlement européen, celui-ci permet le traitement des données du SNDS, notamment parce que son article 9 prévoit, comme je le disais, des exceptions pour les traitements apparaissant comme nécessaires pour des motifs d'intérêt public, intérêt public qui doit être important de manière générale.*

« *En ce qui concerne la santé publique, ces motifs comprennent notamment la protection contre les menaces transfrontalières graves pesant sur la santé et l'objectif de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux. Une troisième exception est prévue pour le traitement nécessaire dans l'intérêt public à des fins de recherche scientifique.*

« *L'ensemble de ces dispositions font donc référence à l'intérêt public, lequel est par ailleurs la "clé d'entrée" du SNDS pour les organismes qui n'y ont pas accès de plein droit. Aussi les deux réglementations coïncident-elles, de sorte que le traitement des données de santé est possible dans le cadre du règlement européen sans prendre de risques juridiques excessifs.*

« *Je vais vous livrer un sentiment, plutôt qu'une analyse juridique. Le règlement européen est, dans son principe, restrictif, mais il admet – ce qui est du reste conforme à notre cadre interne – que, dans l'intérêt public, des exceptions puissent être prévues à ces interdictions de principe, exceptions dont les conditions particulières doivent être fixées par les États membres. Or, la condition de la confidentialité des données est définie par la loi, laquelle vise précisément à aménager des dérogations lorsque l'intérêt public le justifie.*

« *Il me semble donc que le règlement européen ne remet pas en cause l'équilibre tel qu'il a été défini par le législateur, qui autorise la réutilisation des données de santé, premièrement, dans un objectif d'intérêt public, deuxièmement, dans des conditions fixées par la CNIL : agrégats, anonymisation éventuelle, non-réidentification des personnes… Il faut bien avoir à l'esprit cette double condition.* » (1)

*(1) Audition du 17 janvier 2017.*

Dans sa réponse écrite aux questions du rapporteur, la DREES indique que « *l'IDS a fait appel à un cabinet d'avocats pour définir ce concept d'intérêt public de façon à poser les bases d'une doctrine en la matière.* »

### *d. Les dispositions de l'article L. 1460-1 ne coïncident pas exactement avec les stipulations du règlement européen*

i. L'article L. 1460-1 n'exige pas le secret professionnel imposé à des traitements licites par le règlement et mentionné à l'article L. 1461-1

Dans le cas *h* [(1)], le règlement européen exige que le traitement soit opéré « *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.* »

Ce cas reprend celui prévu par l'alinéa 3 de l'article 8 [(2)] de la directive européenne 95/46/CE du 24 octobre 1995, en vigueur jusqu'en 2018. Il peut expliquer que le 2° du IV de l'article L. 1461-1 [(3)] exige que les responsables du traitement des données du SNDS soient soumis à un secret professionnel, ce qui restreint considérablement le champ de la liberté publique posée par l'article L. 1460-1 et par la loi de 1978, qui n'exigent pas ce secret.

Mais l'article 55 de la loi de 1978 dispose que « *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* ».

Le rapprochement des textes législatifs laisse donc planer une incertitude sur le fait que la consultation du SNDS serait ou non soumise au secret. Dans une réponse écrite à une question posée par le rapporteur, la CNIL confirme que :

« ● *le secret médical est d'ordre public ;*

---

*(1) « 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 ; ».*

*(2) « Le paragraphe 1 ne s'applique pas lorsque le traitement des données est nécessaire 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 que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente. »*
*(http://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1484911606040&uri=CELEX:31995L0046)*

*(3) « 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 ; ».*

« ● *les cas de dérogation doivent être expressément prévus par la loi. L'article L. 1461-1 du code de la santé publique rappelle que les responsables des traitements, les personnes en charge de leur mise en œuvre et les personnes accédant au SNDS sont soumises au secret professionnel ;*

« ● *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.* »

On peut en déduire que les données du SNDS ne sont pas des informations publiques au sens des articles L. 322-1 et suivants du code des relations entre le public et les administrations. Elles ont un caractère personnel qui soumet leur communication à la loi de 1978 et non à ce code, comme le précise l'article L. 322-2, à moins que ce caractère leur soit ôté par un procédé d'anonymisation. En outre, leur consultation serait soumise au secret, soit médical, soit professionnel.

ii. L'article L. 1460-1 n'exige pas des recherches qu'il autorise qu'elles soient scientifiques ou historiques

L'article L. 1460-1 du code de la santé publique n'exige pas que la recherche qu'il autorise sur les archives publiques de données de santé soit scientifique ou historique. Cette absence de qualification par le droit national ouvre la voie aux consultations à toutes les fins admises par l'article 9 comme à celles prévues par le chapitre IX du règlement.

Ces recherches pourraient être soustraites aux méthodes disciplinaires propres à la recherche scientifique si la loi de n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ne rétablissait celles-ci en préalable à l'accès au SNDS, sous couvert :

– de l'alinéa a) du 2° du paragraphe II de l'article L. 1461-3 selon lequel l'accès aux données est subordonné à la communication, par le demandeur, d'un protocole d'analyse, précisant notamment les moyens d'évaluer la validité et les résultats de ce protocole, voire du traitement envisagé ;

– de l'alinéa *g* de l'article 11 de la loi de 1978 qui autorise la CNIL à « *certifier ou homologuer et publier des référentiels ou des méthodologies générales aux fins de certification de la conformité à la présente loi de processus d'anonymisation des données à caractère personnel, notamment en vue de la réutilisation d'informations publiques mises en ligne dans les conditions prévues au titre II du livre III du code des relations entre le public et l'administration* » ;

– du paragraphe IV de l'article 4 de la loi de 1978, selon lequel « *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.* »

L'article L. 1460-1 soustrait de la même façon les consultations qu'il autorise aux hiérarchies collégiales, propres à la discipline universitaire, dont l'article 85 du règlement européen ne fait qu'un mode d'expression. Mais l'articulation administrative des contrôles des traitements et de leurs résultats par la CNIL, le CEREES et l'INDS pourrait s'apparenter à celui d'une hiérarchie collégiale.

L'article L. 1460-1 ajoute « *l'étude* » aux finalités de recherche ouvrant l'accès au SNDS, alors qu'elle ne semble pas avoir d'autre définition juridique que celle des « bureaux » qui en seraient chargés par l'article L. 1460-3 du code de la santé publique, afin de soustraire la recherche aux intérêts des laboratoires pharmaceutiques et de l'industrie du médicament et des appareils médicaux, qui assurent le principal de la recherche en produits de santé, en leur imposant la médiation d'un tiers, plus sensible à l'intérêt public.

L'article L. 1460-1 est d'ailleurs plus restrictif encore que le paragraphe II de l'article L. 1461-3 qui encadre l'accès de ces organismes au SNDS puisqu'il ne vise que les organismes « *réalisant des recherches, des études ou des évaluations à des fins de santé publique* » et non à des fins médicales ou de santé.

M. Franck Von Lennep, directeur de la DREES, a indiqué que le ministère publiera un arrêté définissant les critères d'homologation de ces bureaux d'études, qui ne seraient pour le moment définis que par la convention collective nationale des bureaux d'études techniques, des cabinets d'ingénieurs-conseils et des sociétés de conseils [(1)].

L'article L. 1460-1 ajoute aussi « *l'évaluation* » aux finalités légales de consultation des archives publiques de données de santé. Ce terme ne figure dans le règlement européen que pour l'appréciation des traitements de données.

Cette évaluation pourrait servir les finalités qui garantissent « *des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux* », admises par l'alinéa *i* de l'article 9 du règlement européen, mais les traitements nécessaires ne peuvent alors être opérés que sous l'équivalent du secret professionnel recommandé par cet alinéa.

*(1) Audition du 20 décembre 2016.*

iii. L'article L. 1460-1 ne mentionne pas l'exploitation statistique des archives publiques qu'il ouvre à la consultation immédiate

L'article L. 1460-1 du code de la santé publique ne mentionne pas les fins statistiques distinguées par le règlement européen. Elles n'apparaissent qu'à titre de moyen, dans l'article L. 1461-2. Les poser comme fins aurait peut-être soumis le SNDS à la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques.

Cette finalité aurait alors confié l'appréciation des motifs de consultation anticipée des archives publiques de données de santé au comité du secret statistique établi par le décret n° 2009-318 du 20 mars 2009 plutôt qu'à la CNIL.

### 3. Le SNDS inaugure une liberté publique à finalités restreintes, instaurée par l'article L. 1460-1

L'article L. 1460-1 du code de la santé publique vise non le SNDS mais 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* ».

Le paragraphe I de l'article L. 1461-1 qui crée le SNDS dit qu'il rassemble et met à disposition cinq catégories de données. Il ne dit pas explicitement qu'il les archive, ni qu'il se substitue à leur dépôt précédent.

Chacune des cinq sources du SNDS forme un cas particulier qui a son propre régime de dépôt, de traitement et d'ouverture à la consultation publique. Ce régime combine les dispositions législatives du titre VI du livre IV de la première partie du code de la santé publique et celles de la loi de 1978 aux dispositions propres au dépôt légal des données rassemblées.

#### *a. Le SNDS serait une archive des dépôts légaux imposés aux données de l'assurance maladie obligatoire et des causes de décès*

Avant 2016, les organismes qui géraient un régime de base d'assurance maladie étaient soumis, par l'article L. 161-28-1 du code de la sécurité sociale, à une obligation légale de dépôt, dans le SNIIRAM, de données personnelles de santé.

Cet article n'établit qu'un système national d'information inter-régimes obligatoire pour les organismes gérant un régime de base d'assurance maladie. C'est l'article L. 161-29 du même code qui impose aux professionnels de santé et à leurs établissements d'alimenter ce système en y versant, « *dans l'intérêt de la santé publique et en vue de contribuer à la maîtrise des dépenses d'assurance maladie* » le numéro de code des actes remboursables effectués, des prestations servies et des pathologies diagnostiquées.

Ce versement suppose que les professionnels soient liés par une convention à un organisme assureur de sécurité sociale. Il ne s'impose pas aux professionnels qui ne sont pas conventionnés ou aux actes qui ne sont pas remboursés. Il a donc un caractère contractuel, l'article L. 161-29 faisant de ce versement une clause obligatoire du conventionnement du professionnel ou de l'établissement par un organisme de sécurité sociale.

La réutilisation des données collectées à d'autres fins que celles de l'intérêt de la santé publique ou de la maîtrise des dépenses d'assurance maladie doit être agréée dans les conventions passées ou autorisée par la loi. Celle du 26 janvier 2016 ajoute la constitution du SNDS aux finalités du système national d'information mentionnées à l'article L. 161-28-1, qui peuvent apparaître comme une déclinaison restrictive de la finalité générale posée par l'article L. 161-29.

Autorisée par la loi, cette réutilisation des données par un tiers à d'autres fins que celles prévues lors de leur collecte ne peut être empêchée par les intéressés mais ils peuvent néanmoins s'opposer, en application de l'article 56 de la loi de 1978, à ce qu'elle entraîne la levée du secret professionnel.

La loi du 26 janvier 2016 a procédé de la même façon pour faire du SNDS un dépôt d'archives des données sur les causes de décès qui sont soumises à une obligation légale d'enregistrement par l'article L. 2223-42 du code général des collectivités territoriales.

Ce faisant, le SNIIRAM et le CépiDc conservent un statut légal et des finalités propres, indépendamment du SNDS, qui autorisent des traitements dans d'autres conditions que celles prévues par le titre VI du livre IV de la première partie du code de la santé publique.

L'article L. 161-28-1 du code de la sécurité sociale autorise par exemple le traitement des données pour la connaissance des dépenses de l'ensemble des régimes d'assurance maladie par circonscription géographique, par nature de dépenses, par catégorie de professionnels responsables de ces dépenses et par professionnel ou établissement. Cette finalité permet des ciblages individuels interdits au SNDS.

Le même article autorise la consultation du SNIIRAM afin de définir, de mettre en œuvre et d'évaluer des politiques de santé publique. L'évaluation de ces politiques pourra donc s'autoriser de cet article comme du titre VI du livre IV de la première partie du code de la santé publique, peut-être dans des conditions différentes dans les deux cas.

Cependant, répondant par écrit à une question du rapporteur, la DREES assure que « *l'exploitation du SNIIRAM par les pouvoirs publics se fera via le SNDS.* »

À propos du CépiDc, M. Christian Babusiaux a déclaré que la question du registre des décès lui semblait extrêmement sensible et qu'elle soulignait l'intérêt

de maintenir une certaine différenciation entre les bases actuelles plutôt que de vouloir les fondre en une base unique : « *J'ai quelque réticence à prôner la concentration en un système unique de l'ensemble des bases de données aujourd'hui médico-administratives, auxquelles s'ajouteront demain de véritables bases de données de santé qui renseignent sur des historiques anonymisés de santé. Ne vaut-il pas mieux créer un système décentralisé permettant d'accéder à l'une ou l'autre de ses composantes ? Plus un système est centralisé, plus il est vulnérable.*

« *De ce point de vue, le registre des causes médicales de décès est particulièrement sensible – en particulier s'il s'agit de suicides d'adolescents, de décès liés à un mésusage de médicaments ou de décès liés au sida, par exemple. Toutes ces données sont assorties d'un très haut niveau de confidentialité. Il faudra donc sécuriser particulièrement de tels compartiments du SNDS.*

« *À mon sens, le registre national des causes médicales de décès aurait dû, par précaution, être maintenu en dehors du SNDS, car son usage est limité à un certain nombre de cas. Il faut en effet que les médecins aient une confiance absolue dans le mécanisme d'accès à ces données, faute de quoi ils risqueraient – ce qu'ils font d'ailleurs parfois, non sans raison – de ne pas indiquer la véritable cause de la mort sur l'acte de décès.*

« *Certes, les choses ont considérablement progressé depuis dix ans, mais il faut se garder de fragiliser ce registre, qui est un élément essentiel de l'épidémiologie. La confiance est indispensable à une épidémiologie performante. Or, les causes de décès sont un domaine crucial pour la confiance, d'où mon interrogation – mais peut-être suis-je trop rigoureux, ou trop inquiet.* »

M. Franck Von Lennep a, pour sa part, minimisé les risques associés à une trop grande intégration des bases actuelles, tout en suggérant que l'accès à la base des causes de décès pourrait voir sa spécificité préservée : « *Il sera probablement possible à l'avenir, pour les chercheurs qui en ont besoin, d'accéder directement à la base concernant les causes de décès, qui est gérée par l'Institut national de la santé et de la recherche médicale (INSERM). C'est un point mineur, dans la mesure où cette base de données est le plus souvent utilisée avec d'autres.* » [(1)]

***b. Les données des MDPH et des établissements de soins seraient archivées dans le SNDS indépendamment de leurs finalités propres***

Pour ajouter au SNDS les données des maisons départementales des personnes handicapées (MDPH), le législateur a procédé différemment : il n'a pas ajouté des finalités à leurs destinations légales, mais a fait du versement de leurs données au SNDS une obligation légale ayant ses propres fins, indépendamment de celles de leurs sources.

*(1) Audition du 20 décembre 2016.*

Le 4° du I de l'article L. 1461-1 prévoit le versement au SNDS des données médico-sociales « *du système d'information mentionné à l'article L. 247-2 du code de l'action sociale et des familles* ». Cet article L. 247-2 impose aux MDPH d'utiliser un « *système d'information commun, interopérable avec les systèmes d'information des départements, ceux de la Caisse nationale d'allocations familiales et ceux de la Caisse nationale de solidarité pour l'autonomie, dans des conditions précisées par décret.* »

L'article L. 247-2 n'imposait pas d'obligation légale de dépôt ou d'enregistrement mais seulement une obligation d'interopérabilité, alors que l'exploitation d'intérêt public mentionnée par l'article L. 1460-1 du code de la santé publique n'est permise que pour les données recueillies à titre obligatoire.

En outre, ce n'est pas la partie législative du code de l'action sociale qui fixe les finalités de ce système d'opérations communes mais sa partie réglementaire, à savoir l'article D. 247-1.

Il faut donc considérer que le versement des données des MDPH au SNDS est fondé par l'article L. 1461-1 du code de la santé publique pour les finalités prévues aux articles suivants et non pour celles mentionnées à l'article L. 1460-1 ou à l'article D. 247-1 du code de l'action sociale.

Il en va de même s'agissant des données des établissements de santé. Le 1° du I de l'article L. 1461-1 du code de la santé publique autorise l'État à se saisir des données visées à l'article L. 6113-7 du même code, par lesquelles ces établissements analysent leur activité. Les trois premiers alinéas de l'article L. 6113-7 disposent que « *Les établissements de santé, publics ou privés, procèdent à l'analyse de leur activité.*

« *Dans le respect du secret médical et des droits des malades, ils mettent en œuvre des systèmes d'information qui tiennent compte notamment des pathologies et des modes de prise en charge en vue d'améliorer la connaissance et l'évaluation de l'activité et des coûts et de favoriser l'optimisation de l'offre de soins.*

« *Les praticiens exerçant dans les établissements de santé publics et privés transmettent les données médicales nominatives nécessaires à l'analyse de l'activité et à la facturation de celle-ci au médecin responsable de l'information médicale pour l'établissement dans des conditions déterminées par voie réglementaire après consultation du Conseil national de l'ordre des médecins.* »

L'article L. 1461-1, qui organise le versement de ces données dans le SNDS, les prend donc avec leurs conditions et leurs finalités de collecte ainsi que l'exigence de secret médical imposée à leur traitement.

Le législateur aurait été plus fidèle aux dispositions de l'article L. 1460-1, qui ne vise pas les données des établissements privés, et plus conforme à l'article 9 du règlement européen s'il avait prévu que soit versée au SNDS

l'archive des données recueillies par la puissance publique en application de l'article L. 6113-8.

Certaines personnes auditionnées ont cependant expliqué que la consultation du PMSI, indépendamment du SNDS – par exemple par l'intermédiaire du CASD –, était soumise aux dispositions de la loi de 1978, en particulier au référentiel de sécurité, sans que l'on sache si c'est en application du titre VI du livre IV de la première partie du code de la santé publique et pour les finalités autorisées par ce titre, ou de la seule autorité de la loi de 1978 et pour les finalités qu'elle autorise, finalités qui, dans les deux cas, s'imposeraient à celles de l'article L. 6113-7.

M. Franck von Lennep a confirmé qu'« *il sera possible d'avoir accès aux données du SNDS directement, mais il sera également possible d'avoir accès aux différentes bases qui le constituent, en particulier le programme de médicalisation des systèmes d'information (PMSI).*

« *Aujourd'hui, les accès au PMSI – ce qui suffit à certains utilisateurs – sont organisés par l'Agence technique de l'information sur l'hospitalisation (ATIH), selon des modalités diverses : il est possible d'y accéder directement, ou par l'intermédiaire du centre d'accès sécurisé distant aux données (CASD) du Groupe des écoles nationales d'économie et de statistique (GENES).*

« *Ces accès aux données du PMSI se font aujourd'hui dans l'esprit du nouveau référentiel, avec notamment une traçabilité des accès à distance – le ministère de la santé a mis fin depuis l'année dernière à la distribution du PMSI sous forme de CD-ROM.* »

M. Philippe Burnel a souligné à ce propos que l'alignement du régime d'accès du PMSI sur celui du SNDS n'est pas exempt d'effets secondaires : « *La loi a redéfini le SNDS en réunissant dans un même ensemble les données PMSI et SNIIRAM et en en fixant des règles d'accès identiques. De ce fait, en même temps que l'accès devenait ouvert à plus d'acteurs, les conditions en étaient durcies, ce qui a compliqué les choses pour ceux qui utilisaient le PMSI avant la loi de janvier 2016.* » (1)

### *c. Le versement des archives de l'assurance maladie complémentaire serait une obligation plus conventionnelle que légale*

L'obligation faite aux assureurs complémentaires par le 5° du paragraphe I de l'article L. 1461-1 du code de la santé publique de verser au SNDS un échantillon des données qu'ils collectent n'a pas la même nature que les dépôts légaux précédents.

L'article L. 1460-1 du code de la santé publique autorise le traitement de données recueillies à titre obligatoire par les personnes publiques et les

*(1) Audition du 13 décembre 2016.*

organismes de sécurité sociale, sans préciser si cette obligation est légale ou conventionnelle et si les assureurs complémentaires sont des organismes de sécurité sociale.

Le 5° du I de l'article L. 1461-1 oblige les organismes d'assurance maladie complémentaire à verser au SNDS un échantillon représentatif de leurs données de remboursement. Cette obligation est assortie d'une réserve selon laquelle l'échantillon est « *défini en concertation avec les représentants des organismes.* »

Cette réserve n'autorise pas l'État à se saisir des données des assureurs sans leur accord mais n'autorise pas non plus ces derniers à refuser d'en verser au SNDS. Elle n'impose pas le même échantillon pour tous les assureurs. Elle ne précise pas si des limites peuvent être imposées par les déposants aux finalités de leur dépôt.

Elle n'impose pas non plus de recueillir le consentement des personnes physiques concernées par l'échantillon alors que les assureurs ne sont dépositaires de leurs données que dans le cadre conventionnel d'un contrat d'assurance individuel ou collectif, qui devrait prévoir cette cession des données à un tiers.

M. Christian Babusiaux s'est d'ailleurs interrogé sur l'apport de ces données au SNDS : « *Je m'interroge sur les données qui devraient provenir des complémentaires de santé : certes, le texte législatif en fait mention mais qui, en France, pourrait contraindre des entreprises privées et des mutuelles à fournir des données alors même qu'on essaie de les exclure de la gouvernance du système ? Quel serait leur intérêt à apporter des données ? Ajoutons que les assureurs complémentaires relèvent de systèmes très variés et corrélés avec d'autres assurances. En clair, cet apport de données est loin d'être imminent.* » (1)

### *d. Les finalités attribuées au SNDS par les articles L. 1461-1 et L. 1461-3 sont différentes de celles mentionnées à l'article L. 1460-1*

L'article L. 1461-3 du code de la santé publique ouvre deux voies d'exploitation du SNDS, l'une pour les finalités mentionnées à l'article L. 1460-1, l'autre pour l'accomplissement des missions des services de l'État, des établissements publics ou des organismes chargés d'une mission de service public compétents.

Il attribue au SNDS une finalité générale de mise à disposition des données qui figure explicitement au premier alinéa du paragraphe I de l'article L. 1461-1, selon lequel « *le système national des données de santé rassemble et met à disposition* » une liste de catégories de données. Cette finalité générale figure aussi au premier alinéa du paragraphe III de ce même article, selon lequel « *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* ».

*(1) Audition du 17 janvier 2017.*

La suite du paragraphe III dit que cette finalité générale contribue à six autres finalités [(1)], qui seraient donc non seulement plus particulières mais aussi « supérieures » à la finalité générale.

Ces six finalités particulières pourraient distribuer les accès au SNDS en autant de voies si celles-ci n'étaient écartées par les voies d'accès prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et ses décrets d'application et par l'accès ouvert aux dépositaires d'une mission de service public par le III de l'article L. 1461-3.

L'expression de ces six finalités particulières ne reprend pas celles du règlement européen ni celles de l'article L. 1460-1. La finalité du 6° ajoute l'innovation aux motifs d'intérêt public repris par l'article L. 1460-1 – à savoir la recherche, l'étude et l'évaluation – mais restreint leur champ aux domaines de la santé et de la prise en charge médico-sociale.

La finalité du 1° – l'information sur la santé et sur l'offre de soins, la prise en charge médico-sociale et leur qualité – n'a guère d'équivalent dans le règlement européen. Elle correspond au droit public à l'information qu'implique une démocratie sanitaire.

Outre ces finalités légales, il faudra aussi compter, lors de son entrée en vigueur, le 1er avril 2017, avec celles attribuées au SNDS par le décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ». L'article R. 1461-1, codifié par ce décret, décline et complète les finalités des articles législatifs L. 1461-1 et suivants, ajoutant l'innovation aux finalités de recherche, d'étude et d'évaluation dans le domaine de la santé et, au passage, de la prise en charge médico-sociale. [(2)]

---

*(1) « 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° A l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité ;*

*« 2° A la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale ;*

*« 3° A la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales ;*

*« 4° A l'information des professionnels, des structures et des établissements de santé ou médico-sociaux sur leur activité ;*

*« 5° A la surveillance, à la veille et à la sécurité sanitaires ;*

*« 6° A la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale. »*

*(2) Art. R. 1461-1.- Le traitement de données à caractère personnel dénommé système national des données de santé (SNDS), institué à l'article L. 1461-1, est mis en œuvre par la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS) dans les conditions fixées par le présent chapitre.*

*Il a pour finalité, en application des dispositions de l'article L. 1461-1, de mettre à disposition des données qu'il rassemble dans les conditions définies aux articles L. 1461-2 à L. 1461-6 afin de contribuer :*

*1° A l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité, l'orientation des usagers dans le système de santé, en permettant la comparaison des pratiques de soins, des équipements et des tarifs des établissements et des professionnels de santé ;*

*2° A la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale, en favorisant l'identification des parcours de soins des patients, le suivi et l'évaluation de leur état de santé et*

Dans sa réponse écrite à une question du rapporteur, la DREES indique que « *S'agissant des accès permanents, les finalités du SNDS n'ont pas été hiérarchisées, ce sont les missions de recherche, étude, évaluation des organismes, services et établissements concernés qui ont été analysées.* » Elle précise toutefois que les accès permanents à des catégories de données précises ont été positionnés dans le décret précité « *en tenant compte des finalités visées.* »

M. Édouard Geffray a déclaré pour sa part que « *Le cadre juridique actuel est défini par la directive de 1995 et la loi de 1978, notamment ses chapitres IX et X, qui ont été fusionnés en un seul chapitre par la loi de modernisation du système de santé.*

« *Le règlement européen qui entrera en vigueur le 25 mai 2018 le modifie assez substantiellement, notamment parce qu'il crée de nouveaux droits, en particulier le droit à la portabilité – qui permettra aux individus de récupérer les données qu'ils ont fournies pour les utiliser à d'autres fins –, et parce qu'il soumet les responsables de traitement – en l'espèce, la CNAMTS – à des obligations supplémentaires.*

« *Ces derniers devront ainsi intégrer le paramètre de la protection des données dès la conception de leur service, de leur produit ou de leur traitement. Ce principe nouveau – connu sous le nom de* privacy by design *– est intéressant car il s'agit d'un principe de droit "dur" dont le non-respect sera susceptible de sanctions, lesquelles seront, du reste, considérablement renforcées.*

« […] *la réglementation européenne prévoit des "exceptions" en matière de santé et confie au droit national le soin de préciser les "conditions supplémentaires et garanties particulières" applicables en la matière.* » (1)

---

*de leur consommation de soins et de services d'accompagnement social, l'analyse de la couverture sociale des patients, la surveillance de la consommation de soins en fonction d'indicateurs de santé publique ou de risques sanitaires ;*

*3° A la connaissance des dépenses de santé, des dépenses de l'assurance maladie et des dépenses médico-sociales, en permettant d'analyser les dépenses des régimes d'assurance maladie par circonscription géographique, par nature de dépense, par catégorie de professionnels ou de prescripteurs et par professionnel ou établissement, les dépenses d'assurance maladie au regard des objectifs sectoriels de dépenses fixés, dans le cadre de l'objectif national de dépenses d'assurance maladie, par les lois de financement de la sécurité sociale, l'analyse quantitative des déterminants de l'offre de soins et la mesure de leurs impacts sur l'évolution des dépenses d'assurance maladie ;*

*4° A l'information des professionnels de santé, des structures et des établissements de santé ou médico-sociaux sur leur activité, en permettant la transmission aux prestataires de soins des informations pertinentes relatives à leur activité, à leurs recettes et, s'il y a lieu, à leurs prescriptions et la mise à la disposition de leurs représentants de données ne faisant pas apparaître l'identité des professionnels de santé ;*

*5° A la surveillance, à la veille et à la sécurité sanitaires, en développant l'observation de l'état de santé des populations, l'évaluation et la production d'indicateurs relatifs à l'état de santé de la population et l'analyse de leur variation dans le temps et dans l'espace, la détection d'événements de santé inhabituels pouvant représenter une menace pour la santé publique et l'évaluation de leurs liens éventuels avec des facteurs d'exposition et l'évaluation d'actions de santé publique ;*

*6° A la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale.*

*(1) Audition du 24 janvier 2017.*

Dans sa réponse écrite aux questions du rapporteur, la CNIL estime que « *l'utilisation des données du SNDS est nécessairement un traitement ultérieur puisque le SNDS n'est constitué que de données pré-existantes* » et que trois exceptions posées par l'article 9 du règlement européen semblent applicables au SNDS :

« *– celle du traitement nécessaire pour des motifs d'intérêt public important ;*

« *– celle du traitement 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 ;*

« *– celle du traitement nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.* »

Elle précise aussi que l'intérêt public est une notion qui n'est définie par aucun texte d'ordre législatif ou réglementaire et que le critère d'intérêt public du paragraphe IV de l'article 8 de la loi de 1978 est la transposition du « motif d'intérêt public important » du 4° de l'article 8 de la directive 95/46/CE.

***e. Les finalités de traitement de données de santé admises par la loi de 1978 sont plus proches de celles du règlement européen***

Les finalités du SNDS ne se résument pas à celles des articles législatifs et réglementaires du code de la santé publique et à celles des dispositions propres aux sources légales de cette archive nationale d'intérêt public. Toutes ces finalités, déjà bien disparates, doivent encore être composées avec celles de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le paragraphe I de l'article 8 de cette loi reprend le principe posé par l'article 9 du règlement européen. Il 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.* »

Cet interdit de principe est assorti d'exceptions qui reprennent, plus fidèlement que le code de la santé publique, celles de l'article 9 du règlement européen.

En particulier, le 8° du paragraphe I autorise les traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé selon les modalités prévues au chapitre IX de la loi de 1978, sans mentionner le critère

d'intérêt public. Cette exception principale est assortie, par l'article 53, d'exceptions secondaires qui relèvent d'autres lois spéciales [(1)].

En définitive, la loi de 1978 établit une dizaine de régimes de traitement de données à caractère personnel dans le domaine de la santé dont un seulement, celui de l'article 54, relèverait du titre VI du livre IV de la première partie du code de la santé publique.

L'article 54 de la loi de 1978 réserve en effet à la CNIL l'autorisation des 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.

Or l'article L. 1460-1 ne vise pas le domaine de la santé, c'est-à-dire un champ de recherche, mais 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* », c'est-à-dire un dépôt public d'archives administratives. Ce dépôt public n'entre pas exactement dans le domaine réglé par l'article 54.

Quant à la conformité de ces dispositions au règlement européen, elle peut être appréciée au regard de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique qui a introduit, dans l'article 40 de la loi de 1978, le droit à l'effacement, dit aussi droit à l'oubli, prévu par l'article 17 du règlement européen. Cette transposition a consisté à reproduire dans l'article 40 les termes exacts employés par le règlement pour désigner les traitements exemptés du droit à l'effacement, donc soumis à un archivage d'intérêt public, à savoir ceux nécessaires :

« *1° Pour exercer le droit à la liberté d'expression et d'information ;*

« *2° Pour respecter une obligation légale qui requiert le traitement de ces données ou pour exercer une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;*

« *3° Pour des motifs d'intérêt public dans le domaine de la santé publique ;*

---

*(1) Il s'agit : 1° des traitements de données à caractère personnel ayant pour fin le suivi thérapeutique ou médical individuel des patients ; 2° 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° 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° 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° 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° 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.*

« *4° A des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, dans la mesure où le droit mentionné au présent II est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement.* »

Le statut législatif du SNDS pourrait se revendiquer de chacune de ces exceptions au droit à l'oubli, sans être restreint à celle du 4° qui reprend exactement les termes de l'exception *j* de l'article 9 du règlement européen.

Cependant, ces dispositions ne correspondent ni au 8° de l'article 8 de la loi de 1978, ni aux articles 53 et 54 de cette loi, ni au titre VI du livre IV de la première partie du code de la santé publique.

***f. Le décret d'application de la loi de 1978 permet à une personne de s'opposer à un traitement dont elle serait informée***

L'article 38 du décret n° 2005-1309 du 20 octobre 2005, dans sa rédaction issue du décret n° 2016-1872 du 26 décembre 2016, qui entrera en vigueur le 1er avril 2017, dispose que « *La personne qui entend s'opposer au traitement à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé des données à caractère personnel la concernant peut exprimer son refus par tout moyen auprès soit du responsable de la recherche, de l'étude ou de l'évaluation, soit de l'établissement ou du professionnel de santé détenteur de ces données excepté dans le cas prévu au II de l'article R. 1461-9 du code de la santé publique.* »

L'article R. 1461-9 – qui entrera également en vigueur le 1er avril 2017 – dispose que :

« *I.- Les modalités d'information des personnes auxquelles les données se rapportent sont fixées aux articles 32 et 57 de la loi n° 78-17 du 6 janvier 1978 et aux articles 35 et 36 du décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

« *II.- Les droits d'accès, de rectification et d'opposition s'exercent, dans les conditions définies aux articles 92 à 95 du décret n° 2005-1309 du 20 octobre 2005 modifié, auprès du directeur de l'organisme gestionnaire du régime d'assurance maladie obligatoire auquel la personne est rattachée.*

« *III.- Le droit d'opposition prévu aux premier et troisième alinéas de l'article 56 de la loi n° 78-17 du 6 janvier 1978 précitée porte sur l'utilisation des données dans les traitements mentionnés au 1° du I de l'article L. 1461-3 du code de la santé publique. Il ne s'applique pas aux traitements prévus au 2° du I du même article.* »

En d'autres termes, une personne concernée pourrait s'opposer auprès de la CNAMTS, dépositaire du SNDS, ou de l'opérateur, à un traitement autorisé par

la CNIL mais pas à un traitement opéré par une personne morale disposant d'un accès permanent au système national ni à un traitement autorisé par la loi.

Dans ces deux derniers cas, l'intéressé ne pourrait que s'opposer à la levée du secret professionnel à l'occasion de ce traitement. Le cas le plus singulier est d'ailleurs celui des professionnels de santé puisque le second alinéa de l'article L. 1461-2 du code de la santé publique déroge, à leur sujet, au principe de publication d'agrégats anonymes et à l'interdiction de réutiliser les données publiées pour identifier les personnes concernées.

Il dispose que « *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.* »

L'article L. 162-1-11 du code de la sécurité sociale prévoit que « *Les organismes gestionnaires des régimes obligatoires de base de l'assurance maladie assurent, par tous moyens adaptés, une mission générale d'information des assurés sociaux, en vue notamment de faciliter l'accès aux soins et à la protection sociale et de leur permettre de connaître les conditions dans lesquelles les actes de prévention, de diagnostic ou de soins qu'ils reçoivent sont pris en charge.*

« *Les assurés sociaux peuvent obtenir toutes informations utiles portant notamment sur les tarifs applicables, les taux de remboursement et les conditions de prise en charge des services et des produits de santé, ainsi que sur le bon usage des soins ou de ces produits.* »

Ces dispositions autorisent-elles davantage que la publication des honoraires demandés par les professionnels de santé exerçant dans le secteur libéral et des tarifs pratiqués par les pharmacies d'officine ?

Autorisent-elles par exemple la publication d'appréciations sur la prise en charge des patients, analogues aux appréciations et classements publiés sur l'activité des établissements de soins ? Le rapporteur y est clairement défavorable.

Les professionnels concernés pourraient-ils demander que les données du SNDS permettant de justifier ces appréciations soient maintenues sous le secret professionnel, les appréciations restant alors subjectives et sans preuve ?

Interrogés par le rapporteur sur une exploitation possible du SNDS afin d'établir un classement des professions de santé et sur leur opinion à propos des critères de ce classement, les représentants de l'UNPS ont apporté des réponses circonstanciées. (1)

*(1) Audition du mardi 20 décembre 2016.*

M. William Joubert a tout d'abord rappelé la spécificité de l'activité d'un professionnel de santé, qui suppose une confidentialité particulièrement forte : « *La commission de l'open data s'était prononcée en faveur d'une possibilité de correction des données personnelles concernant les médecins et les professions de santé de ville sur internet. Face à l'éventualité d'un système de notation, il faut réaffirmer que la santé n'est pas un service comme un autre – elle exige une confidentialité, un rapport intime entre les patients et les professionnels, ainsi qu'une déontologie que ne connaissent pas d'autres services. Pour ces raisons, elle doit être traitée différemment.*

« *Quels seront les critères premiers de l'évaluation d'un médecin ? Le service – délai d'attente, propreté de la salle d'attente… – ou la qualité de la prise en charge et le diagnostic ? Ces critères de notation suscitent de grandes interrogations. On en connaît les effets potentiellement pervers : les exemples dans d'autres domaines montrent que des officines vont se mettre en place, qui pourront être rémunérées, afin de profiter de ce nouveau marché. Est-on prêt à prendre de tels risques dans le domaine de la santé, sachant que cela peut déstabiliser le service lui-même ? Quand vous commencez à prendre à charge un patient en pensant aux critères de notation, votre travail en souffre.* »

M. Patrick Corne a néanmoins souligné l'intérêt, pour les professionnels de santé, de disposer d'une source d'informations permettant de lutter contre les approximations et les informations peu fiables : « *Si l'exploitation des données du SNDS était bien faite, elle pourrait constituer une réponse. Si ce réservoir énorme de données que nous sommes le seul pays au monde à posséder était exploité de manière complète, on pourrait démentir les informations qui circulent sur internet ; on sait que tout et n'importe quoi circule sur internet.* »

M. William Joubert est, par ailleurs, revenu sur la difficulté d'apprécier la qualité du service délivré par un professionnel de santé *via* les seules données contenues dans le SNDS : « *Le SNDS va approcher le traitement qualitatif des données de façon plutôt marginale, à travers les affections de longue durée et la classification commune des actes médicaux (CCAM). Nous avons du mal à saisir de quelle manière la qualité du service d'un professionnel de santé pourrait être analysée par un service tel que le SNDS.* »

S'agissant des patients, ceux qui seront accueillis dans des établissements de soins se verront remettre, en application de l'article 37 du décret du 20 octobre 2005, un document ou un autre moyen approprié leur permettant de prendre utilement connaissance de mentions publiées, selon l'article 36, à destination des autres personnes intéressées par le SNDS, sur le site internet des établissements ou organismes dépositaires des sources.

Ces dispositions réglementaires ne précisent pas si ces mentions décriront les traitements demandés ou seulement ceux autorisés et s'ils les décriront un par un ou en des termes très généraux ou dans les termes prévus par le règlement européen.

Il est cependant probable que ces mentions s'inspireront des dispositions de l'article 14 du règlement relatives aux traitements nécessaires puisque l'article 36 du décret ne s'applique qu'aux traitements de données préalablement rendues non directement identifiantes, autrement dit à celles qui ne permettent guère d'informer individuellement et en détail les intéressés des traitements auxquels leurs données sont exposées.

Pour toutes les raisons exposées ci-dessus, le rapporteur réaffirme avec vigueur qu'il est absolument défavorable à une « classification » des professionnels de santé sur une base individuelle.

#### *g. L'exploitation du SNDS aura,* in fine*, une forte dimension contractuelle*

Le code de la santé publique s'engage dans la voie d'une contractualisation de l'exploitation du SNDS qui est conforme à l'intention du règlement européen mais n'est pas pleinement assumée par le législateur.

Le code confond des finalités de traitement des données de santé que le règlement européen distingue, les unes de droit public, les autres soumises au secret professionnel, les dernières d'intérêt scientifique, historique ou statistique.

En les confondant, il ne reprend pas exactement les termes par lesquels le règlement européen désigne les finalités licites de traitement des données personnelles. Il leur préfère des termes moins précis, enchevêtrés d'un article à l'autre, modulés par les textes réglementaires d'application.

Cette confusion abandonne à la convention conclue entre le consultant occasionnel du SNDS et la CNIL la définition précise des droits et limites d'exploitation accordés au consultant et de l'obligation de rendre public ses travaux à laquelle il doit consentir en contrepartie.

Cette obligation de publier déroge aux règles de la recherche publique et de la propriété intellectuelle pour un motif d'intérêt public qu'il appartiendra à la jurisprudence et, en dernière instance, au Conseil constitutionnel d'apprécier.

### 4. Vers une réforme du statut législatif du SNDS ?

#### *a. Le principe du contrôle* a posteriori *et le critère de l'intérêt public pourraient justifier de réviser le statut législatif du SNDS*

M. Christian Babusiaux a formé le vœu d'une réforme législative du statut du SNDS qui ne retienne qu'un contrôle *a posteriori* des traitements de données et révise le critère retenu de l'intérêt public pour les admettre. Il s'est exprimé sur ces deux sujets en des termes tout à fait clairs : « *L'essentiel serait d'inverser la problématique. Les autorisations ponctuelles sont trop bureaucratiques. L'IDS était arrivé à en accorder environ 140 par an, soit un rythme gérable – qui ne semble pas s'être infléchi depuis. Demain, en revanche, dans une société où l'on*

*recourt davantage aux données, les demandes d'accès pourraient se multiplier, d'où un engorgement des instances et de la CNIL.*

« *Peut-être vaut-il mieux instaurer – comme dans d'autres domaines – un véritable système régulé, plutôt qu'administré. La loi pourrait fixer les principes généraux des conditions à remplir par les acteurs concernés, que préciseraient des cahiers des charges. L'INDS assurerait la régulation du processus, et la CNIL disposerait de pouvoirs de contrôle et de sanction renforcé.* » (1)

Interrogé par le rapporteur sur le modèle idéal qui permettrait de répondre à l'enjeu de prévention tout en ouvrant l'utilisation des données au service de la santé de nos concitoyens, M. Babusiaux a répondu : « *Deux solutions s'offrent selon moi au législateur. La première consiste à amender de manière chirurgicale certains points de la loi. S'agissant de la notion d'intérêt public, par exemple, j'ai suggéré, pour éviter les blocages, de retenir la notion d'intérêt pour plusieurs types d'acteurs.*

« *L'accès aux données ne doit évidemment pas répondre à un intérêt corporatiste ; cependant, il peut correspondre à l'intérêt des patients et des professionnels de santé, ou à celui de l'assurance maladie, des hôpitaux ou encore des complémentaires de santé – en clair, à "plusieurs groupes d'acteurs" dont les intérêts sont divergents, d'où le caractère plus opérationnel de cette notion par rapport à la notion certes noble, mais plus impondérable, d'intérêt public.*

« *D'autre part, il conviendrait de ne pas se contenter de tenir compte de la nature juridique des organismes concernés. Imaginons un organisme privé sans but lucratif qui conduit des recherches visant à mieux connaître les parcours de soins : son besoin d'accéder aux données est tout aussi important et légitime que celui d'un organisme public.*

« *Or, aujourd'hui, la loi ouvre l'accès aux données à raison de la nature juridique des organismes, par exemple aux administrations – qui en font beaucoup trop peu usage, hélas – et non aux organismes privés. Pour quelle raison ? C'est la finalité recherchée qui doit primer : il faut s'assurer qu'elle corresponde bien à l'intérêt d'un ensemble d'acteurs.*

« *Ensuite, j'estime, outre l'accès dont bénéficient déjà les équipes des CHU et de l'Institut national de la santé et de la recherche médicale (INSERM) à l'échantillon généraliste de bénéficiaires, qu'il faut ouvrir la voie vers un accès permanent à l'ensemble de la base pour des équipes dûment accréditées. Plutôt qu'une autorisation au cas par cas, c'est l'autorisation donnée à des équipes qualifiées qui importe : lesdites équipes doivent alors remplir un cahier des charges qui fait l'objet d'une vérification et, une fois dûment agréées, elles peuvent accéder aux bases sous réserve d'un droit de contrôle.*

*(1) Audition du 17 janvier 2017.*

« *En somme, il est possible d'apporter un certain nombre d'amendements précis à l'article 193 de la loi du 26 janvier 2016. L'autre solution repose davantage sur une conception politique de fond de la place respective des administrations publiques, entendues au sens large, et de la société civile.*

« *Les auteurs de la loi actuelle distinguent en quelque sorte entre les "purs" et les "impurs" – d'un côté la sphère publique, de l'autre la société civile –, distinction qui se traduit dans les conditions d'accès aux données de santé et la constitution du GIP du futur INDS. Encore une fois, cela relève davantage d'une conception d'ensemble – et appelle donc une révision globale de l'article 193 de la loi du 26 janvier 2016.* »

***b. D'éventuelles non conformités de la loi nationale au règlement européen pourraient conduire à une refonte substantielle du statut législatif du SNDS***

Une mission d'information de la commission des lois examine, depuis décembre 2016, les incidences sur la législation française des nouvelles normes européennes en matière de protection des données personnelles.

Entre le 1er avril 2017 et le 25 mai 2018, la consultation du SNDS s'exercera sous l'empire de la directive 95/46 du 24 octobre 1995. Son article 8, alinéa 4, autorise, sous réserve de garanties appropriées, les États membres à prévoir, pour un motif d'intérêt public important, des dérogations à la protection des données personnelles de catégorie particulière telles que les données de santé.

La conformité du statut du SNDS au règlement européen reposera donc sur l'appréciation des mesures techniques et organisationnelles qui permettent aux personnes physiques d'exercer leurs droits individuels et à la CNIL d'exercer le contrôle que réclame le règlement.

Lors de son audition, M. Édouard Geffray a informé la mission des développements récents et prochains au regard de la conformité de la loi nationale aux stipulations à venir du règlement européen :

« *Le Parlement sera donc saisi, probablement à la fin du mois de juin 2017, d'un nouveau projet de loi "Informatique et libertés", qui visera à tirer toutes les conséquences du règlement européen et qui traitera notamment des données de santé.*

« *Pour résumer le débat, le Parlement devrait ainsi se prononcer sur le point de savoir si nous conservons le dispositif issu de la loi de modernisation de notre système de santé ou si nous remettons l'ouvrage sur le métier.*

« *Selon notre première analyse, le régime actuel pourrait demeurer, compte tenu du périmètre des exceptions prévues par le règlement européen – cette analyse doit cependant être affinée par la Direction des affaires civiles et du Sceau, qui pilote le projet au niveau interministériel.*

« *Je crains donc que le chantier ne soit pas totalement achevé, alors même que les décrets d'application de la loi de modernisation du système de santé ne sont pas encore publiés. De fait, actuellement, nous en sommes réduits à nous demander si un régime juridique dont nous ne connaissons pas encore tous les contours est bien compatible avec un texte dont la clarté n'est pas évidente…*

« *L'intérêt public, qui est mentionné dans la loi, doit être qualifié par l'INDS, l'intérêt scientifique étant apprécié, quant à lui, par le CEREES. Ensuite, les conditions de protection des données relèvent de la CNIL. Le dispositif est ainsi fait qu'en cumulant le critère d'entrée, les conditions de traitement internes et l'assimilation de la ré-identification à un détournement de finalité passible de sanction, nous avons les moyens, me semble-t-il, de maîtriser l'objet dans un cadre conforme au niveau d'exigence européen et à celui du législateur.* » (1)

Le rapporteur relève que, sans attendre le projet de loi annoncé par le secrétaire général de la CNIL, les dispositions législatives ou codifiées de l'article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé pourraient être modifiées par ordonnance. L'article 225 de la loi habilite d'ailleurs le Gouvernement à assurer, par ordonnances, la cohérence des textes au regard des dispositions de cette loi et à abroger les dispositions devenues sans objet. Cette habilitation a déjà donné lieu à une première ordonnance n° 2017-31 du 12 janvier 2017.

Au-delà de ces considérations de technique législative, le rapporteur ne peut manquer de formuler une observation : il est assez regrettable que sur un sujet qui, bien que technique à la base, n'en est pas moins fondamentalement sociétal – que voulons-nous faire de nos données personnelles de santé et quelle protection sommes-nous prêts à leur accorder ? – un télescopage calendaire entre les processus législatifs national et européen, en 2015-2016, ait abouti à ce qu'il faille remettre prochainement en chantier des dispositions importantes alors même que les mesures d'application du dispositif voulu par le législateur national n'ont pas encore été complètement déclinées au plan réglementaire.

À plus brève échéance, des sujets très concrets sont également ouverts, qui concernent la « vie quotidienne » du système de données de santé. En particulier, les questions relatives au renforcement de la sécurité informatique devront trouver rapidement des réponses convaincantes, tant il est vrai que le succès du SNDS et le développement de ses usages dépendront en grande partie de la confiance que les publics concernés pourront placer dans cet outil et lui conserver dans la durée.

*(1) Audition du 24 janvier 2017.*

## B. UNE SÉCURITÉ INFORMATIQUE QUI N'EST PAS MENACÉE DANS L'IMMÉDIAT, MAIS QUI DOIT FAIRE L'OBJET D'UN RENFORCEMENT

### 1. L'enjeu de sécurité souligné par la Cour des comptes est désormais assumé par la CNAMTS

#### *a. Depuis 2009, la CNAMTS a engagé des actions visant à sécuriser son système d'information*

La Cour des comptes appelait dans son rapport à renforcer la sécurité du système national des données de santé et dressait une liste des atteintes à prévenir :

– une détérioration des matériels ;

– une pénétration des logiciels ;

– une altération des données ;

– une divulgation d'information.

La Cour soulignait que « *Jusqu'en 2013, les équipes concernées n'ont pas constamment attaché à la sécurité la priorité appropriée, alors même qu'indépendamment du rapport de la Cour établi en 2010, pas moins de trois autres rapports avaient souligné en 2009-2011 des lacunes et des défaillances à corriger sans attendre.* »

Elle rappelait avoir attiré l'attention des autorités à ce sujet dans un chapitre de son rapport sur l'application des lois de financement de la sécurité sociale pour 2010, dont les recommandations n'avaient pas été suivies puisque « *Encore début 2016, le plus récent rapport de test d'intrusion par un prestataire spécialisé remontait à 2010. Sa conclusion avait été qu'un "attaquant n'ayant pas de compte sur le portail ne pouvait réaliser aucune action dangereuse" pour le SNIIRAM, mais que toute personne ayant un compte sur le portail du SNIIRAM, même en accès très limité, pouvait "rebondir sur une grande partie du système d'information de la CNAMTS". Plusieurs risques étaient en partie classés comme étant d'une gravité majeure, avec une probabilité ou un impact "catastrophiques".* » [(1)]

Des redressements immédiats ont été opérés à la suite de ce test, mais sans toujours remédier suffisamment aux failles, alors qu'il y avait pourtant urgence à parer aux risques croissants de piratage auxquels sont confrontés de nombreuses institutions et opérateurs.

La Cour reconnaît que, depuis 2013, la CNAMTS s'est engagée dans une sécurisation de ses systèmes d'information qui bénéficie au SNDS qu'elle constitue et héberge. Cette politique a été discutée au cours de la table ronde des acteurs de l'assurance maladie tenue le 17 janvier 2017.

---

*(1) Cour des comptes,* op. cit., *pages 38 et 39.*

M. Nicolas Revel a rappelé que « *La CNAMTS est depuis longtemps consciente de l'enjeu attaché à la sécurisation des accès. Au-delà du constat qu'il n'y a jamais eu d'intrusion réussie au sein du SNIIRAM, nous sommes conscients qu'il s'agit de données sensibles. Elles ne sont toutefois pas nominatives et ont donc moins de valeur, vis-à-vis du risque de piratage informatique, que des données existant dans d'autres bases partagées par tous les assureurs de santé, publics et privés, et comprenant parfois des coordonnées bancaires.*

« *Dès 2009, la CNAMTS a engagé des travaux continus pour assurer la sécurisation du SNIIRAM. La Cour souligne bien qu'un gros travail a été effectué. Nous nous projetons, bien entendu, dans la phase suivante car notre algorithme a vocation à être modernisé et le SNDS sera plus ouvert et comprendra davantage d'utilisateurs et de données.*

M. Revel est convenu que « *Le jour où nous subirions une intrusion et un vol de données, y compris nominatives, se poserait immanquablement la question de savoir s'il faut maintenir une base de données nationale aussi considérable et agrégée. C'est un enjeu de crédibilité et de pérennisation de l'outil.* » Il a cependant mis en parallèle le statut d'ores et déjà correctement sécurisé des données du SNIIRAM et du futur SNDS et celui, beaucoup plus vulnérable, des données personnelles de santé issues des objets connectés, qui sont appelées à se multiplier sensiblement dans les toutes prochaines années : « *Entre parenthèses, nous n'avons pas vocation – même si cela pourrait être un sujet à l'avenir – à récupérer les données liées aux objets connectés, qui vont se développer très fortement. Nous prenons en charge les données liées aux remboursements, à la prise en charge des actes et des séjours en établissement, auxquelles nous ajouterons celles relatives aux décès puis au médico-social.*

« *Il est exact que nous recevrons beaucoup de données liées à la récupération et à l'exploitation des données sur le suivi des patients par objets connectés sur toutes sortes de pathologies. La question est de savoir ce que pourrait être un usage anonymisé public de ces données.* »

Dans sa réponse écrite aux questions du rapporteur, la CNAMTS apporte des détails montrant combien la sécurité a été placée au centre de ses préoccupations : « *Un plan d'action a été mis en place depuis plusieurs années et le dossier central de sécurité du SNIIRAM a été mis à jour et présenté à la CNIL mi 2015, qui l'a considéré comme de qualité. Avec le DCS, un plan d'action a été établi comprenant des mesures techniques et organisationnelles pour sécuriser les conditions d'accès et d'exploitation.*

« *Ce plan d'action sur le seul SNIIRAM a également permis de mettre en place le plan d'action sécurité sur le SNDS de son ouverture au printemps 2017 jusqu'à l'échéance de fin janvier 2019, date à laquelle le système cible doit être opérationnel. Ce plan d'action est un des éléments fourni à la CNIL pour l'examen de l'arrêté portant le référentiel de sécurité.* »

Les résultats du plan d'action de la CNAMTS ne seront toutefois connus que lorsque les atteintes portées à la sécurité des systèmes d'information contenant des données personnelles protégées seront portées à la connaissance de la CNIL, conformément à une obligation de déclaration incluse dans le règlement européen qui entrera en vigueur en mai 2018.

M. Édouard Geffray a d'ailleurs rappelé que *« Aujourd'hui, il n'existe pas d'obligation de notification à la CNIL des failles de sécurité des bases de données. Cette obligation – qui ne pèse, actuellement, que sur les opérateurs de télécommunications – sera introduite par le règlement européen sur la protection des données, qui entrera en vigueur le 25 mai 2018. Je ne suis donc pas en mesure de vous dire si les organismes dont il est question ici pâtissent de telles failles.*

« *Cependant, nous observons, de manière générale, que le nombre de saisies, qu'elles soient spontanées ou le fait de tiers, concernant des failles de sécurité ne cesse de croître, si bien qu'elles deviennent le lot quotidien de la CNIL. Ces failles – qui peuvent être dues, par exemple, à des attaques extérieures ou à la négligence d'agents qui égarent leur ordinateur ou leur téléphone non crypté – sont donc un enjeu majeur. Le 25 mai 2018, nous pourrons vous donner une photographie en temps réel des informations qui nous seront transmises dans ce domaine.* » (1)

Lors de son audition, M. Philippe Loudenot, fonctionnaire de sécurité des systèmes d'information pour les ministères chargés des affaires sociales, a cependant souligné que l'obligation de déclaration des incidents affectant la sécurité informatique des établissements de santé, prévue par le règlement européen, était anticipée par l'article 110 de la loi de modernisation de notre système de santé. Celui-ci a inséré dans le code de la santé publique, à l'initiative de notre collègue M. Gérard Bapt, un article L. 1111-8-2 qui prévoit que « *Les établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins signalent sans délai à l'agence régionale de santé les incidents graves de sécurité des systèmes d'information. Les incidents de sécurité jugés significatifs sont, en outre, transmis sans délai par l'agence régionale de santé aux autorités compétentes de l'État.* » (2)

### *b. Peu inquiète du risque d'intrusion, la CNAMTS s'est surtout attachée à améliorer la qualité des données hébergées*

Le rapporteur a évoqué à plusieurs reprises le risque d'intrusion, dans le SNDS, voire dans les dossiers médicaux personnalisés, afin d'en extraire des informations réidentifiantes pour en demander rançon par chantage aux personnes concernées.

M. Nicolas Revel a jugé que le SNIIRAM n'est pas dans la même situation que d'autres bases de données personnelles de santé : « *Dans notre*

*(1) Audition du 24 janvier 2017.*

*(2) Audition du 7 février 2017.*

*réflexion sur les risques d'intrusion, la cible la plus vulnérable est représentée par les bases de données nominatives. Or le SNIIRAM ne comprend pas de telles données.* »

Le rapporteur entend bien cette approche mais tient à rappeler les propos déjà mentionnés de M. Christian Babusiaux, qui prenait l'exemple du CépiDc pour expliquer comment les risques affectant la sécurité du SNDS pourraient nuire à la confiance qu'inspirent aux professionnels de santé les systèmes d'information des assureurs obligatoires et les inciter à ne pas les renseigner fidèlement (voir page 55).

Le risque de divulgation d'informations personnelles nuirait à la qualité des données collectées par le SNDS et biaiserait les généralisations qui en sont tirées. Il doit donc être pris en compte dans la politique d'amélioration de la qualité des données, mise en œuvre par la CNAMTS.

Dans sa réponse écrite aux questions du rapporteur, la CNAMTS indique que « *La qualité des données est un sous projet identifié depuis le début du SNIIRAM avec un protocole inter régimes qui a mis en place et gère tout un ensemble de contrôles permettant d'assurer l'homogénéité entre les flux arrivant des différents régimes.*

« *La qualité des données, c'est aussi la gestion de la donnée de bout en bout de sa transformation et de la traçabilité de sa transformation, le lien avec les nomenclatures. Sur le PMSI, la CNAMTS et l'ATIH ont une mise en place depuis plusieurs années des échanges formalisés sur le retour sur les bilans d'exploitation des données.* »

À cet égard, M. Dominique Martin a mis en garde contre une extension du SNDS qui pourrait le fragiliser : « *Faudra-t-il enrichir les données accessibles du SNIIRAM ? Certainement. Celles-ci sont déjà considérables et d'une grande finesse, mais nous avons tout intérêt à ce qu'elles soient complétées par d'autres données, de deux types en particulier. Il s'agit, d'une part, des données de l'assurance maladie hors remboursement : beaucoup de médicaments ou de produits de santé non remboursés soulèvent des problématiques de sécurité sanitaire – pensons aux prothèses mammaires PIP. Il s'agit, d'autre part, des données socio-démographiques, qui nous permettraient de disposer d'éléments de contexte très utiles dans l'analyse des risques, les données du SNIIRAM étant, à l'origine, avant tout médico-économiques*

« *Il faut toutefois être attentif à ce que cet enrichissement n'aboutisse pas à une usine à gaz qui rende difficile l'exploitation des données. Dans leur structure actuelle, les données sont déjà extrêmement complexes à utiliser : cela exige formation, préparation, encadrement, compétences et réclame des moyens en matière de systèmes d'information. Veillons à ne pas mettre en danger l'édifice tel qu'il existe aujourd'hui.* » (1)

*(1) Audition du 31 janvier 2017.*

Lors de la table ronde des acteurs de l'assurance maladie organisée le 17 janvier 2017, M. Claude Gissot, directeur de la direction de la stratégie de la CNAMTS, a expliqué que les producteurs de données s'étaient mis d'accord sur des formats de versement qui ont amélioré la qualité des données collectées par la CNAMTS et la fréquence des mises à jour :

« *Le régime général de la CNAMTS alimente tous les jours l'entrepôt de données, qui reprend toutes les feuilles de soins jour par jour. Le RSI et la MSA le font tous les dix jours. Ces données sont ensuite pour la plupart restituées mensuellement. Les mutuelles décompteuses ou les sections locales mutualistes assurent aussi une alimentation régulière.*

« *Au final, nous avons tous les mois les données de l'ensemble des régimes, les grands régimes mais aussi ceux qui sont qualifiés de petits régimes, qui s'appuient sur les systèmes d'information de la CNAMTS, de la SNCF ou de la MSA, pour que tous produisent la même qualité de données, selon des normes aujourd'hui bien maîtrisées.* »

M. Alain Pelc a confirmé cette situation globalement satisfaisante pour les données versées par la CCMSA : « *La CCMSA s'est engagée dans le projet SNIIRAM dès son lancement en l'an 2000. Aujourd'hui, le système statistique de la MSA est entièrement basé sur le SNIIRAM tel qu'il a été conçu – en réalité, c'est un précurseur du SNIIRAM. Autrement dit, il n'y a aucune différence entre les données que traite la MSA et celles qui alimentent le SNIIRAM.*

« *D'autre part, nous accompagnons le SNIIRAM d'un point de vue technique : nous contribuons à la définition et à l'évolution de la norme mise en œuvre par les autres régimes – cette norme est un peu différente de celle de la CNAMTS.*

« *La MSA aurait pu être critiquée sur un point : nous avons un peu tardé à mettre à disposition les données relatives aux affections de longue durée (ALD). Ce problème est désormais résolu : depuis le 1er avril 2014, nous alimentons régulièrement le SNIIRAM avec ces données. Je précise que la MSA produit les données du SNIIRAM pour deux régimes spéciaux dans le cadre de conventions de partenariat : celui de la SNCF et celui de la RATP.*

« *Du point de vue de la qualité et de la régularité, la production des données par la MSA ne soulève aucune difficulté. Nous continuerons à suivre la CNAMTS pour toutes les questions relatives au SNIIRAM. Nous l'alimentons à un rythme hebdomadaire. S'il fallait accélérer la production des données, nous ferions le nécessaire à cette fin, car nous sommes très attachés au SNIIRAM et à tout ce qu'il apporte.* »

M. Pascal Perrot s'est exprimé dans le même sens : « *En ce qui concerne l'alimentation du SNIIRAM, le RSI est aujourd'hui au rendez-vous. Depuis le 16 décembre dernier, il applique la norme d'échange commune (NEC) au lieu de*

*la norme NTEIR (norme technique d'échange inter-régimes), recommandée par la Cour des comptes.*

« *Il s'agit d'une évolution technique importante, qui nous permet d'alimenter le dispositif avec les données relatives à toutes les ALD postérieures au 1er décembre 2013, qu'il s'agisse des ALD répertoriées, des ALD hors liste ou des polypathologies. Nous avions pris un peu de retard en la matière.*

« *En outre, nous avons mené des travaux sur les données relatives aux indemnités journalières de maladie et aux médicaments, et nous sommes, là aussi, au rendez-vous. Nous alimentons le SNIIRAM environ tous les dix jours.* »

En revanche, M. Nicolas Revel a indiqué que l'intégration des données des MDPH souffrirait de l'absence d'un système d'information partagé, en dépit de l'obligation légale d'interopérabilité et bien que la CNAMTS ait œuvré à « *doter les établissements médico-sociaux d'un système d'information. Nous l'avons fait sur les établissements d'hébergement pour personnes âgées dépendantes (EHPAD) et nous sommes en train d'y travailler sur les établissements médico-sociaux prenant en charge le handicap. Il convient par ailleurs de doter les maisons départementales des personnes handicapées (MDPH) d'un système d'information partagé, ce qui n'est pas aujourd'hui le cas.* »

Lors de la table ronde du 6 décembre 2016 qui réunissait les assureurs, les mutuelles et les complémentaires santé, les représentants de la Fédération nationale de la mutualité française (FNMF) ont relevé que la faisabilité de l'intégration de l'échantillon de données des complémentaires santé a été validée par le projet MONACO – précédemment évoqué par le rapporteur – mais n'est pas industrialisée.

Selon Mme Agnès Bocognano, directrice déléguée santé à la direction santé de la FNMF, « *nous avons acquis une certaine expérience grâce au projet MONACO (Méthodes, outils et normes pour la mise en commun des données des assurances complémentaires et obligatoires) qui, même si ses résultats sont d'une ampleur moindre que celle qui était attendue, a montré qu'un tel dispositif pouvait fonctionner.*

« *Nous avons ainsi développé, au sein de la mutualité et avec les mutuelles, un système qui permettrait véritablement d' "industrialiser" le partage des données. Encore une fois, nous ne partons donc pas de rien ; nous avons besoin, pour limiter les futurs coûts de développement et de gestion, de nous appuyer sur l'expérience existante. C'est sans doute nécessaire pour que cela se fasse dans de bonnes conditions et dans des délais acceptables.* »

M. Mathieu Cousineau, responsable Pôle métier assurances à la direction santé de la FNMF, a précisé les apports et les limites du projet MONACO pour concevoir un dispositif robuste de partage des données : « *nous avons mené, dans le cadre du projet MONACO, une expérimentation à laquelle ont participé l'ensemble des familles de complémentaire et qui nous a permis de tester la*

*capacité d' "accrocher" les données de l'assurance maladie obligatoire à celles de l'assurance maladie complémentaire.*

« *Nous souhaiterions pouvoir capitaliser sur cette expérimentation, d'une part parce qu'elle a produit un certain nombre de résultats positifs et, d'autre part, parce que chaque organisme a réalisé des investissements importants dans ce cadre.*

« […] *En ce qui concerne le nouveau dispositif, je dirai que nous devons trouver le bon équilibre entre l'ambition, le réalisme et le délai. De fait, ces trois éléments sont liés. Dans le cadre du projet MONACO, par exemple, nous avons dû parfois en rabattre pour garantir le succès de l'expérimentation. Notre première attente est que le système existe et que soit défini un périmètre de travail commun, en particulier dans le domaine du reste à charge, qui est le plus immédiatement opérationnel et pour lequel on peut capitaliser le plus facilement sur les expériences passées. Le domaine de la prévention est plus hétérogène, si bien que nous devrons réfléchir à la manière dont nous pouvons formaliser les contenus et les échanges. Le délai sera plus long. Il faudrait donc en quelque sorte distinguer deux lots.* »

### 2. L'algorithme de pseudonymisation des données personnelles a été particulièrement discuté

Dans les développements conséquents qu'elle a consacrés au sujet de la sécurité du système d'information des données personnelles de santé – SNIIRAM ou SNDS –, la Cour des comptes a pointé du doigt plusieurs éléments de fragilité potentielle [(1)]. M. Philippe Burnel est revenu, lors de son audition, sur les failles relevées par la Cour, précisant notamment qu'une « *divergence* » entre la Cour et le ministère « *portait sur l'obsolescence de l'algorithme de hachage, qui aurait pour conséquence de lever l'anonymat. Si le premier risque est celui d'une infraction, d'une entrée illicite dans le système, le second serait qu'à l'occasion d'une entrée tout à fait légitime, cette fois, l'on puisse obtenir la clé de hachage permettant d'identifier les individus.*

« *La Cour a donc pointé l'ancienneté de la version utilisée et préconisé le passage à l'algorithme de la génération suivante. Selon la CNAMTS et le responsable SSI du ministère, le problème ne se posera pas au cours des quatre ou cinq ans à venir, même s'il faudra bien planifier ce changement, dont les informaticiens nous annoncent d'ailleurs qu'il sera lourd de conséquences, notamment financières.* » [(2)]

Cette divergence d'appréciation a été longuement évoquée au cours de la table ronde des acteurs de l'assurance maladie tenue le 17 janvier 2017. M. Alain Issarni, directeur des systèmes informatiques de la CNAMTS, a cependant

*(1) Cour des comptes,* op. cit., *pages 38 à 47.*

*(2) Audition du 13 décembre 2016.*

souhaité en cerner correctement le périmètre : « *Le phénomène d'intrusion n'a pas du tout été signalé par la Cour des comptes. La question est de savoir, s'il devait se produire une intrusion, ce que l'on fait des données.*

« *Les données que nous stockons sont anonymisées mais pas complètement ; on n'y trouve pas le numéro d'inscription au répertoire (NIR) ni l'identité de la personne, mais il faut tout de même, pour des prestations liées à un assuré, une forme d'identifiant qui soit toujours le même, afin de pouvoir utiliser intelligemment les données. Une succession d'éléments totalement indépendants et décorrélés ne servirait à rien ; il faut pouvoir corréler ces données à un assuré, sans pour autant identifier celui-ci. C'est pourquoi a été mis en place un système dit de "pseudo-anonymisation".*

« *Le système que nous utilisons, FOIN 2, est pointé du doigt parce que l'algorithme est un peu ancien. Les données d'identité de l'assuré, le NIR et d'autres, sont passées à la moulinette par un procédé que les spécialistes appellent SHA-1 – qui est le procédé pointé du doigt – pour créer un identifiant. Ensuite, nous créons un autre identifiant dans le SNIIRAM par un second passage de moulinette. Personne n'a, de façon connue, cassé le code SHA-1 à ce jour.*

« *Ce cryptage n'est pas réversible : il n'existe pas de système pour revenir à l'information initiale. Aussi, quand bien même quelqu'un serait parvenu à casser l'algorithme, il lui faudrait posséder les données nominatives et, avec le code cassé, les passer à la moulinette pour les comparer avec les pseudo-identifiants du SNIIRAM afin de pouvoir remonter à l'identité d'une personne. C'est la grande force de ce système.*

« *Cela nous crée en contrepartie une difficulté. Si nous voulons changer de système, il faut revenir à la donnée initiale et la recrypter différemment. En outre, il faudra donner à tous ceux qui ont des cohortes et ont déjà l'identifiant lié à FOIN 1, à FOIN 2 et même au FOIN 3, car certains passent trois fois la moulinette, la correspondance qui existera entre ce qu'ils ont aujourd'hui et le nouvel identifiant pseudo-anonymisé que nous aurons alors. C'est ce qui explique la difficulté à changer de cryptage.*

« *J'insiste cependant sur le fait que, si l'algorithme est pointé du doigt, les spécialistes s'accordent à dire qu'il n'y a pas urgence et que le changement peut se faire à l'horizon 2020, voire un peu au-delà.* »

M. Nicolas Revel a également souligné que la CNAMTS est en train d'élaborer un plan de sécurité adapté à la nouvelle phase, qui a été transmis pour examen à la CNIL. Ce plan prévoit une première série de mesures qui ont vocation à être mises en œuvre au cours des deux prochaines années, ainsi qu'une évolution de l'algorithme au cours de la période de quatre ans sur laquelle portera la prochaine convention d'objectifs et de gestion (COG). Il a mis en avant le fait que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a indiqué, dans une évaluation récente, que l'algorithme actuellement utilisé est, certes,

ancien, mais toujours robuste, et qu'une personne qui parviendrait à percer cet algorithme saurait comment anonymiser des données non cryptées, mais ne saurait pas comment remonter des données du SNIIRAM vers les données originelles.

Le rapporteur est bien conscient que, lorsque le basculement vers le nouvel algorithme aura été décidé, il faudra « récupérer » le stock de données et y appliquer rétroactivement le nouvel algorithme de pseudonymisation.

Au demeurant, la CNAMTS n'est pas le seul utilisateur de l'algorithme de chiffrage des identifiants individuels dans le SNDS. Elle l'utilise pour les données du SNIIRAM mais les autres opérateurs alimentant le SNDS l'utilisent aussi, certains dans des versions différentes, avant d'y verser leurs données.

Mme Cécile Malguid, sous-directrice santé de la Fédération française de l'assurance (FFA), a dit ne pas être certaine que « *le processus d'anonymisation soit strictement identique à celui de la CNAM, mais cela ne signifie pas qu'il n'y a ni sécurité ni anonymisation. Les critères de sécurité à respecter, rappelés dans ce Pack de conformité, sont le fruit d'un échange entre la CNIL et les assureurs. Nous sommes soumis à des contraintes de sécurité et à des obligations concernant l'utilisation des données.* » (1)

Dans sa réponse écrite aux questions du rapporteur, M. Kamel Gadouche a replacé le sujet de l'algorithme de hachage dans une vision plus large des déterminants de sécurité pertinents pour le SNDS : « *Le hachage du NIR par la méthode FOIN n'est qu'un des éléments de sécurisation de l'ensemble de la chaîne. Il est vrai qu'à notre connaissance l'algorithme utilisé pour le hachage est SHA-1 est déclaré obsolète depuis quelques années car des possibilités de collision ont été identifiées. Cependant, prise dans sa globalité, la procédure de sécurisation, compte tenu des éléments à notre connaissance, ne semble pas compromise (identification des acteurs, conventionnement avec l'institution et les utilisateurs…). Comme l'indique le rapport de la Cour des comptes, il est recommandé d'utiliser un algorithme de hachage plus récent ainsi que de mettre en place une procédure de renouvellement des clés secrètes (comme le prévoit d'ailleurs dans un autre domaine, l'article 34 de la loi pour une République numérique).* »

M. Philippe Loudenot est revenu sur le risque de sécurité présenté par l'algorithme de pseudonymisation : « *S'agissant de l'algorithme FOIN utilisé par la CNAMTS, il y a eu, selon moi, une confusion : une partie de cet algorithme est obsolète pour consulter les sites internet en toute sécurité, mais cela n'empêche pas d'employer ledit algorithme à des fins de chiffrement. En termes de sécurité pure, il convient de surveiller cet élément, mais il ne s'agit pas d'un point bloquant pour l'utilisation des algorithmes FOIN-1 et FOIN-2. Selon notre analyse, qui est partagée par l'ANSSI, nous avons encore cinq à dix belles années devant nous. Ce qui ne veut pas dire qu'il faut mettre ce problème de côté : la*

*(1) Table ronde du 6 décembre 2016.*

*CNAMTS a d'ores et déjà inscrit à son programme de travail la modification et l'évolution de l'algorithme de chiffrement.* » [1]

Le rapporteur prend acte de ce que les acteurs du SNDS sont pleinement sensibilisés au sujet de la sécurité du système d'information d'une part, de l'obsolescence de l'algorithme de hachage et de la nécessité de le remplacer d'ici quelques années d'autre part. Il souligne à nouveau l'impérieuse nécessité d'assurer autant que raisonnablement possible la sécurité du SNDS, celle-ci étant la principale, sinon l'unique garantie que les citoyens et les professionnels pourront continuer de placer leur confiance dans un système ayant vocation à accueillir toujours plus de données qui restent éminemment personnelles, fussent-elles néanmoins pseudonymisées.

### 3. La désignation de la CNAMTS comme opérateur d'importance vitale, recommandée par la Cour des comptes, n'est pas acquise

La Cour des comptes recommande de reconnaître à la CNAMTS le statut d'opérateur d'importance vitale (OIV) pour « *la soumettre aux règles et contrôles périodiques externes de sécurité* » [2]. À l'issue des travaux de la MECSS, le rapporteur doit constater que cette proposition n'a pas rencontré le succès espéré par ses promoteurs.

#### *a. La désignation des opérateurs d'importance vitale*

Un OIV est un opérateur économique ayant un rôle primordial dans le fonctionnement de la Nation – tel un réseau télécom ou une banque – et soumis de ce fait à des obligations de sécurité particulières. En 2016, le Gouvernement recense 249 opérateurs d'importance vitale (OIV), publics et privés, dont 22 dans le secteur de la santé.

Selon l'article R. 1332-3 du code de la défense, « *les opérateurs d'importance vitale sont désignés pour chaque secteur d'activités d'importance vitale* (SAIV) *par arrêté du ministre coordonnateur* » [3]. Cette désignation intervient après concertation avec le ou les ministres intéressés et après avis de la commission interministérielle de défense et de sécurité (CIDS) [4] des secteurs d'activités d'importance vitale.

Un arrêté du 2 juin 2006 [5] fixe douze secteurs d'importance vitale, au sein desquels on peut identifier quatre dominantes – régalienne [6], humaine [7],

---

*(1) Audition du 7 février 2017.*

*(2) Cour des comptes,* op. cit., *recommandation n° 3, page 11.*

*(3) Le même article prévoit que ces arrêtés ne sont pas publiés et qu'ils ne sont pas non plus communicables, en application des articles L. 311-5 et suivants du code des relations entre le public et l'administration.*

*(4) Prévue par l'article R. 1332-10 du code de la défense.*

*(5) Modifié par l'arrêté du 3 juillet 2008.*

*(6) Activités civiles de l'État ; Activités militaires de l'État ; Activités judiciaires.*

*(7) Alimentation ; Gestion de l'eau ; Santé.*

économique [1] et technologique [2]. Les produits de santé sont inclus dans le secteur « Santé », dont le ministre coordonnateur est le ministre chargé de la santé.

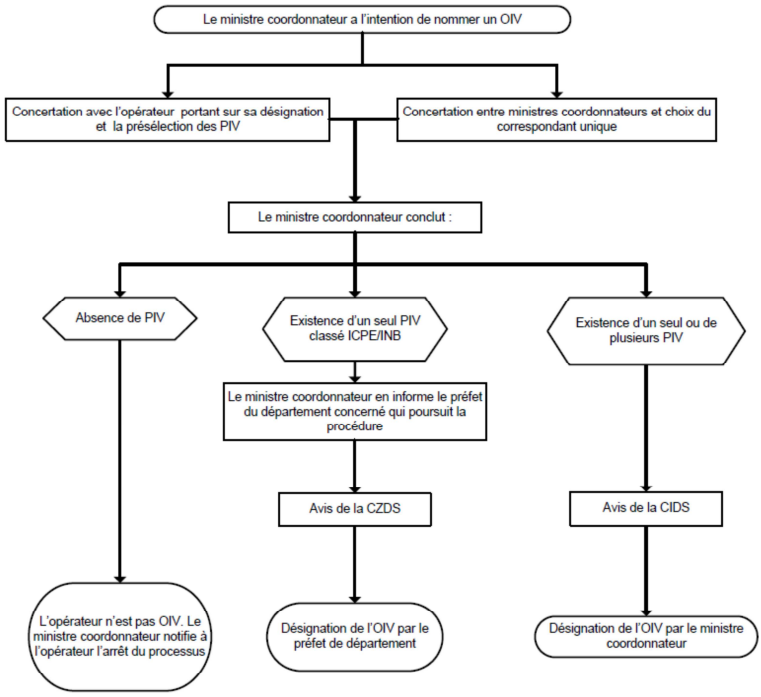



**Figure 3 : Désignation d'un OIV – processus initié par un ministre coordonnateur**

*Source : Instruction générale interministérielle relative à la sécurité des activités d'importance vitale, 7 janvier 2014*

Deux conditions doivent être réunies pour qu'un opérateur puisse être désigné d'importance vitale :

– son activité doit être exercée en tout ou partie dans l'un des secteurs d'importance vitale ;

– il doit gérer ou utiliser un point d'importance vitale (PIV), c'est-à-dire « *un établissement, une installation ou un ouvrage sis sur le territoire national dont le dommage, l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population* » [3].

*(1) Énergie ; Transports ; Finances.*

*(2) Communications électroniques, audiovisuel et information ; Industrie ; Espace et recherche.*

*(3) Instruction générale interministérielle relative à la sécurité des activités d'importance vitale, 7 janvier 2014, p. 21.*

Le ministre coordonnateur notifie à l'opérateur son intention de le désigner comme OIV. Celui-ci dispose de deux mois pour présenter ses observations.

***b. Les engagements incombant à l'opérateur d'importance vitale***

La désignation comme OIV impose à l'opérateur concerné un principe de coopération à la protection contre toute menace, notamment à caractère terroriste, des établissements, installations et ouvrages ayant un rôle primordial dans le fonctionnement de la Nation. Le schéma général est le suivant : **1/** l'État est responsable de la protection contre ces menaces sur le territoire national considéré dans son ensemble ; **2/** l'opérateur est responsable de la protection du point d'importance vitale dans le périmètre de celui-ci, sous le contrôle de l'autorité administrative ; **3/** l'État et l'opérateur organisent conjointement la protection des « alentours » du point d'importance vitale.

i. Les obligations générales pesant sur l'OIV

L'OIV doit mettre en œuvre les directives nationales de sécurité (DNS), élaborées par le ministre compétent (ministre coordonnateur du SAIV concerné). Les DNS sont fondées sur une analyse de risque qui tient compte de scénarios de menaces ; elles précisent les objectifs et les politiques de sécurité du secteur ; elles définissent des mesures planifiées et graduées de vigilance, de prévention, de protection et de réaction contre toute menace, notamment à caractère terroriste. Elles sont arrêtées par le Premier ministre.

Dans ce cadre, l'OIV doit :

– désigner un délégué pour la défense et la sécurité. Celui-ci est l'interlocuteur privilégié de l'administration, qui l'habilite au niveau « confidentiel – défense » ;

– rédiger un plan particulier de protection (PPP) pour chaque point d'importance vitale identifié [(1)]. Tout PPP doit être approuvé par l'autorité administrative ;

– s'il gère plusieurs points d'importance vitale, rédiger un plan de sécurité opérateur (PSO), décrivant son organisation et sa politique de sécurité. Le PSO doit être approuvé par l'autorité administrative ;

– assurer le contrôle de l'accès à ses points d'importance vitale, notamment en mettant en œuvre une enquête administrative qui peut donner lieu à la consultation du bulletin n° 2 du casier judiciaire et de

*(1) Au titre de la protection des alentours du PIV, il revient au préfet de département, en lien avec l'opérateur, d'arrêter un plan de protection externe (PPE) qui précise les mesures planifiées de vigilance, de prévention, de protection et de réaction prévues par les pouvoirs publics.*

traitements automatisés de données à caractère personnel, à l'exception des fichiers d'identification [1].

ii. Les obligations particulières relatives à la protection des systèmes d'information

La loi relative à la programmation militaire pour les années 2014 à 2019 [2] pose l'obligation pour les OIV de renforcer la sécurité des systèmes d'information qu'ils exploitent [3] – les systèmes d'informations d'importance vitale (SIIV). Les dispositions correspondantes ont été codifiées aux articles L. 1332-6-1 à L. 1332-6-6 du code de la défense. La France devient ainsi le premier État à réglementer la cybersécurité de ces infrastructures.

L'opérateur d'importance vitale doit identifier ceux de ses systèmes d'information qui doivent être qualifiés d'importance vitale. Il effectue à cet effet une analyse d'impacts sur chaque système d'information, au regard des types généraux de systèmes susceptibles de relever de cette catégorie, dont une liste est arrêtée pour chaque secteur d'activité d'importance vitale. En matière de produits de santé, l'annexe III de l'arrêté du 10 juin 2016 [4] liste des types de systèmes d'information pouvant être reconnus d'importance vitale ; cette annexe n'est pas publiée mais notifiée « *aux personnes ayant besoin d'en connaître* ».

Cette qualification effectuée, l'opérateur adresse à l'Agence nationale de sécurité des systèmes d'information (ANSSI) la liste des systèmes d'information d'importance vitale identifiés [5]. Il est précisé que « *la liste des systèmes d'information d'importance vitale est couverte par le secret de la défense nationale* » [6]. L'ANSSI accompagne les OIV dans la sécurisation et l'homologation de leurs systèmes d'information d'importance vitale.

Des mesures préventives sont attendues en matière de sécurité des réseaux et systèmes d'information de l'opérateur, qui doit détecter et gérer les risques en la matière. Il est chargé de notifier aux autorités compétentes les incidents ayant un impact significatif sur sa sécurité, et la CNIL doit être tenue informée des éventuelles failles relatives aux données personnelles.

Le renforcement de la sécurité des OIV implique la mise en œuvre de « *systèmes qualifiés de détection des évènements susceptibles d'affecter la sécurité de leurs SI* ». Un contrôle du niveau de sécurité et du respect des règles de

---

*(1) Article L. 1332-2-1 du code de la défense.*

*(2) Loi n° 2013-1168 du 18 décembre 2013.*

*(3) Article 22.*

*(4) Arrêté fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale* « Produits de santé » *et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense.*

*(5) Article 2 de l'arrêté précité.*

*(6) Article R. 1332-41-2 du code de la défense.*

sécurité [1] peut être effectué par l'ANSSI, un service de l'État désigné par le Premier ministre ou un prestataire de service qualifié.

La loi prévoit que les opérateurs informent le Premier ministre des incidents affectant le fonctionnement ou la sécurité des SIIV qu'ils gèrent. Enfin, si une crise majeure menace ou affecte la sécurité des SIIV, le Premier ministre peut décider des mesures à mettre en œuvre.

### *c. La prise en compte des règles définies par l'Union européenne en matière de cybersécurité*

Si le dispositif français de cybersécurité est ambitieux, il ne peut être pleinement efficace que dans le cadre de la politique commune définie à l'échelle de l'Union européenne.

La directive (UE) 2016/1148 du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite « directive NIS » [2], a été adoptée le 6 juillet 2016. Elle doit être transposée dans les droits nationaux avant le 9 mai 2018.

Cette directive vise à renforcer les capacités nationales de cybersécurité des États membres. Elle dispose par exemple que chaque État doit se doter d'autorités nationales compétentes et de stratégies nationales en la matière. Elle prescrit la création d'un « *groupe de coopération* » des États membres pour faciliter le partage d'informations et des alertes aux attaques informatiques.

En droit de l'Union européenne, le concept d'« opérateur d'importance vitale » est remplacé par celui d'« opérateur de services essentiels » (OSE), bien que leur domaine soit sensiblement le même. Un OSE est une « *entité publique ou privée* » [3] exerçant son activité dans l'un des sept secteurs énumérés [4] et répondant à trois critères d'identification [5].

La directive précitée tend à harmoniser les pratiques nationales en matière d'OSE.

Elle dispose [6] que les opérateurs doivent prendre « *les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent*

---

*(1) Article L. 1332-6-1 code de la défense.*

*(2) Network and Information Security.*

*(3) Article 4, paragraphe 4, de la directive précitée.*

*(4) Annexe II de la directive précitée : énergie, transports, banques, infrastructures de marchés financiers, santé, fourniture et distribution d'eau potable, infrastructures numériques.*

*(5) Article 5, paragraphe 2, de la directive précitée : fourniture d'un service essentiel au maintien d'activités sociales et économiques critiques ; fourniture tributaire des réseaux et systèmes d'information ; un incident aurait un effet disruptif important sur la fourniture du service.*

*(6) Article 14 de la directive précitée.*

*dans le cadre de leurs activités* » et les mesures appropriées pour « *prévenir les incidents [compromettant] la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de ces services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services* ».

Enfin, est prévue la notification des « *incidents ayant un impact significatif sur la continuité des services essentiels* » à l'autorité compétente ou à un centre de réponse aux incidents de sécurité informatique (CSIRT). Les autres États membres devront être informés par l'autorité destinataire de la notification si elle estime que « *l'incident a un impact significatif sur la continuité des services essentiels de ces États membres* ».

Le dispositif mis en place par la loi de programmation militaire 2014-2019 est globalement conforme aux dispositions de la directive NIS ; les adaptations de la législation française à cette directive devraient donc être mineures.

#### *d. L'intérêt de désigner la CNAMTS comme opérateur d'importance vitale est contesté*

Au cours de la table ronde des acteurs de l'assurance maladie tenue le 17 janvier 2017, M. Nicolas Revel a abordé l'hypothèse du classement de la CNAMTS comme opérateur d'importance vitale : « *Peut-être avons-nous tort mais nous ne pensons pas que le SNIIRAM doive relever de cette catégorie qui, comme son nom l'indique, concerne des opérations d'importance vitale pour le bon fonctionnement du pays, comme peuvent l'être la production d'électricité ou le recouvrement de l'impôt.*

« *Dans le cas qui nous occupe, il s'agit de données anonymisées qui sont utilisées pour des études, de la recherche. Si le SNIIRAM devait cesser de fonctionner pendant deux ou trois semaines, cela pourrait être contrariant pour une équipe de recherche bloquée dans ses travaux, mais le pays continuerait de fonctionner et la planète de tourner. À mon avis, ce n'est donc pas la bonne catégorie en termes de niveau de sécurisation.* »

M. Édouard Geffray a souligné le fait que le statut de l'opérateur importe moins que le degré effectif de sécurité dont ses bases de données bénéficient : « *Sur la qualification juridique d'opérateur d'importance vitale, qui emporte un certain nombre de conséquences, je serais bien en peine de me prononcer car la question excède notre champ de compétence. En ce qui concerne le niveau de garantie substantielle que l'on est en droit d'attendre – et qui, aujourd'hui, est apprécié notamment à travers la qualification d'opérateur d'importance vitale mais qui peut tout aussi bien être recherché en dehors de cette qualification –, il me semble que cette méga-base de données doit bénéficier d'une sécurité extrêmement élevée. Il s'agit tout de même de la plus belle base de données de santé du monde !* » (1)

*(1) Audition du 24 janvier 2017.*

Pour le général Arnaud Martin, Haut fonctionnaire de défense et de sécurité au secrétariat général des ministères chargés des affaires sociales, la qualification d'opérateur d'activité essentielle, élaborée par l'ANSSI, devrait être préférée à celle d'opérateur d'importance vitale :

« *Nous avons émis un avis réservé quant à la recommandation de la Cour des comptes de classer la CNAMTS au sein des opérateurs d'importance vitale (OIV). Parmi les trois directives nationales de sécurité (DNS) qui régissent le secteur de la santé, il n'y en a aucune à laquelle nous pourrions rattacher la CNAMTS.*

« *Celle-ci étant placée sous la double tutelle du ministre chargé de la sécurité sociale et du ministre chargé du budget, nous aurions pu envisager de la rattacher à la DNS relative au secteur des finances. Cependant, j'ai travaillé sur ce point avec mon homologue des ministères économiques et financiers, et nous n'avons trouvé aucune structure* ad hoc *à laquelle rattacher la CNAMTS.*

« *Notre réflexion est la suivante : autant il nous semble tout à fait envisageable et même nécessaire de mettre en place des audits triennaux pour s'assurer du niveau de sécurité du SNIIRAM, à l'instar de ce qui se fait pour les OIV – la Cour des comptes a d'ailleurs fait une ouverture à ce sujet –, autant il ne nous semble guère opportun de considérer la CNAMTS comme un OIV. Si l'on s'en tient à la lettre du dispositif de résilience de l'État, la CNAMTS n'entre pas dans cette catégorie.*

« *En revanche, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) mène actuellement une réflexion sur la notion d' "opérateur de services essentiels" dans le cadre de la transposition de la directive européenne sur la sécurité des réseaux et des systèmes d'information, dite "directive NIS" – Network and Information Security. Cette catégorie correspondrait peut-être mieux à la nature des enjeux en matière de données de santé.*

« […] *D'après la lettre de notre dispositif de résilience, un OIV est un opérateur exerçant une activité dont l'arrêt causerait un tort considérable au fonctionnement de notre pays. Au vu de l'ensemble de ses activités, même si leur arrêt provoquerait bien évidemment des difficultés ou des dommages collatéraux, la CNAMTS ne répond pas exactement à cette définition. À titre de comparaison, un certain nombre d'établissements de santé sont classés parmi les OIV, car on ne peut pas se permettre que leur activité cesse, en raison de la nature même de cette activité. D'où notre réserve quant à la recommandation de la Cour des comptes.* »(1)

*(1) Audition du 7 février 2017.*

#### 4. Le référentiel de sécurité devra choisir entre un accès à distance au SNDS, authentifié, chiffré et tracé, et un accès physique sur place

Lors de son audition, M. Kamel Gadouche a décrit les deux modes d'accès possibles aux données du SNDS, par analogie avec ceux recensés pour ouvrir les données fiscales à la consultation mis en œuvre par le CASD : « *Le CASD est né de la volonté de l'INSEE de mettre à la disposition des chercheurs les données individuelles détaillées couvertes par le secret statistique sans faire aucun compromis sur la sécurité. Le projet a été engagé en 2008 en étudiant les méthodes utilisées à l'étranger. Ce recensement a montré deux types d'accès à ces données : accès physique d'une part, accès par la voie informatique d'autre part.*

« *Dans le premier cas, l'utilisateur se rend dans les locaux du diffuseur de données. Il est fouillé à l'entrée et son identité est vérifiée avant qu'il n'accède à un ordinateur, non relié au réseau, où ont été enregistrées les données mises à disposition, et il peut y travailler. Lorsqu'il souhaite récupérer un résultat, il le demande spécifiquement ; à ce moment, un opérateur étudie ce résultat pour déterminer s'il ne contient pas de données confidentielles dissimulées volontairement ou involontairement. Cette vérification* a priori *étant faite, le fichier demandé est transmis à l'utilisateur, pas nécessairement le jour même. Un dispositif de ce type existe depuis plusieurs décennies en Amérique du Nord et depuis un peu moins longtemps en Allemagne et au Royaume-Uni et dans pratiquement tous les pays européens.*

« *La seconde méthode utilisée est la transposition informatique du dispositif "physique". Une infrastructure de traitement sécurisée garantit que les données restent confinées dans une bulle sécurisée sur un serveur auquel l'utilisateur peut se connecter à distance pour travailler sur des bases de données individuelles détaillées, sans qu'à aucun moment il puisse lui-même récupérer un fichier de données.* » (1)

L'article R. 1461-7 introduit dans le code de la santé publique par le décret n° 2016-1871 du 26 décembre 2016 précité prévoit qu'un référentiel de sécurité établisse des règles de la gestion sécurisée du SNDS et qu'il soit arrêté par les ministres chargés de la santé, de la sécurité sociale et du numérique après avis de la Commission nationale de l'informatique et des libertés.

Le référentiel de sécurité devra préciser le mode d'accès aux données retenu. M. Franck Von Lennep a indiqué à la mission que l'arrêté sur le référentiel de sécurité conclura « *un travail de plusieurs mois mené en 2016 avec les producteurs de données et des spécialistes de la sécurité – notamment l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et le haut fonctionnaire de défense et de sécurité du ministère – et en lien avec les services de la CNIL.*

*(1) Audition du 10 janvier 2017.*

« *Le référentiel de sécurité a été soumis à la CNIL, qui l'examinera en début d'année prochaine* [2017]. *Il est très attendu des producteurs de données, puisqu'il est indispensable à la mise en œuvre technique du SNDS. Bien sûr, dans la mesure où nous les avons associés à notre travail, ils ne le découvriront pas tout à fait. Le calendrier court jusqu'en 2019, avec différentes étapes d'ici là. Certains problèmes doivent être réglés dès l'ouverture du SNDS.*

« […] *L'objectif est à la fois de sécuriser les données là où elles sont et de contrôler leurs usages, ce qui n'était guère ou pas du tout fait jusqu'ici. Le référentiel de sécurité prévoit ainsi une traçabilité qui n'existait pas pour le PMSI. Le niveau de sécurité est donc significativement relevé.*

« *Mais il s'insère toujours dans une gradation : d'abord l'open data, ensuite le PMSI sur CD-ROM, enfin les données pseudonymisées dans des bulles dont on ne peut les extraire, tous les accès et requêtes étant tracés. C'est ce dernier niveau que cible notre référentiel de sécurité. Le niveau encore supérieur, applicable à des données du type de celles qui concernent le nucléaire, ne nous semblait pas nécessaire.* » (1)

M. Philippe Loudenot a ajouté que « *S'agissant du Centre d'accès sécurisé aux données, par exemple, le fait que la solution envisagée soit déjà de nature technique me gêne. Le CASD est un excellent outil* […] *; il est parfaitement adapté aux enjeux de la protection des données personnelles. Cependant, il s'agit déjà d'une solution technique. La grande difficulté que nous avons rencontrée a consisté à faire abstraction de l'ensemble des solutions techniques dont nous disposons pour envisager le nouveau référentiel de sécurité en recensant l'intégralité des risques recensés – étant entendu que la sécurité totale est une chimère.*

« *Arrive un moment où il faut choisir le produit le plus adapté aux usages afin qu'il soit possible de faire pleinement confiance aux systèmes installés. Encore une fois, le CASD est une excellente solution mais, ayant travaillé dans le milieu de la recherche, je sais d'expérience qu'il se trouvera partout quelqu'un pour tenter de contourner les mécanismes de sécurité, toujours pour de bonnes raisons, y compris – au pire – en demandant à un stagiaire de copier toutes les données apparaissant à l'écran dans un fichier Excel, ce qui signifie que nous n'aurons plus aucune maîtrise des informations en question. Nous devons aussi envisager ces risques.*

Le Secrétariat général pour la modernisation de l'action publique (SGMAP) examine six solution techniques sous l'angle de la sécurité mais aussi du point de vue économique. Pour M. Loudenot, « *À ce stade, l'ANSSI, le CASD et MindCare ont élaboré des solutions ; il existe également un projet de centre de calcul sécurisé entre la DREES et la DARES. En outre, les études conduites par le SGMAP permettront d'identifier les modèles économiques les plus pertinents.*

*(1) Audition du 20 décembre 2016.*

*Cependant, il faut toujours rester attentif à l'utilisation de tels modèles techniques en fonction des usages et des conditions d'utilisation. Le SNDS traitera des données sensibles mais aussi des données ouvertes qui ne nécessitent pas un niveau de sécurité élevé. J'en reviens systématiquement à l'analyse de risque : que veut-on protéger, à quel niveau et la mise en œuvre des décisions que nous aurons prises est-elle effective et contrôlable ?* » (1)

Cependant, comme l'a souligné à juste titre Mme Mylène Girard, chef de la mission « Accès aux données de santé » de la DREES, le choix d'un mode d'accès aux données est lié à celui d'un modèle économique d'exploitation du SNDS et le SGMAP devra donner un avis sur les deux sujets.

Dans sa réponse écrite aux questions du rapporteur, M. Kamel Gadouche revient sur le projet de référentiel dont il a eu connaissance et expose des développements particulièrement circonstanciés qu'il paraît utile au rapporteur de reproduire ici *in extenso.*

« *Il semble que le principe du confinement des données et de leur traitement à distance au sein d'espaces sécurisés mis à la disposition des utilisateurs (c'est le principe fondateur du CASD) n'apparaisse plus dans le projet de référentiel de sécurité des données de santé. Nous pensons que pour assurer une traçabilité efficace, sans avoir à reconstruire tous les systèmes d'information de tous les organismes demandant l'accès, les utilisateurs ne doivent plus pouvoir disposer "chez eux" de jeux de données confidentielles qu'ils auraient ainsi la possibilité de copier et disséminer sans que nul ne puisse le savoir…*

« *Il est admis enfin par tous que les utilisateurs autorisés (projet de traitement autorisé dans les conditions prévues par la loi et utilisateurs habilités par le responsable du projet de traitement) doivent passer par une procédure d'authentification forte pour accéder aux données et pour demander l'autorisation de "sortir" des résultats de traitements hors de la "bulle" où ils auront effectué le traitement.*

« *En revanche, il n'y a pas d'accord sur le type d'authentification forte nécessaire. Le CASD exige un enregistrement individuel des utilisateurs avec présence physique à une séance d'enrôlement et de sensibilisation ; le projet de référentiel, renvoyant à un palier 2 de la Politique générale de la sécurité des systèmes d'information en santé (PGSSI-S) autorise des procédures d'authentification à deux étages (l'utilisateur s'authentifie en local vis-à-vis de son organisme et l'organisme garantit l'authenticité vis-à-vis du serveur distant) ; certes cela supprime la contrainte de l'enregistrement individuel et cela peut fonctionner correctement en théorie mais cela suppose de faire confiance à des procédures d'authentification locale qui ont toutes les chances d'être diverses et pas toujours fiables tant que les responsables ne sont pas fortement sensibilisés à la sécurité des systèmes d'information (et aux peines encourues) et soumis à un*

*(1) Audition du 7 février 2017*

*contrôle… Or, précisément, la faisabilité et les coûts importants des audits prévus par le référentiel peuvent laisser sceptiques ; or tout reposerait sur eux…*

« *Il n'y a pas d'accord non plus sur la nécessité ou non de maîtriser les postes de travail. Le CASD prône l'usage d'un boitier sécurisé qu'il fournit lui-même et auquel l'utilisateur branche son clavier et son écran pour effectuer les traitements ; le référentiel est muet sur la question laissant la possibilité d'effectuer les traitements depuis les postes de travail professionnels voire depuis des postes de travail personnels… Il n'a pas été procédé à notre connaissance à une évaluation approfondie des deux solutions par un audit technique… Or s'il est facile de prendre le contrôle à distance des postes de travail ou si un poste de travail peut extraire par des procédés astucieux les données confidentielles du serveur où elles sont traitées, on expose le système à un grave risque de sécurité ; un tel audit est indispensable. Le CASD soutient que l'usage de boitiers sécurisés banalisés, transmis à l'utilisateur ou envoyés simplement par voie postale, limite considérablement les coûts de déploiement, d'assistance et de maintenance, c'est-à-dire une grande part des coûts cachés de la plupart des solutions logicielles existantes.*

« *Le principe du référentiel de sécurité implique une mise en concurrence entre des solutions conformes au dit référentiel. Pour ne pas multiplier des solutions distinctes, nous pensons que les différents producteurs de données auraient intérêt à choisir ensemble un ou deux prestataires communs selon un cahier des charges élaboré lui aussi en commun… Cela simplifierait considérablement les procédures ultérieures d'audit de sécurité (qui seront à multiplier par le nombre de dispositifs dans l'hypothèse où "chacun fait comme il veut") et la gouvernance de ces dispositifs ; plus généralement, la place faite par le projet de référentiel à des procédures d'autocontrôle (et à l'effet dissuasif des sanctions) suppose des acteurs ayant une bonne expérience de ces procédures.*

« *Quant à la multiplication des audits, elle se révélera très coûteuse, ou bien ces audits risquent de n'être jamais réalisés. Le choix de prestataires communs supprimerait évidemment les problèmes d'interopérabilité et d'appariement entre des jeux de données de sources différentes ; il permettrait aussi d'obtenir une garantie de qualité du service (qu'il sera très difficile d'imposer au producteurs des données eux-mêmes tant le rapport de force avec l'utilisateur est déséquilibré ; alors qu'il est possible de l'imposer à un prestataire si la qualité de service est définie dans son contrat).*

« *Cela évoque un modèle "concession de service public", où les utilisateurs paieront le prestataire en fonction du service (au-delà éventuellement d'un seuil de gratuité) ; ce sujet comme celui de la qualité de service est crucial puisque la notion de traitement de données à distance revient à une externalisation partielle des dispositifs de traitement des données pour les utilisateurs qui dès lors souhaiteront des performances et des services adaptés à leurs besoins.*

« *Gérer du service à la carte pour un nombre important d'utilisateurs n'est pas le métier de la plupart des producteurs de données… Pour le producteur de données – CNAMTS ou ATIH –, le fait de confier le service de mise à disposition à un concessionnaire réduira sensiblement le coût de cette activité, puisque le coût pourra être facturé par le prestataire et ajusté selon les exigences spécifiques des utilisateurs (le fait pour le producteur des données de financer une gratuité pour un service de base lui coûtera moins cher que la gestion d'un service complet et sur mesures).* »

Au-delà des « modèles techniques » qui peuvent être mis en place, l'interaction entre l'homme et les dispositifs conçus à partir de ces modèles est un élément essentiel de la sécurité. M. Claude Gissot a par exemple relevé que la supervision des sorties de données hors de l'espace sécurisé reste sous la responsabilité d'un être humain, qu'il y ait ou non ce qu'il a appelé un « *sas de décontamination* » : « *Il me semble que le modèle de la bulle, utilisé par le CASD, vous a été présenté par Philippe Cunéo et Kamel Gadouche. Dans ce modèle, la bulle où sont effectuées toutes les opérations est protégée par une sorte de sas de décontamination où les données sont examinées par un être humain qui juge de ce qui peut sortir ou pas.*

« *Le SNIIRAM n'a pas de sas de décontamination mais les utilisateurs sont bien entendu formés à la protection des données. Des exigences techniques et organisationnelles vont être bientôt précisées dans un référentiel de sécurité. Nous nous y conformerons, quelles que soient les méthodes utilisées. Actuellement, le CASD n'est pas encore de taille à accueillir la totalité des données d'assurance maladie.* » (1)

Pour sa part, M. Dominique Blum a insisté sur le fait que la sécurité du dispositif – quel qu'il soit – devra être placée entre les mains de « *spécialistes* », ce qui devrait avoir une conséquence en termes de maîtrise du nombre des points d'accès : « *Le Centre d'accès sécurisé aux données (CASD), hébergé par l'Institut national de la statistique et des études économiques (Insee) à Paris, organise l'accès à des données individuelles détaillées dans d'autres domaines que la santé. Les données fiscales, apparemment considérées comme encore plus sensibles que les données médicales par ceux qui les mettent à disposition de leurs utilisateurs respectifs – ce que je regrette – sont par ce biais rendues accessibles aux chercheurs de France et de pays étrangers, dans un cadre de sécurité qui a fait la preuve de son efficacité.*

« *Le référentiel de sécurité visé dans le projet de décret pour l'accès aux données du SNDS est actuellement analysé par la CNIL. Ma recommandation est de ne pas multiplier les points d'accès et de confier la sécurité du dispositif à des spécialistes. De ce point de vue, je reste très critique sur la responsabilité de l'ATIH qui, lors de la création du PMSI, n'avait pas mesuré la nécessité de sécuriser les informations collectées, car elle n'en avait ni les compétences ni la*

*(1) Audition du 17 janvier 2017.*

*culture. S'en serait-elle préoccupée que certaines informations transmises à la CNIL n'auraient pas été un peu biaisées et que des dispositions auraient été prises depuis longtemps pour assurer la sécurité du système.* » (1)

### 5. La responsabilité juridique du fournisseur d'accès au SNDS doit être précisée s'il se confirme que sa consultation est une liberté publique

Lors de son audition, M. Dominique Martin a évoqué en ces termes les risques dont pourraît pâtir la sécurité juridique du SNDS, qui prend un relief particulier – notamment au regard du principe général de responsabilité civile – dans la perspective de voir des contrôles *a posteriori* se substituer aux actuels contrôles *a priori* : « *l'ouverture du système, grande avancée actuelle, doit nécessairement s'accompagner d'une sécurisation à la fois juridique et informatique. Du point de vue juridique, compte tenu des organismes qui ont aujourd'hui accès aux données, la situation actuelle, régie par les accords-cadres, sous l'égide de la CNIL, me paraît tout à fait équilibrée ; mais l'ouverture des données à des opérateurs privés ou leur ouverture plus large aux opérateurs publics suppose que tout cela soit regardé de très près.*

« *La proposition faite par la Cour de contrôles* a posteriori *relativement stricts me semble de bon sens. À mes yeux, les contrôles* a posteriori *assortis de sanctions sévères sont souvent aussi efficaces et plus efficients que des contrôles* a priori *qui peuvent entraver le déroulement du processus et sont souvent lourds à mettre en place.* » (2)

La responsabilité juridique associée à la fourniture d'un accès à une base de données dépend du mode d'accès retenu, direct ou par réseau, et, dans ce dernier cas, du caractère interne, indépendant ou ouvert au public dudit réseau.

Les rôles respectifs de l'INDS, de la CNIL et de la CNAMTS, voire d'intermédiaires techniques, dans l'accès aux données du SNDS doivent à cet égard être envisagés dans le cadre d'une procédure légale d'encadrement de l'exercice d'une liberté publique, indifférente à la modalité technique de l'accès.

Lors de son audition, M. Franck Von Lennep a rappelé qu'en matière d'accès aux données, « *il faut distinguer les problèmes techniques – sécurité des données mais aussi capacité pour l'utilisateur à s'en servir dans son environnement de travail, ce qui nécessite des investissements des producteurs de données – des problèmes juridiques, c'est-à-dire l'autorisation délivrée soit par la CNIL, soit par d'autres acteurs.* » (3)

Mais, du point de vue du règlement contentieux d'un dommage causé à une personne concernée par cet exercice, dans l'hypothèse, classique en droit des publications, où la personne lésée demanderait réparation à l'auteur d'une

*(1) Audition du 13 décembre 2016.*

*(2) Audition du 31 janvier 2017.*

*(3) Audition du 20 décembre 2016.*

publication portant atteinte à ses droits ou à ses intérêts mais aussi à l'éditeur de cette publication et au fournisseur d'accès aux données dont ont été extraites les informations litigieuses, le plaignant pourrait demander réparation solidairement aux personnes morales de droit public qui auront permis à cet auteur d'accéder aux données du SNDS.

Quelles seraient alors les personnes publiques responsables, sachant que la fourniture d'accès est, en droit, partagée entre l'INDS, le CEREES, la CNIL et la CNAMTS et que l'accès technique est éventuellement fourni par plusieurs prestataires techniques ? Cette question, toute théorique encore puisque le seul contentieux comparable fut, pour le moment, le recours intenté par Celtipharm contre l'arrêté d'ouverture du SNIIRAM à la consultation, n'a pas reçu de réponse.

## C. UNE GOUVERNANCE DU SNDS ENCORE IMPRÉCISE

### 1. La gouvernance du SNDS est aussi divisée que celle du SNIIRAM

#### *a. La direction du SNIIRAM a pâti du conflit entre le COPIIR et l'IDS*

L'étude d'impact de l'article 47 du projet de loi de modernisation de notre système de santé [(1)] affirme que le pilotage du système de données de santé était déficient. Elle cite, à l'appui de ce diagnostic, celui porté par M. Pierre-Louis Bras dans son rapport sur la gouvernance et l'utilisation des données de santé [(2)] et les conclusions du rapport de la commission dite open data [(3)] :

« *Le pilotage, centré sur les procédures d'autorisation, a souffert jusqu'à la période récente de l'absence d'une doctrine claire. Il est aujourd'hui éclaté entre un grand nombre d'acteurs : la CNAMTS, le COPIIR SNIIRAM (23 membres dont des représentants de l'assurance maladie, des professionnels de santé et l'État), la CNIL et son comité consultatif, le ministre chargé de la sécurité sociale et l'Institut des données de santé (IDS).*

« […] *Au final, aucune autorité n'assure suffisamment la gouvernance et le pilotage de l'ensemble du système de données, alors même que les procédures en cause sont nombreuses et complexes, voire "touffues et contestées" selon les termes du rapport d'octobre 2013* [(4)] *déjà cité.*

« *Il apparaît pourtant que le système de données de santé constitue 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.* »

---

*(1) Devenu l'article 193 de la loi n° 2016-41 du 26 janvier 2016.*

*(2) M. Pierre-Louis Bras,* op. cit.

*(3) Commission open data en santé,* op. cit.

*(4) Il s'agit du rapport de M. Pierre-Louis Bras.*

Le rapport établi par la Cour des comptes à la demande de la MECSS rappelle que le SNIIRAM a été construit sous l'empire de l'article 21 de la loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale pour 1999. Cet article a, d'une part, codifié le statut du SNIIRAM dans l'article L. 161-28-1 du code de la sécurité sociale et, d'autre part, créé un conseil pour la transparence des statistiques de l'assurance maladie dans les articles L. 161-28-2 à L. 161-28-4 du même code.

L'article L. 161-28-1 ne fixe qu'un cadre général et renvoie les modalités techniques de gestion du système à un protocole négocié entre les régimes de sécurité sociale, puis approuvé par un arrêté du ministre chargé de la sécurité sociale. Ce protocole soumettait le SNIIRAM à l'organisation habituelle d'un projet informatique. Un comité d'orientation et de pilotage de l'information inter-régimes (COPIIR) supervisait le montage du projet. Sa réalisation incombait à la CNAMTS, sous la tutelle du bureau chargé des systèmes d'information de la direction de la sécurité sociale.

La création, par l'article 64 de la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, sous la référence L. 161-36-5 du code de la sécurité sociale, d'un groupement d'intérêt public nommé Institut des données de santé (IDS) a perturbé cette organisation.

Selon le rapport établi par M. Jean-Michel Dubernard pour l'examen du projet de loi en première lecture par l'Assemblée nationale (1), la création de l'IDS était attendue par les organismes d'assurance complémentaire en santé, afin d'accroître le partage de données. Elle avait d'ailleurs été préconisée par le Haut conseil pour l'avenir de l'assurance maladie, par M. Christian Babusiaux (2) et par le conseil pour la transparence des statistiques de l'assurance maladie.

Selon M. Dubernard, « *C'est précisément ce conseil, doté d'un champ et de moyens d'action trop restreints, auquel se substitue l'Institut des données de santé. Volontiers qualifié d' "INSEE de la santé", l'institut ne devrait pourtant pas en posséder les missions d'études ; en revanche, l'objectif poursuivi est bien d'en faire un établissement collecteur et diffuseur de données bénéficiant d'une crédibilité incontestée.*

« *Sur la forme, le choix du groupement d'intérêt public apparaît des plus judicieux pour faire échanger avec souplesse des acteurs aussi différents que les caisses, les assureurs, les professionnels de santé ou les établissements. Quant au fond, les données susceptibles d'être utilisées par les membres du GIP sont bien évidemment anonymes, et protégées par la CNIL.* »

---

*(1) M. Jean-Michel Dubernard,* Rapport fait au nom de la commission spéciale chargée d'examiner le projet de loi (n° 1675) relatif à l'assurance maladie, *Assemblée nationale, XII^e^ Législature, n° 1703, 24 juin 2004.*

*(2) Christian Babusiaux, Louis Bréas, Laurence Eslous, Dominique Thouvenin,* L'accès des assureurs complémentaires aux données de santé des feuilles de soins électroniques, *Ministère de la santé, de la famille et des personnes handicapées, 26 mai 2003.*

Mis en place par une convention approuvée par un arrêté ministériel du 30 avril 2007, le groupement a travaillé presque exclusivement sur le SNIIRAM. Selon la Cour des comptes, l'IDS a « *brouillé les frontières avec le COPIIR et contribué à fragiliser le positionnement des deux instances.*

« *Ainsi, les actions de l'IDS en faveur de l'amélioration de la qualité et de la cohérence des bases de données ont donné lieu à 154 propositions d'évolution relatives aux règles de gestion, à la correction d'anomalies et l'architecture des bases.*

« *L'IDS a, par ailleurs, animé des clubs utilisateurs sur les magasins de données agrégées du SNIIRAM et sur l'EGB* [(1)]*, ainsi que sur le PMSI en tant que composante du SNIIRAM. Leur activité est telle que la CNAMTS a suspendu ses propres clubs d'utilisateurs externes pour participer, plus ou moins régulièrement, à ceux de l'IDS.* » [(2)]

Le conflit entre le COPIIR et l'IDS s'est déroulé dans l'indifférence des pouvoirs publics. Le rapport de la Cour des comptes critique « *un pilotage confus qui a conduit à la paralysie de sa gouvernance depuis 2013* » [(3)].

### *b. La loi du 26 janvier 2016 reconduit une gouvernance duale des archives de santé*

La direction de la sécurité sociale a décidé, avec la CNAMTS, de ne plus réunir le COPIIR après le 18 avril 2013, en attendant que les réflexions sur l'ouverture des données de santé aboutissent.

Elles ont abouti à l'article 193 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé qui, selon l'étude d'impact jointe au projet de loi, implique plus fortement l'État dans le pilotage stratégique du SNDS.

En même temps qu'elle affirme une reprise en main par l'État des archives pseudonymes des données de santé, l'étude d'impact explique que le projet de loi reconduit la gouvernance duale qui a opposé le COPIIR à l'IDS : « *Le projet de loi pose le principe d'un pilotage stratégique par l'État, dans le cadre d'une gouvernance qui s'appuiera sur deux piliers :*

« *– la CNAMTS à qui la loi confie le rôle d'opérateur principal du nouveau système national des données de santé (le SNDS) ;*

« *– l'Institut national des données de santé, groupement d'intérêt public prenant la suite de l'actuel IDS, qui regroupera l'ensemble des parties prenantes pour permettre l'expression des avis sur l'utilisation des données de santé en général, mais qui donnera aussi, un avis, s'il y a lieu, sur le bénéfice collectif*

---

*(1) EGB : Échantillon généraliste des bénéficiaires.*

*(2) Cour des comptes,* op. cit.*, page 22.*

*(3) Cour des comptes,* op. cit.*, page 15.*

*attendu, ou non, d'études pour lesquelles il est demandé à la CNIL une autorisation d'accès à des données personnelles.* » (1)

L'étude d'impact reconnaît aussi que « *La gouvernance du système comportera plusieurs dimensions : le pilotage par l'État des services rendus par les opérateurs du SNDS, au premier rang desquels la CNAMTS liée à l'État par une convention d'objectifs et de gestion, la production des textes réglementaires en application de la présente loi, la garantie de la sécurité du dispositif, la gestion du modèle économique du système (les données publiques seront gratuites mais il est prévu d'instaurer une redevance assise sur l'usage des données en accès restreint).*

« *Mais la gouvernance des données médico-administratives et plus largement des données de santé présente aussi d'autres aspects qui justifient la création du GIP INDS décrit dans l'ensemble constitué par la présente loi et ses textes d'application :*

« *– la concertation avec les acteurs et l'expression de leurs avis, en toute transparence, sur les modalités d'accès aux données de santé et sur les orientations, le pilotage et les résultats du SNDS ;*

« *– une instance où seront réunis des représentants des usagers, des professionnels et établissements de santé (et médico-sociaux), des organismes payeurs et de l'État se prêtera aussi à des échanges sur les informations à rendre publiques concernant l'activité des professionnels et établissements ;*

« *– l'expression d'avis et la construction progressive d'une doctrine, en concertation avec la CNIL et les autres acteurs concernés, sur la finalité d'intérêt général de certaines études pour lesquelles une autorisation d'accès est demandée à la CNIL ;*

« *La diversité des acteurs réunis au sein de l'INDS le rendra légitime pour donner un avis sur le bénéfice collectif à attendre de tel ou tel projet d'étude pour lequel l'accès à des données personnelles (déidentifiées) serait demandé ;*

« *Ce sera une instance de rapprochement des organes d'expertise et d'instruction, le GIP devant servir aussi de support au comité d'expertise scientifique mentionné à l'article 54 de la LIL et au comité national d'harmonisation des comités de protection des personnes. Réunissant ainsi en son sein les comités chargés de l'instruction des demandes d'autorisation en amont de la CNIL, il deviendra le guichet unique facilitant les démarches des chercheurs, et des autres porteurs de projets d'études.* »

---

*(1) Étude d'impact du projet de loi relatif à la santé, n° 2302, déposé sur le bureau de l'Assemblée nationale le 15 octobre 2014.*

### *c. Les décrets du 26 décembre 2016 installent un florilège de comités*

Le décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé », qui porte application de l'article 193 de la loi du 26 janvier 2016, entrera en vigueur le 1er avril 2017. En attendant l'installation de l'Institut national des données de santé, son article 2 prévoit que le comité stratégique mentionné à l'article R. 1461-10 du code de la santé publique en tienne lieu.

Ce comité comprendra des représentants des organismes responsables des bases de données alimentant le SNDS, une personnalité qualifiée et le président de l'Institut national des données de santé, auquel se substitue jusqu'à sa désignation celui de l'actuel Institut des données de santé.

Lors de son audition, M. Franck Von Lennep a indiqué que la mission « Accès aux données de santé » de sa direction, dirigée par Mme Mylène Girard et composée de quatre personnes, avait installé le comité de pilotage stratégique du SNDS dont elle assure le secrétariat. Ce comité « *rassemble les directions du ministère de la santé et les producteurs de données de santé, et se réunit trois à quatre fois par an. Il fixe les grandes lignes du projet et rend des arbitrages. Cette nouveauté – le Système national d'information inter-régimes de l'assurance maladie (SNIIRAM) n'était pas gouverné de cette façon – répond vraiment à un besoin, ce que la Cour des comptes avait d'ailleurs souligné.* » (1)

Dans sa réponse écrite aux questions du rapporteur, la DREES précise qu'y siègeraient une personnalité qualifiée et des représentants de la CNAMTS, de l'ATIH, de l'INSERM-CepiDC, de la direction de la sécurité sociale, de la direction générale de l'offre de soins, de la direction générale de la santé, de la délégation à la stratégie des systèmes d'information de santé (Secrétariat général des ministères chargés des affaires sociales), du Haut fonctionnaire de défense et de sécurité, de la direction générale de la cohésion sociale, de la DGRI et la présidente de l'IDS (puis de l'INDS) qui « *représentera tous les acteurs publics et privés dans cette instance* ».

Outre le secrétariat, la DREES indique qu'elle assurera le pilotage du comité stratégique. Elle définira les priorités stratégiques en matière de données de santé, informera des différentes évolutions et de l'avancée des décisions et arbitrera les sujets de débat.

Réuni à l'invitation des ministres chargés des affaires sociales et de la santé, ce comité doit fixer les orientations de développement du système national des données de santé, reprenant ainsi les compétences du COPIIR SNIIRAM sans que ce dernier, qui n'est plus réuni, soit pour autant supprimé.

Le même article du code prévoit que la CNAMTS réunira un « comité de pilotage opérationnel » du SNDS afin de planifier et de coordonner les actions

*(1) Audition du 20 décembre 2016.*

engagées avec des représentants de la DREES, de l'ATIH, de l'INSERM, de la Caisse nationale de solidarité pour l'autonomie et des organismes d'assurance maladie complémentaires contribuant à l'alimentation du SNDS.

La composition, les missions et les modalités de fonctionnement de ces deux comités doivent être précisées par arrêté.

L'article R. 1461-19 du code de la santé publique prévoit que l'Agence nationale de santé publique réunisse un comité des services, des établissements et organismes bénéficiant d'un accès permanent au SNDS, ouvert aux consultations du comité stratégique.

Le docteur Jean-Claude Desenclos a donné quelques éléments de contexte relatif à ce comité des utilisateurs permanents et aux conditions de sa mise en place : « *Lors des discussions qui ont eu lieu en amont, nous avions insisté pour que le comité stratégique rattaché à la DREES et qui réunit les producteurs de données et l'État, intègre également les utilisateurs, sachant que l'utilisation des données fait également partie de la définition de la stratégie.*

« *Notre demande n'a pas été entendue, mais on nous a proposé que Santé publique France anime un comité des utilisateurs rattaché à l'INDS et qui, chaque année, rapportera au comité stratégique. C'est un bon compromis, qui doit permettre une vision prospective du système et des évolutions à mettre en œuvre, qu'il s'agisse d'avancées techniques ou du choix stratégique de la définition du périmètre des bases de données.*

« *Je m'interroge en revanche davantage sur la propension qu'a le ministère de la santé à nous convoquer à haute fréquence – toutes les deux ou trois semaines – pour participer à des rencontres supposées aider à la mise en place et à la régulation du système. On ne perçoit pas toujours à quelle logique obéit cette effervescence administrative, qui nous oblige à consacrer beaucoup de temps à des réunions où nous ne faisons que répéter ce que nous avons déjà dit par ailleurs.* » (1)

Au demeurant, M. Philippe Burnel a présenté une organisation du SNDS plus riche de comités que celle décrite dans la loi du 26 janvier 2016 et assez proche de celle du SNIIRAM, critiquée par la Cour des comptes :

« *Le SNDS est conçu en trois lieux. D'abord, un lieu de pilotage stratégique, qui réunit les décideurs publics, sous la présidence de l'État, pour définir les évolutions du SNDS, identifier les bases de données à y intégrer, se prononcer sur l'opportunité d'un sous-échantillon d'accès plus facile, bref définir les règles d'alimentation et les grands principes régissant la vie du système.*

« *Ensuite, le comité des producteurs, qui rassemble les producteurs de bases de données – la CNAMTS, l'ATIH, demain les structures du secteur médico-*

*(1) Audition du 31 janvier 2017.*

*social telle la Caisse nationale de solidarité pour l'autonomie (CNSA). C'est un lieu de nature plus technique, où les acteurs s'accordent sur les formats de fichiers, les modalités de transmission, les modèles d'agrégation, la définition de délais, d'indicateurs, etc. Cet aspect est assez classique.*

« *Le troisième lieu est plus nouveau, même s'il existait déjà sous la forme de l'Institut des données de santé (IDS) : c'est l'INDS. Il est doté de deux missions que l'on a initialement envisagé de séparer, avant que la concertation au sein de la commission open data ne montre que la quasi-totalité de nos interlocuteurs souhaitaient les voir réunies.*

« *La première mission consiste à accueillir le secrétariat du comité d'experts chargé d'analyser les demandes d'accès des acteurs privés ou des administrations qui ne disposent pas d'un accès permanent, avant de les transmettre à la CNIL à laquelle il appartiendra in fine d'autoriser ou non le traitement.*

« *Le rôle du comité d'experts, qui était lui aussi déjà exercé, est assez simple dans son principe : il s'agit de déterminer si l'étude est sérieuse du point de vue méthodologique, s'il est justifié d'utiliser les données comme annoncé pour atteindre les finalités annoncées, si le nombre de données demandées n'est pas trop élevé, etc.*

« *L'idée était ensuite d'englober ce guichet d'autorisation dans une structure de concertation ou de démocratie sociale au sein de laquelle toutes les parties prenantes demeureraient représentées et qui prolongerait, en quelque sorte, la commission open data.*

« *Il était important, en effet, que perdure un lieu où tous les acteurs pourraient régulièrement dialoguer, afin d'exprimer leurs besoins – ceux des industriels, des patients, des professionnels, indépendamment de la conception propre à l'administration de l'évolution du SNDS – et de préserver et garantir l'intérêt public.* » (1)

Dans sa réponse écrite aux questions du rapporteur, la DREES indique que la gouvernance des données de santé se met en place progressivement et qu'un arrêté à son sujet est en cours d'élaboration. Elle soutient que le rôle des différents acteurs y est parfaitement clair et sans ambigüité mais précise toutefois que :

« ● *L'État assume les orientations stratégiques en matière de données de santé : la DREES pilote un comité stratégique qui réunit toutes les directions d'administration centrale concernées, les producteurs et l'IDS (puis l'INDS).*

« ● *La politique d'audit et de contrôle sera confiée, par émanation du comité stratégique, au haut fonctionnaire de défense et de sécurité qui pilotera le comité d'audit qui doit prochainement être installé.*

*(1) Audition du 13 décembre 2016.*

« ● *La CNAMTS est responsable du traitement. A ce titre :*

« *– Elle réunit les producteurs de données dans un comité [des] producteurs ;*

« *– Elle pilotera une commission [de] sécurité qui doit être prochainement installée.*

« ● *L'INDS aura pour mission de structurer et prioriser les expressions des besoins des utilisateurs au sein d'un comité utilisateurs et d'une commission d'instruction.* »

Dans sa réponse écrite aux questions du rapporteur, la CNAMTS précise que la commission d'audit et de contrôle vérifiera « *l'adéquation entre les finalités autorisées du SNDS et les autorisations données par l'INDS ou la CNIL.* »

Le comité d'audit, la commission de sécurité, le comité des utilisateurs et la commission d'instruction des demandes d'accès ajoutent quatre instances collégiales aux quatre cités par M. Brunel, le comité de pilotage opérationnel prévu par les textes pouvant s'identifier au comité des producteurs cités par les deux réponses.

***d. Le rôle de la CNAMTS reste à préciser***

Dans son rapport, la Cour des comptes constate que la CNAMTS, de gestionnaire technique, est devenue *« le seul vrai pilote du système* » [(1)] et qu'elle a noué un dialogue direct avec les utilisateurs réguliers réunis au sein de l'IDS.

En pilotant simultanément le développement et, avec le concours de l'IDS, la consultation du SNIIRAM, les départements de maîtrise d'ouvrage informatique et d'études statistiques de la CNAMTS, auquel la Cour des comptes attribue la réussite du projet, en conservaient aussi le contrôle.

La nouvelle organisation qui résulte de la loi de 2016 laisse à la CNAMTS la maîtrise technique du SNDS mais elle devra compter, comme auparavant, avec l'INDS dans le comité des utilisateurs. Interrogée par le rapporteur sur ses relations à venir avec l'INDS, la CNAMTS a sobrement répondu par écrit que « *La CNAMTS est responsable du traitement SNDS. L'INDS, quant à lui, a pour mission de : réunir l'État, les producteurs et utilisateurs des données de santé publics et privés ; veiller à la qualité des données, aux conditions de leur mise à disposition garantissant leur sécurité et facilitant leur utilisation ; assurer un secrétariat unique pour les demandes d'accès aux données de santé, hors recherches relevant de la loi Jardé [(2)] ; émettre un avis sur l'intérêt public des demandes d'accès ; faciliter la mise à disposition directe d'échantillons et jeux de*

*(1) Cour des Comptes*, op. cit.*, pages 21 sq.*

*(2) Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine.*

*données agrégées (dans un cadre homologué par la CNIL) et contribuer à l'expression des besoins pour plus de données en open data. »*

***e. La CNAMTS sous-traiterait à l'INSERM certaines fournitures d'accès***

Le paragraphe II de l'article L. 1461-1 du code de la santé publique fait de la CNAMTS le responsable du traitement des données du SNDS, dans le cadre d'orientations générales définies par l'État, en concertation avec les organismes responsables des systèmes d'information et des données. Il vise explicitement les traitements par lesquels elle réunit et organise ces données mais n'exclut pas ceux par lesquels ces données sont consultées puis réutilisées.

L'article L. 1461-7 précise qu'un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés « *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* ».

M. Claude Gissot a précisé que si la loi fait de la CNAMTS le diffuseur des données du SNDS, celle-ci n'a pas vocation à regrouper toutes ces données dans une seule base, « *ce qui signifie qu'il pourrait y avoir d'autres hébergeurs de données, notamment de données appariées. C'est ainsi que se positionne l'INSERM, qui travaille à partir de cohortes. Le CASD pourra accueillir des données issues d'un appariement associant des sources de l'assurance maladie et d'autres sources publiques. Il suffira qu'il vérifie leur compatibilité avec le référentiel de sécurité qui sera bientôt imposé.* » (1)

L'article R. 1461-3 confirme que la CNAMTS rassemble et met à disposition les données mais ajoute que l'INSERM « *peut, en tant que coordinateur national d'infrastructures de recherche utilisant des données de santé, être chargé, dans le cadre d'une convention conclue avec la Caisse nationale de l'assurance maladie des travailleurs salariés, d'assurer la réalisation des extractions et la mise à disposition effective de données du système national des données de santé, pour des traitements mis en œuvre à des fins de recherche, d'étude ou d'évaluation.* »

L'INSERM, responsable du CépiDc et du versement des données de cette base aux archives du SNDS, pourrait fournir un accès à ce système en tant que sous-traitant de la CNAMTS. Cette sous-traitance, prévue par le règlement européen, donnerait lieu à une convention qui, selon l'article R. 1461-3, « *précise le service de l'Institut chargé d'assurer ces opérations, les conditions de suivi des demandes de mise à disposition de données, des extractions de données réalisées, des personnels habilités à réaliser des extractions ainsi que les mesures de sécurité mises en œuvre*. »

*(1) Audition du 17 janvier 2017.*

Le rapporteur relève cependant que Mme Chantal Cases a limité le rôle de l'INSERM à la mise à disposition de données dans une bulle d'accès, peut-être comparable à celle du PMSI ouverte par le CASD [(1)].

### 2. Le rôle de l'INDS retient particulièrement l'attention

#### *a. L'INDS serait le secrétariat des demandes d'accès soumises à la CNIL et le comité des utilisateurs du SNDS, avec plus de moyens que l'IDS*

L'étude d'impact de l'article 47 du projet de loi de modernisation de notre système de santé [(2)] indique que *« L'INDS assurera enfin un rôle de guichet pour l'accueil et l'orientation des projets d'études ou de recherche dans une procédure d'autorisation qui demeure assez complexe et exige une assistance.* »

Le rapport établi en vue de la première lecture du projet de loi du 16 juin 2004 relatif à l'assurance maladie [(3)] voyait dans l'IDS un équivalent de l'INSEE dans le domaine de la santé tout en reconnaissant qu'il était privé des missions d'études de l'INSEE. La loi de modernisation de notre système de santé a changé l'IDS en INDS sans modifier son statut de groupement d'intérêt public ni lui donner de missions d'études.

L'article L. 1462-1 du code de la santé publique prévoit que l'INDS facilite l'exploitation statistique du SNDS mais ne la réalise pas lui-même. L'INDS n'a pas reçu la responsabilité exclusive du SNDS. Il n'est ni le dépositaire légal de cette archive publique ni son principal exploitant. Il est l'aiguillon des exploitants du SNDS.

Le rôle de l'INDS dans l'organisation décrite par M. Philippe Burnel est cependant plus délicat et plus stratégique que ce que suggère la sobre liste de ses compétences légales.

Certes, Mme Chantal Cases s'est d'abord montré rassurante : « *La loi rend l'architecture générale beaucoup plus lisible : la DREES est responsable du pilotage du système, la CNAMTS de la gestion des bases de données et le futur INDS aura pour tâche de faciliter les accès aux données et les échanges avec les utilisateurs. Le nouveau paysage est donc assez clair.* » [(4)]

Elle a ensuite expliqué que « *La seule compétence qui devra être partagée est la connaissance générale des possibilités offertes par ces bases de données et de la manière de les mettre en œuvre. Ainsi, l'INDS n'a pas pour mission de développer des compétences particulières en matière de sécurité informatique des données, mais il devra avoir les compétences suffisantes pour faire remonter les*

---

*(1) Audition du 20 décembre 2016.*

*(2) Devenu l'article 193 de la loi n° 2016-41 du 26 janvier 2016.*

*(3) M. Jean-Michel Dubernard,* Rapport fait au nom de la commission spéciale chargée d'examiner le projet de loi (n° 1675) relatif à l'assurance maladie, *Assemblée nationale, XII^e^ Législature, n° 1703, 24 juin 2004.*

*(4) Audition du 20 décembre 2016.*

*observations des utilisateurs à ce sujet. En revanche, nous devons maîtriser parfaitement les utilisations possibles des bases de données – aussi avons-nous prévu de recruter de nouveaux statisticiens – et leur circuit de transmission.*

« […] *Le futur INDS sera le lien entre tous les utilisateurs des données, publics et privés. Il est important que ces derniers participent à la réflexion sur les besoins et la mise en œuvre des accès. Déjà, l'IDS dans sa structure actuelle ne compte pas seulement des producteurs de données de santé ou des producteurs potentiels : les usagers aussi sont représentés, qui utilisent les données par l'intermédiaire de laboratoires ou de bureaux d'études. Cela étant, l'application de l'article 193 de la loi emportera une transformation profonde.* »

Dans sa réponse écrite aux questions du rapporteur, la DREES indique que l'INDS « *a vocation à assurer une fonction de secrétariat ; évaluer l'intérêt public des projets ; épauler les utilisateurs dans l'expression de leurs besoins ; favoriser le dialogue avec les producteurs de données ; prioriser les demandes des utilisateurs ; si nécessaire, soumettre les arbitrages au comité stratégique et mettre en œuvre des procédures simplifiées.* »

Elle exclut que l'INDS puisse réaliser lui-même ou se substituer aux institutions existantes pour réaliser des études et recherches à partir du SNDS puisque « *les champs concernés par ces données sont multiples. L'expertise sur ces champs est aujourd'hui répartie dans différentes institutions aux missions très différentes. Il serait illusoire de chercher à réunir toute cette expertise dans un seul institut.* »

Loin de cantonner l'INDS dans un rôle secondaire, M. Patrick Corne a pointé du doigt le problème majeur posé par la gouvernance duale du SNDS : *« Il est normal que le SNDS soit géré par la CNAMTS. En revanche, l'articulation entre le SNDS qui stocke les données et l'INDS, dont les missions sont floues est défaillante. Ce système, très complexe, n'est pas propice à un travail rapide et consensuel.*

« *La gestion du SNDS par la CNAMTS ne nous pose aucun problème. Il n'en va pas de même pour l'articulation entre l'INDS et le SNDS. Non seulement nous ignorons la place qui sera la nôtre dans la nouvelle gouvernance mais nous considérons que le filtre de l'INDS risque de créer une inertie. Je pense que nous ne sommes pas les seuls à nous en inquiéter. Les chercheurs, lorsqu'ils comprendront qu'ils ne pourront plus accéder aux données, vont réagir aussi.* » (1)

Quels que soient les contours que les textes actuels et les pratiques à venir dessineront du rôle de l'INDS et de la gouvernance duale du SNDS, la question des moyens du futur Institut ne peut être éludée. M. Christian Babusiaux s'est ainsi ému des moyens alloués l'INDS : « *J'en viens à la réalité concrète. Je dois à cet égard vous faire part de mon inquiétude. Tout d'abord, la convention constitutive de l'INDS n'a été ni créée ni strictement définie ; il est doté d'un*

*(1) Audition du 20 décembre 2016.*

*budget prévisionnel en pointillés, même si celui-ci est très ambitieux puisqu'il est question de le doubler. Est-ce justifié ? Certes, l'IDS était quelque peu à l'étroit dans son budget, mais faut-il pour autant le doubler dans les circonstances actuelles, et les partenaires y sont-ils prêts ? Compte tenu de la convention d'objectifs et de gestion (COG) de la caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS), cela ne semble guère réaliste… Ajoutons-y le départ progressif de la petite équipe de l'IDS.* » (1)

Après avoir souhaité que les laboratoires et industriels de la santé puissent « *être associés à une gouvernance dont les modalités restent à définir, qu'il s'agisse de la régulation de l'accès aux données ou de la juste représentation des industriels* », M. Philippe Maugendre, directeur des relations gouvernementales de SANOFI, a souligné : « *Nous appelons également de nos vœux une mise en adéquation des moyens humains aux tâches de l'INDS : on ne pourra faire l'économie d'équipes composées à la fois de scientifiques et de personnes à même de traiter les nombreuses demandes, en particulier du fait de l'attribution à l'Institut de la gestion de l'accès au PMSI.* » (2)

En réponse à une question posée par le rapporteur, M. Franck Von Lennep a déclaré que la transformation de l'IDS en INDS implique « *d'augmenter, probablement de plus de 50 %, le budget actuel* » (3).

Les représentants de l'actuel IDS ont confirmé les appréciations portées par les autres intervenants et brossé les grandes lignes du « format cible » qui pourrait être retenu pour le futur INDS. Ainsi, Mme Yvanie Caillé, directrice générale, a rappelé que « *L'IDS repose habituellement sur 6 équivalents temps plein (ETP) mais, depuis quelques mois, les effectifs ont diminué en raison de départs et de changements. C'est pourquoi, au 31 décembre, nous ne serons plus que 3 ETP. Des procédures de recrutement, que nous espérons efficaces, sont en cours pour reconstituer les effectifs.*

« […] *Compte tenu des nouvelles missions de l'INDS, il est prévu que nous retournions le plus rapidement possible à 6 ETP au début de 2017, pour passer à 9 ETP à la fin de la même année, et l'effectif devrait se stabiliser autour de 12 personnes en 2018.*

« […] *Même si l'on peut parler de continuité, nous sommes en phase de création d'une nouvelle structure, avec de nouvelles missions, et un certain nombre de changements vont intervenir. Nous nous laissons donc la possibilité de voir comment les effectifs évolueront, et s'ils permettent de répondre à ces nouvelles missions.* »

Mme Chantal Cases a complété ce propos en mettant en parallèle les besoins en effectifs supplémentaires et la nature des tâches que devra assumer le

*(1) Audition du 17 janvier 2017.*

*(2) Table ronde du 24 janvier 2017.*

*(3) Audition du 20 décembre 2016.*

futur institut : « *Je pense que cet effectif de 12 personnes, à moyen terme, est raisonnable. En effet, l'INDS aura à gérer le flux des demandes et – comme l'IDS d'ailleurs – à faciliter l'accès aux données et l'institution d'un dialogue entre les utilisateurs, les utilisateurs et les producteurs, en organisant des groupes de travail et des commissions. Cela étant, je passe sur d'autres missions de l'INDS, sur lesquelles on reviendra et qui nécessiteront aussi des moyens.*

« *Quoi qu'il en soit, nous n'allons pas réaliser, concrètement, des extractions de données. Nous allons faciliter les choses, mettre en place des réflexions, des analyses sur les besoins, la qualité et les retours d'expérience des utilisateurs. Tout cela ne nécessite pas forcément de nombreuses personnes, mais une bonne organisation avec les partenaires de l'INDS. C'est pour cette raison que les moyens paraissent relativement limités. Les plateformes d'accès aux données seront séparées, se trouveront ailleurs, et utiliseront d'autres moyens.* »

***b. L'INDS serait aussi une instance de la démocratie sanitaire développant une doctrine de l'intérêt public***

En assurant le secrétariat des demandes d'accès occasionnelles au SNDS et l'instruction de leur intérêt public, l'institut sera une instance de contrôle au sens du règlement européen, presque concurrente de la CNIL et, comme l'a expliqué M. Philippe Burnel, une instance de démocratie sanitaire dialoguant avec le CEREES et les organismes publics compétents : *« Les associations de patients, en particulier, craignaient que la séparation entre les experts, d'une part, et la démocratie sanitaire, de l'autre, n'encourage les experts à privilégier les recherches conduites par des scientifiques, de grande qualité méthodologique, au motif que le progrès des connaissances est en soi une finalité d'intérêt public.*

« *Les objectifs poursuivis par les patients, légitimes mais formalisés de manière moins experte, risquaient ainsi d'être pénalisés par la dichotomie entre les deux structures. D'où l'idée de réunir les uns et les autres pour mettre les experts en relation avec des interlocuteurs qui les laisseront juger de l'aspect méthodologique, mais pourront faire valoir auprès d'eux la contribution à l'intérêt public d'un dossier, même mal ficelé, et leur suggérer de donner des conseils au demandeur pour l'améliorer.*

« *Ma conviction personnelle est que cette notion d'intérêt public, dont la définition est par nature ouverte, va évoluer et faire peu à peu l'objet d'une jurisprudence au sein de l'INDS. Nous en aurons probablement une conception plus large dans trois à cinq ans.* »

M. Nicolas Revel a, lui aussi, relevé la place centrale de l'INDS dans la construction progressive d'une « doctrine » de l'intérêt public au regard de l'accès aux données de santé : « *Des divergences d'appréciation peuvent survenir, entre les opérateurs souhaitant accéder au SNIIRAM et l'INDS, sur la notion d'intérêt public de leurs sujets d'étude. Nous n'avons pas eu à connaître à ce jour de telles difficultés. Dans le domaine de la santé, l'intérêt public ne se réduit pas au fait*

*d'être une personne morale de droit public ; de nombreux enjeux sanitaires ou d'efficience médico-économique peuvent être portés par des opérateurs de toute nature. C'est pourquoi la loi a souhaité identifier de manière précise deux finalités interdites, au-delà desquelles le champ est potentiellement ouvert.* » (1)

Dans le même registre, mais sur une tonalité légèrement différente, M. Christian Babusiaux s'est interrogé sur la portée juridique du critère d'intérêt public et a souligné les risques juridiques que font peser les incertitudes actuelles : « *Qu'est-ce que l'intérêt public ? Nous en percevons intuitivement la nature mais, génération après génération, sa définition juridique reste en débat. N'y a-t-il pas là un potentiel nid à contentieux, alors que le système devrait plutôt être conçu de manière fluide et efficace dans l'intérêt des acteurs qui seront habilités à accéder aux données ? À cet égard, le ministère de la santé et l'IDS ont créé un groupe pour réfléchir à la définition de l'intérêt public, notamment au moyen d'un questionnaire, au demeurant très bien fait. C'est dire l'incertitude qui entoure cette notion retenue par le législateur.* » (2)

### *c. La participation des industriels et des syndicats de professionnels aux travaux de l'INDS est possible*

La composition de l'INDS est du domaine réglementaire. Elle suscite autant d'intérêt que d'interrogations, que M. Christian Babusiaux a exprimées avec une vigueur certaine :

« *Nous ignorons quelle sera la composition exacte de l'INDS ; à ma connaissance, elle n'est toujours pas précisée. Mme la ministre de la santé a indiqué que, fort de ses treize composantes, elle serait plus large que celui de l'IDS : cette ambition est compréhensible et louable, mais quel en sera le périmètre exact ? La loi du 13 août 2004 relative à l'assurance maladie avait précisé les contours de ce qui est devenu l'IDS en 2007. L'article 193 de la loi du 26 janvier 2016 ne fixe aucun périmètre clair.*

« *Il semble par exemple que l'on envisage d'y inclure les entreprises pharmaceutiques. À titre personnel, je me suis permis, lors de l'élaboration de la loi, de déconseiller cette participation : il me semble en effet qu'introduire les laboratoires pharmaceutiques ou leurs organisations dans le processus d'autorisation d'accès aux données est non seulement une erreur technique, mais aussi une faute politique.*

« *On nous indique que le LEEM – le syndicat des entreprises du médicament – et ses adhérents ne seront pas totalement membres de l'INDS. Un groupement d'intérêt public (GIP) peut-il donc se composer de membres et de demi-membres ? Cela ne poserait-il pas un problème statutaire ? On commencerait, semble-t-il, à s'en apercevoir…*

---

*(1) Audition du 17 janvier 2017.*

*(2) Audition du 17 janvier 2017.*

« *De même, nous ignorons si les complémentaires de santé en feront ou non partie, et si elles seront représentées par leur union, l'UNOCAM, ou bien, celle-ci n'ayant pas de vocation législative, par les fédérations la composant. En somme, deux ans et demi après que le Conseil des ministres ait approuvé le projet de loi, à la fin de l'été 2014, le périmètre de l'INDS demeure incertain.* » (1)

L'article L. 1462-1 du code de la santé publique qui instaure le GIP INDS y associe « *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.* »

L'association des assureurs complémentaires à l'INDS semble liée à l'exécution de la convention, prévue par l'article L. 1461-1, de versement au SNDS d'un échantillon convenu de leurs données d'assurance maladie, à moins qu'ils ne soient comptés parmi les utilisateurs privés de données de santé.

Selon M. Philippe Maugendre, « *Il va ainsi falloir mettre en place la convention constitutive du GIP de l'INDS – qui jouera le rôle de guichet unique pour le traitement des demandes d'accès – et nous attendons d'être associés à une gouvernance dont les modalités restent à définir, qu'il s'agisse de la régulation de l'accès aux données ou de la juste représentation des industriels.* » (2)

Précédemment, M. Patrick Corne avait expliqué que « *l'UNPS siégeait en tant que fournisseur de données, aux côtés de l'État et de la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS), au comité d'orientation et de pilotage d'information inter-régimes (COPIIR) du Système national d'information inter-régimes de l'assurance maladie (SNIIRAM).*

« *De ce fait, nous participions à la gouvernance du SNIIRAM et, surtout, nous pouvions déterminer nos accès à la base de données et gérer la délivrance des habilitations qui nous est confiée par la loi. Le COPIIR a disparu et doit être remplacé par le Système national des données de santé (SNDS).*

« *Or, même si nous attendons toujours les décrets, nous ignorons quelle place nous sera réservée au sein de la gouvernance de cette nouvelle instance. Cependant, il semble que nous serons considérés comme utilisateur et que nous n'aurons droit, à ce titre, qu'à un strapontin.* » (3)

Le rapporteur appuie la demande implicite de l'UNPS, tout en considérant qu'il faut être prudent quant aux modalités de participation des industriels et des syndicats de professionnels aux travaux de l'INDS en particulier, au fonctionnement du SNDS en général. Sans faire de procès d'intention, il faut se garder de voir des décisions relevant par essence de l'exercice régalien des

*(1) Audition du 17 janvier 2017.*

*(2) Audition du 24 janvier 2017.*

*(3) Audition du 20 décembre 2016.*

pouvoirs de l'État orientées par des considérations qui ne seraient pas exclusivement guidées par la recherche de l'intérêt général.

### D. SANS MODÈLE ÉCONOMIQUE, L'EXPLOITATION DU SNDS REPOSE SUR DES FINANCEMENTS LIMITÉS OU INTÉRESSÉS

#### 1. L'exploitation du SNDS est coûteuse pour la CNAMTS et son alimentation l'est pour les autres producteurs de données

Dans son rapport remis à la MECSS, la Cour des comptes souhaitait que le SNIIRAM fasse l'objet d'une comptabilité et d'un financement distincts dans le parc informatique de la CNAMTS, afin d'équilibrer son exploitation par « *un modèle économique qui permette de trouver les ressources nécessaire à son développement* » (1).

Selon la Cour, « *En raison de sa nature de dispositif dérivé des systèmes de liquidation de l'assurance maladie, les coûts de développement et de sécurisation du SNIIRAM ont jusqu'à présent intégralement été couverts par la CNAMTS. Toutefois, des investissements considérables doivent être anticipés pour sa sécurisation, le développement du nouveau SNDS, le développement et sa maintenance.*

« *Ces coûts seront nécessairement élevés, en raison, on l'a vu, des enjeux de sécurité inhérents aux très grandes bases de données à caractère personnel, aux besoins très lourds de mise à niveau à moyen terme de la sécurité du SNIIRAM, ou encore aux investissements matériels et humains nécessaires à la construction des bases de données du secteur médico-social et des organismes d'assurance maladie complémentaire.*

« *À cela s'ajoutent les coûts récurrents engendrés par la mise à disposition avec une fréquence en forte hausse des données et l'accompagnement des utilisateurs.* »

Aux dépenses du SNIIRAM s'ajoutent, pour la CNAMTS et l'INSERM, celles d'hébergement et de traitement des autres sources de données du SNDS. Leurs producteurs doivent aussi s'acquitter des frais liés à l'anonymisation et au versement périodique de leurs données.

Le rapport de M. Pierre-Louis Bras estimait à 10 millions d'euros le montant des travaux d'urbanisation du système d'information qui supporte la base de données. Il n'a pu estimer les coûts d'exploitation du système ni répartir ceux-ci entre les opérateurs (2). Faute de pouvoir quantifier le modèle économique de cette exploitation, il recommandait de privilégier une tarification des études et des

*(1) Cour des comptes,* op. cit., *pages 110 à 116.*

*(2) M. Pierre-Louis Bras,* op. cit., *page 72*

recherches « *permettant d'assurer une évolution des moyens consacrés à la base en fonction des demandes* » [(1)].

Le modèle économique du SNDS a donné lieu à un échange de vues au cours de la table ronde des acteurs de l'assurance maladie organisée le 17 janvier 2017. Le dialogue entre le rapporteur et M. Nicolas Revel a permis d'apporter des éclairages substantiels.

M. Nicolas Revel. « *Jusqu'à présent, il n'était pas nécessaire d'afficher le coût du SNIIRAM. Mais, dès lors que nous nous engageons dans une réflexion sur l'opportunité de faire payer les acteurs qui souhaiteront accéder au SNIIRAM – la question n'est pas tranchée à ce stade –, nous n'aurons pas de grande difficulté à établir ce coût, qui pourra servir de fondement à l'application d'une éventuelle redevance. Celle-ci n'aurait d'ailleurs pas vocation à couvrir la totalité des charges, puisque la CNAMTS utilise elle-même beaucoup le SNIIRAM.* »

M. le président Pierre Morange, rapporteur. « *Ainsi que je l'ai indiqué au cours d'auditions précédentes, le modèle économique doit garantir l'efficience du système, et je suis résolument partisan de la perception d'une taxe. D'après les chiffres que nous a communiqués son directeur lorsque nous l'avons auditionné, le CASD, qui met notamment à disposition les données du PMSI, demande une contribution moyenne de 800 euros par utilisateur et par an, pour un coût réel de 1 200 euros, qui comprend notamment les dépenses de sécurité informatique.* »

M. Nicolas Revel. « *Nous aurons à réfléchir à la couverture probablement partielle – de même que dans l'exemple que vous venez de citer – des coûts que nous supportons, certains étant liés à l'augmentation de l'effort de sécurisation nécessaire du fait de l'ouverture accrue du système.*

« *Cette ouverture accrue implique aussi un effort d'accompagnement des futurs utilisateurs de la part de la CNAMTS, car les données du SNIIRAM, dont la base est le remboursement des soins, ne se lisent pas au premier coup d'œil : chaque fois qu'un nouvel accès au SNIIRAM, permanent ou provisoire, est autorisé, la CNAMTS forme l'acteur concerné à son utilisation.*

« *Cet accompagnement va d'ailleurs parfois au-delà de la simple formation. La question d'un investissement de notre part dans les ressources et les compétences humaines pour accompagner les futurs utilisateurs va se poser. Cet investissement aura un coût. La question de savoir comment nous le finançons pourra être intégrée à la réflexion sur le modèle économique.* »

Le directeur général de la CNAMTS a ajouté que celle-ci souhaitait que la réflexion sur le modèle économique aboutisse dans le courant de l'année 2017.

Sollicité à son tour, M. Alain Pelc a présenté successivement le point de vue de la Caisse centrale de la Mutualité sociale agricole et quelques réflexions

---

*([1]) M. Pierre-Louis Bras,* op. cit.*, page 72*

personnelles : « *Concernant le modèle économique, il nous a semblé important d'éviter les redondances, tout au moins pour l'alimentation de la base de données. C'est pourquoi la MSA a profité de la mise en place du SNIIRAM pour revoir complètement ses flux de production de données, de manière à n'avoir qu'un seul flux.*

« *S'agissant du modèle économique général, la question de l'accès aux données est très importante. En tant que statisticien et à titre personnel – mes propos n'engagent pas la MSA –, je suis un fervent défenseur de la gratuité de l'accès aux données, dès lors que sont respectées la loi du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques et la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cela n'empêcherait pas de prévoir une contribution à la production de données, sous certaines conditions, lorsque les demandes vont au-delà de l'usage courant.* »

Aux coûts de la collecte, de l'hébergement et de la mise à disposition des données s'ajoutent aussi, pour les finances publiques, les coûts d'instruction des demandes d'accès et de contrôle des traitements opérés, supportés par la CNIL et l'INDS, ainsi que l'indemnisation des membres du CEREES qui examinent l'intérêt scientifique des demandes.

M. Franck Von Lennep est convenu que ces coûts devraient être pris en compte dans la construction du modèle économique du SNDS : « *Tout cela suppose des moyens pour le CEREES comme pour l'INDS. Nous l'avons toujours dit depuis que nous avons commencé à préparer le texte. En d'autres termes, le comité d'expertise doit être suffisamment étoffé et ses experts un tant soit peu rémunérés pour un travail qu'ils font généralement en dehors de leur activité professionnelle, très souvent le week-end, et auquel ils consacrent plusieurs heures dès lors que le dossier est un peu compliqué, sans compter les réunions au cours desquelles ils en discutent ensemble.*

« *Il faut donc une vingtaine d'experts indemnisés – nos discussions à ce sujet avec le ministère de la recherche sont en bonne voie – et un INDS doté d'un budget suffisant pour recruter des équipes d'experts de bon niveau ; la présidente et la directrice de l'IDS, que vous allez auditionner après nous, y œuvrent. Nous y travaillons naturellement avec elles et nous sommes en train d'évaluer les moyens dont l'INDS aura besoin, compte tenu du flux prévisible de dossiers, pour respecter les délais auxquels nous nous engageons.* » (1)

### 2. Les recettes d'exploitation seront limitées faute d'édition et de distribution sur abonnement de résultats comparables aux publications de l'INSEE

La Cour des comptes reconnaît que la loi ouvre peu de possibilités à la CNAMTS de tirer du SNDS des recettes d'exploitation : « *Le choix du législateur*

*(1) Audition du 20 décembre 2016.*

*d'inscrire le SNDS dans une politique plus large d'ouverture et de gratuité de l'accès aux données restreint* de facto *ces possibilités, sans les interdire pour autant*. » (1)

***a. Le statut juridique du SNDS fera échapper celui-ci aux règles de communication des informations publiques***

i. Le cadre légal de l'*open data* ne s'applique qu'aux informations publiques

La loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public modifie 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. Selon la Cour des comptes, elle « *opère un changement de paradigme : la réutilisation des informations publiques est désormais libre et gratuite, sauf exceptions encadrées par un double filtre.*

« *Ne peuvent mettre en place des redevances que les administrations au sens de la loi du 17 juillet 1978 relative à la liberté d'accès des documents administratifs et à la réutilisation des informations publiques ("loi CADA") tenues de couvrir par des recettes propres une part substantielle des coûts liés à l'accomplissement de leurs missions de service public.*

« *De plus, le produit total du montant de cette redevance ne peut dépasser le montant total des coûts liés à la collecte, à la production, à la mise à disposition ou à la diffusion des informations publiques.*

« *Un décret en Conseil d'État fixera la liste des catégories d'administrations autorisées à établir des redevances. Mais, il apparaît d'ores et déjà que la CNAMTS pour la gestion technique du SNIIRAM et du SNDS ni la DREES n'y seront pas autorisées.* » (2)

La Cour constate cependant que la loi du 28 décembre 2015 ne s'applique qu'aux informations publiques au sens de la loi CADA, dont les dispositions ont été reprises dans le code des relations entre le public et l'administration par l'ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration, entrée en vigueur le 1er janvier 2016.

L'article L. 300-2 de ce code définit comme document administratif les documents produits ou reçus par des personnes morales dans le cadre de leur mission de service public. Ces documents sont communiqués de droit à toute personne ou sont publiés, et les informations qui en sont extraites deviennent, par l'article L. 321-1 du même code, des informations publiques.

---

*(1) Cour des comptes*, op. cit, *page 111*.

*(2) Cour des comptes*, op. cit, *page 112*.

Ces dispositions doivent être composées avec celles du titre III du livre I[er] du code du patrimoine sur le dépôt légal et du livre II du même code sur les archives, en particulier les articles L. 212-3 et L. 213-2, que ni le code des relations entre le public et l'administration ni le rapport de la Cour des comptes ne mentionnent.

Le code de la santé publique, modifié par la loi du 26 janvier 2016, n'est guère précis quant au régime juridique des données du SNDS. Le statut de ce système national doit être considéré de quatre points de vue : celui de l'origine de production des données, celui de la nature des informations qu'elles révèlent, publiques ou privées, voire couvertes par un secret, celui de la personnalité morale de leur hébergeur et celui des traitements qu'elle subisse depuis leur collecte.

ii. Certaines données du SNDS sont produites par des personnes privées

Les données du SNIIRAM et du PMSI produites par des personnes morales de droit public, en particulier les établissements publics de santé, relèveraient du domaine public, de même que les données obtenues des groupements d'intérêt public gérant une MDPH et celles du CépiDc.

En revanche, le statut des données du SNIIRAM produites par des professionnels de santé exerçant dans le secteur libéral, en ville ou en établissement, et celui des données obtenues des établissements de santé privés peuvent être rapprochés de celui des données provenant des assureurs complémentaires. Il n'est pas exclu qu'elles doivent être considérées comme des archives privées soumises à une obligation légale de dépôt par l'article L. 1461-1 du code de la santé publique.

Collectées par la CNAMTS, établissement public à caractère administratif disposant d'une personnalité morale distincte de l'État, les données du SNDS ne seront pas exclusivement hébergées et communiquées par elle. L'article L. 1461-7 renvoie à un décret en Conseil d'État, pris après avis de la CNIL, le soin de désigner les organismes chargés de gérer la mise à disposition effective des données du système national des données de santé et les données permettant une identification directe des personnes. Ce décret doit déterminer leurs responsabilités respectives.

Or l'article R. 1461-3 codifié par le décret n° 2016-1871 du 26 décembre 2016 – qui entrera en vigueur le 1[er] avril 2017 – ne précise pas ces responsabilités. Il attribue la gestion du SNDS et des clés de réidentification à la CNAMTS mais son paragraphe II autorise les « *organismes gérant les composantes* » du SNDS à continuer de les mettre à disposition.

En septembre 2013, M. Pierre-Louis Bras relevait déjà qu'une confusion s'était installée entre la gestion du SNIIRAM par la CNAMTS et la propriété de la base de données [(1)]. Il préconisait de définir l'ensemble de la base comme un bien

*(1) M. Pierre-Louis Bras,* op. cit.*, page 48*

public, placé sous l'autorité du ministre chargé de la santé et sous le contrôle du Parlement.

La confusion relative aux droits de propriété du SNIIRAM atteint le SNDS. Non seulement la CNAMTS n'est que l'opérateur légal du SNDS et non son propriétaire, mais l'INSERM dispose, par le paragraphe II de l'article R. 1461-3, d'un droit conventionnel d'extraction et de « *mise à disposition effective* » de certaines données en sus de celles du CépiDc, qu'il produit.

Le référentiel de sécurité en cours de rédaction pourrait en outre confier l'hébergement de données à des tiers en vue de leur communication à distance, par un réseau ou un accès sécurisé.

iii. Les données collectées contiennent quelques informations déclarées publiques par la loi

Même si les données du SNDS étaient reconnues comme des archives publiques ou privées mais d'intérêt public au sens du droit européen, il ne s'agirait pas nécessairement d'informations publiques.

L'article L. 1461-2 du code de la santé publique ne qualifie d'informations publiques, par référence au code des relations entre le public et l'administration, que les données relatives à l'activité des professionnels de santé publiées par les organismes gestionnaires des régimes obligatoires de base d'assurance maladie.

iv. La plupart des données individuelles du SNDS sont couvertes par le secret médical mais un procédé d'anonymisation peut en extraire des informations publiques

La Cour des comptes établit une distinction entre des données agrégées et les données individuelles, à la lecture des articles L. 1461-2 et L. 1461-3 du code de la santé publique. Elle admet que les secondes puissent être modifiées de telle sorte que l'identification directe ou indirecte de la personne concernée par chaque enregistrement soit impossible. Seules celles qui seraient encore réidentifiantes conserveraient un caractère personnel qui les exclurait des informations publiques.

La Cour suggère cependant que cette distinction n'est pas celle retenue par le droit européen, qui substitue à l'anonymat des données – déclaré à l'issue d'un traitement homologué – une simple présomption – exposée à la démonstration d'une preuve contraire – que des données ne présentent aucun risque de réidentification.

Passer d'une déclaration ou d'une reconnaissance du caractère anonyme, donc public, d'une information à une présomption fragilise le régime juridique de l'*open data.* En effet, le traitement et la publication de données ne suffisent plus à garantir le caractère public de l'information qui en est extraite. Un retrait de publication peut être exigé ou une interdiction d'exploitation voire de citation instaurée dès que la preuve d'une réidentification est apportée.

Cette simple présomption est particulièrement fragile lorsque les données communiquées le sont par exception au secret médical, puisque, comme le rappelle la Cour des comptes, les données individuelles du SNDS sont « *de nature à porter atteinte à la vie privée ou au secret médical, ce qui justifie des procédures d'accès particulièrement contraignantes et leur communication ne constitue donc pas un droit.* »

La levée du secret qui les couvre, même si elle est possible et d'usage courant, obéit à des procédures particulières et motivées qui suffisent à exclure que la communication des données protégées soit un droit au sens de l'article L. 321-2 du code des relations entre le public et les administrations.

Parmi les données du SNDS, celles qui ont conservé un caractère personnel et celles qui sont couvertes par un secret protégé par loi ne sont pas des informations publiques et leur communication peut donc être payante.

***b. Le code de la santé publique distingue trois catégories de données, ayant chacune leur régime juridique et tarifaire de communication***

Les articles L. 1461-2, L. 1461-5 et R. 1461-5 du code de la santé publique rendent certains accès au SNDS gratuits indépendamment de la distinction posée par les 1° et 2° du paragraphe I de l'article L. 1461-3 entre accès permanents et accès occasionnels. L'accès permanent n'implique pas un accès gratuit ; de même, des accès occasionnels pourraient être gratuits ou payants.

C'est d'abord la nature des données – en particulier les traitements opérés pour que les personnes concernées ne soient plus identifiables – qui emporte leur régime juridique et tarifaire de communication. Le statut du demandeur entre ensuite et secondairement en ligne de compte.

i. La consultation est gratuite pour toutes les données agrégées ou anonymes

Les articles L. 1461-2 et R. 1461-5 du code de la santé publique rendent gratuite la mise à disposition et la réutilisation des données pseudonymes agrégées et des données rendues anonymes du SNDS, en précisant que la réutilisation de ces données ne peut avoir ni pour objet ni pour effet d'identifier les personnes concernées. Cette précision paraît être contradictoire avec leur caractère anonyme allégué et renforcer l'interprétation selon laquelle cet anonymat n'est que présomptif ; elle vise cependant à interdire les croisements et appariements avec d'autres données personnelles non issues du SNDS qui permettraient, sous réserve de traitements suffisamment « puissants », de remonter à l'identité des personnes.

La Cour des comptes souligne que, « *En l'état, la notion de donnée ne "présentant aucun risque de réidentification" a pour conséquence que, compte tenu des travaux de la DREES et de la doctrine de la CNIL, ni l'accès à l'EGB, ni l'accès au DCIR, ne seront concernés par cette disposition.*

« *Seraient par contre concernées l'ensemble des données agrégées présentes dans les* datamarts, *pour certains desquels la CNAMTS s'est par ailleurs d'ores et déjà engagée dans une politique de mise à disposition du grand public. Toutefois, le périmètre exact de ces données mériterait d'être précisé, car certaines extractions des bases individuelles pourraient probablement rentrer dans ce champ, en fonction des variables choisies.* » (1)

Le régime de mise à disposition gratuite concernerait également, selon l'article L. 1461-2 du code de la santé publique, « *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.* »

ii. Les consultations de données semi-agrégées sont gratuites pour les personnes qui répondent à une demande des autorités et pour les services publics administratifs

Serait également gratuit, en application de l'article L. 1461-5, l'accès aux données de santé autres que celles mentionnées à l'article L. 1461-2 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.* »

Selon la Cour des comptes, le premier cas concernerait « *les études en vie réelle des médicaments ou produits de santé, réalisées par les laboratoires pharmaceutiques à la demande de la HAS ou de l'ANSM* ». Les accès seraient gratuits, que les consultants soient de droit public ou privé.

La distinction est aisée à opérer dans les demandes d'accès occasionnelles puisque la preuve d'une requête de l'autorité publique à l'origine de la demande peut être apportée. Mais elle est plus délicate pour les personnes disposant d'un accès permanent à la base de données, soit par décret, soit par souscription d'un accord-cadre pour l'accès aux données les plus usuelles.

Chaque traitement devrait alors être déclaré par l'opérateur et recensé par le système comme répondant à une demande des autorités ou étant à l'initiative de l'opérateur. Ce procédé tempérerait la simplicité d'un dispositif visant à mettre les bases à la disposition des mêmes opérateurs de droit privé contre redevance.

Le second cas de gratuité, pour les besoins exclusifs de services publics administratifs, recoupe en partie le premier et en partie aussi la liste des opérateurs disposant d'un accès permanent à la base par décret mais nombre d'entre eux sont des établissements ou services à caractère scientifique et technologique et non à caractère administratif. Les unions régionales de professionnels de santé sont des organismes professionnels régis par le décret n° 2010-585 du 2 juin 2010 mais pas des services publics administratifs.

---

*(1) Cour des comptes,* op. cit., *page 111.*

M. Dominique Martin a évoqué un changement législatif qui rendrait payante pour les opérateurs publics la consultation du SNDS afin d'en dresser une comptabilité analytique qui permette d'anticiper et de couvrir les investissements requis, comme le souhaite la Cour des comptes : « *En ce qui concerne les opérateurs publics,* […]*, nous avons accès aux informations de manière totalement gratuite. Certes, nous mobilisons des moyens et des emplois pour conduire les requêtes, ce qui représente un coût pour l'établissement et pour la collectivité. Mais l'agence ne rémunère pas la CNAMTS pour accéder aux données.*

« *Peut-on imaginer que, demain, des opérateurs publics comme nous doivent le faire ? L'opération serait neutre si on nous allouait les subventions correspondantes ; mais, dans ce cas, on tournerait en rond du point de vue macroéconomique, que ces subventions viennent de l'État ou qu'elles émanent de redevances, ce qui nous maintiendrait dans l'environnement de la sécurité sociale et reviendrait à faire circuler de l'argent : cela ne paraît guère sensé.* » (1)

L'argument d'une « circulation » inutile des deniers publics entre personnes publiques peut effectivement être entendu comme facteur de complexité administrative, même si l'exercice de « vérité des coûts » n'est pas dépourvu de tout intérêt.

iii. L'accès des consultants privés aux données individuelles des patients pourrait leur être facturé mais les règles de tarifications restent à définir

La troisième et dernière catégorie correspond aux données individualisées du SNDS, qu'elles soient ou non chaînées pour regrouper l'ensemble des actes dispensés au patient ou acquittés par l'assuré qui le couvre.

L'accès à ces données serait en tout état de cause gratuit pour les personnes publiques visées par l'article L. 1461-5 du code de la santé publique. Il pourrait être payant pour les autres.

Tout en soulignant l'incertitude créée par le silence de la loi, M. Philippe Burnel a évoqué cette seconde possibilité : « *La loi ne dit pas que l'accès aux données sera payant mais ne dit pas non plus qu'il sera gratuit : la question n'est pas tranchée. Dans l'état actuel de la réflexion – mais je vous renvoie une fois encore à mon collègue Franck Von Lennep sur ce point –, l'accès serait gratuit pour les acteurs publics, pour éviter des complications inutiles puisque les faire payer reviendrait à ce qu'ils se paient eux-mêmes ; en revanche, il ne me paraîtrait pas illégitime que les acteurs privés contribuent aux coûts marginaux de l'ouverture.* » (2)

La Cour des comptes estimait toutefois que les possibilités de tarification étaient doublement restreintes : « *d'une part parce qu'elles ne peuvent intervenir*

*(1) Audition du 31 janvier 2017.*

*(2) Audition du 13 décembre 2016.*

*que dans un nombre limité de cas, et d'autre part parce que le montant de la redevance qui pourrait être instaurée est encadré* » (1).

Elle ajoutait que « *dans un contexte marqué par une volonté constante des pouvoirs publics d'encourager la mise à disposition et la réutilisation gratuite des données, les possibilités de mettre en place une valorisation des données du SNDS doivent tenir compte d'un principe général de non enrichissement des administrations et des établissements publics qui limiterait le produit total des tarifications à la couverture des coûts. C'est ce qui a été introduit pour les données du secteur des transports nécessaires à l'information du voyageur, par la loi pour la croissance, l'activité et l'égalité des chances économiques du 6 août 2015.* »

L'étude d'impact du projet de loi de modernisation de notre système de santé était réservée sur la facturation des consultations du SNDS. Elle excluait de faire contribuer financièrement les utilisateurs du SNDS par une taxe, qui aurait été assise à la fois sur le nombre d'études basées sur l'accès au SNDS acquises par l'entreprise taxée et sur le chiffre d'affaires de celle-ci : « *Cette option n'a pas été retenue car la technique de la redevance, payée par les seuls organismes utilisateurs des données, quelle que soit leur nationalité était applicable, plus juste et plus souple*. » (2)

Elle écartait aussi une redevance portant sur l'avantage économique induit par l'accès au SNDS pour les utilisateurs de ses données, lesquels peuvent tirer un parti considérable de leur exploitation, notamment en termes d'augmentation du potentiel commercial des médicaments dont les effets sanitaires bénéfiques auront été étayés par les études effectuées sur une base de données publique riche et fiable : « *Cette option n'a pas été retenue car elle comportait un élément de fragilité juridique à travers la rupture du principe d'égalité qu'elle impliquait, bien que cette rupture puisse être, dans certains cas, compatible avec le droit. Elle supposait aussi qu'on sache mesurer l'avantage économique en question, ce qui risquait de donner lieu à des difficultés et des contentieux.* »

Si l'on peut adhérer à la recommandation formulée par la Cour des comptes, qui appelle à inventer un dispositif financier « *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* » (3), le rapporteur note que les contours d'un tel dispositif ne sont guère précisés et que les exemples étrangers cités à l'appui de la recommandation de la Cour doivent être considérés selon les régimes de droits d'auteurs et d'édition en ligne applicables.

---

*(1) Cour des comptes,* op. cit., *page 112.*

*(2) Voir http://www.assemblee-nationale.fr/14/projets/pl2302-ei.asp.*

*(3) Cour des comptes,* op. cit., *page 116.*

### *c. L'équilibre économique du SNDS reste à trouver*

La Cour des comptes explique de façon détaillée dans son rapport que la soutenabilité financière du SNDS n'est pas garantie, compte tenu de la multiplicité des facteurs à prendre en compte : « *Le modèle économique du SNDS à construire doit ainsi chercher à couvrir les coûts associés à la mise à disposition sécurisée des données et aux contraintes spécifiques du SNDS, tout en proposant un système qui répond en termes de qualité et d'efficacité aux attentes des utilisateurs.*

« *Une offre de base, de qualité, doit certes être accessible gratuitement, pour ne pas décourager les utilisations du SNDS. Mais cet objectif devrait s'accompagner d'une réflexion plus large qui permettrait, dans le cadre du champ autorisé de tarification, de faire financer le système et son développement, par les acteurs qui en bénéficient et pourraient, à terme, en tirer profit.*

« *Ainsi, au-delà de la question cruciale de la couverture des investissements de sécurisation et de développement du SNDS, des modalités de financements complémentaires sont à articuler : d'une part, une tarification des travaux de mise à disposition des données couvrant leurs coûts spécifiques et d'autre part, le financement de l'accompagnement des utilisateurs.*

« *Faire financer les travaux de mise à disposition des données par les utilisateurs (réalisation d'extraction spécifiques, construction de requêtes presse-boutons…) pourrait reposer sur des facturations juridiquement différenciées en fonction de la nature du demandeur, de la demande formulée (quantité de données, type de données, fréquence de mise à disposition) ou de l'usage fait des données. Ces financements viendraient alimenter les budgets des organismes en charge de la mise à disposition des données.* » (1)

Les représentants de la DREES ont également souligné la difficulté de l'exercice, qui fait d'ores et déjà l'objet de réflexions approfondies de la part des administrations concernées. M. Franck Von Lennep a, par exemple, mis en évidence le lien étroit entre le modèle économique à construire et les besoins des utilisateurs : « *La convention d'objectifs et de gestion (COG) actuelle de la CNAMTS comprend pour la première fois un chapitre consacré aux données de santé, avec des moyens spécifiques. La prochaine COG ne sera discutée qu'en 2017, mais la question des moyens dédiés à la gestion des données de santé est d'ores et déjà soulevée.*

« *Il faudra traiter la question des outils technologiques et de la sécurité – le SNDS devra de toute façon répondre aux besoins de sécurité établis par le référentiel – mais aussi celle de l'accompagnement des utilisateurs et des services qui leur seront proposés.*

« *Vous évoquiez la question du modèle économique. Faut-il tout financer sur les fonds alloués à l'ATIH et à la CNAMTS, ou pouvons-nous prévoir un*

*(1) Cour des comptes,* op. cit.*, page 114.*

*financement complémentaire par les utilisateurs ? C'est l'un des chantiers en cours.*

« *Nous avons demandé au secrétariat général pour la modernisation de l'action publique (SGMAP) de mener une mission sur le SNDS. Elle vise d'abord à mieux appréhender les besoins des utilisateurs et surtout les utilisations actuelles des données, que nous ne connaissons finalement pas si bien que cela, surtout si l'on prend en considération que ces données du SNDS doivent être comprises au sein d'un environnement – logiciels d'interrogation, utilisation avec d'autres données issues d'autres sources…*

« *Nous devons nous assurer qu'il n'y aura pas de rupture de service lors de l'ouverture du SNDS. D'autre part, cette mission doit proposer des pistes pour un modèle économique. La DREES avait commencé à réfléchir à ce sujet, avec l'ensemble de nos partenaires, notamment privés. La loi prévoit une gratuité des données pour les acteurs qui répondent à un besoin de service public ; elle laisse dès lors ouverte la possibilité d'une contribution demandée aux autres acteurs.*

« *La mission du SGMAP est en cours : nous ne pouvons donc pas vous répondre précisément sur ce sujet.* » (1)

Mme Mylène Girard a apporté quelques précisions bienvenues sur le calendrier du processus : « *La première étape, c'est-à-dire l'établissement du panorama des utilisateurs, est terminée. La deuxième étape, celle du recensement des coûts, commence. Nous espérons disposer d'une première vision globale au mois de février, afin de pouvoir prendre des décisions en toute connaissance de cause aux mois de février ou de mars.* »

Il est à souhaiter que des lignes directrices suffisamment précises puissent être définies en temps utile pour la mise en service du SNDS. En tout état de cause, cette démarche souligne la nécessité de mettre en place, à la CNAMTS, à l'INDS et à la CNIL, une comptabilité analytique qui permettra de connaître les coûts afin d'équilibrer les recettes et les dépenses sans dégager de profits.

#### *d. La vente sur abonnement d'agrégats statistiques commentés pourrait être plus rentable que la mise à disposition de la base contre redevance*

Selon l'article R. 1461-5 du code de la santé publique, sont constitués à partir du système national des données de santé :

« *1° Des jeux de données anonymes mis à disposition du public dans les conditions prévues au premier alinéa de l'article L. 1461-2 ;*

« *2° Des jeux de données agrégées et semi-agrégées adaptés à différents types de recherches, d'études ou d'évaluation. Les données semi-agrégées sont*

*(1) Audition du 20 décembre 2016.*

*individualisées pour les professionnels ou les établissements de santé et agrégées pour les bénéficiaires des soins* ;

« *3° Des échantillons généralistes représentatifs de l'ensemble des bénéficiaires de l'assurance maladie, comprenant tout ou partie des données relatives aux personnes les constituant*. »

Les premiers jeux, correspondant aux *datamarts*, seraient en *open data*, les seconds et l'EGB seraient gratuits pour les besoins des autorités et des personnes répondant aux demandes des pouvoirs publics.

Les jeux semi-agrégés, livrés gratuitement aux demandeurs de droit public, pourraient être servis sur facturation aux intéressés de droit privé.

La séparation entre jeux gratuits de données et traitements exigeant un accès du demandeur aux données individuelles est aisée à opérer dans les demandes occasionnelles dans lesquelles les algorithmes de traitement envisagés sont décrits. Cette séparation est beaucoup plus délicate à tracer dans les traitements opérés par les personnes disposant d'un accès permanent au SNDS ou par ceux qui sont autorisés à y opérer des traitements dont la méthodologie générale est connue sans que les algorithmes d'agrégation soient précisément définis. C'est pour ces derniers qu'un enjeu financier pourrait motiver la facturation d'une redevance ou d'un abonnement.

Pour M. Christophe Roussel, membre du groupe Affaires publiques du SNITEM et directeur du développement chez 3M France, département des systèmes d'information de santé/marchés de la santé, « *La construction idéale serait celle qui répondrait à tous les besoins des industriels : utiliser des données, soit à la demande des autorités, soit pour des études décidées par les entreprises elles-mêmes, soit pour nourrir le développement industriel. Mais les données utilisées pour différents buts ne sont pas les mêmes.*

« *Ainsi, les données agrégées présentées en open data offrent un intérêt majeur : souvent, ces données appauvries suffisent amplement à répondre aux questions des industriels, notamment dans le secteur du dispositif médical. Leur usage résout en outre bien des problèmes de sécurité informatique, notamment le risque de réidentification, tout en évitant, pour les industriels, toute solution de continuité dans l'accès aux données.*

« *Un système idéal proposerait donc des informations très fines quand c'est indispensable, mais donnerait aussi l'accès à des jeux de données agrégées qui permettent à l'industriel de travailler sans craindre une faille de sécurité.* » (1)

M. Dominique Blum considère, pour sa part, que les jeux agrégés par la puissance publique pourraient ne pas répondre aux souhaits d'évaluation des pratiques médicales en démocratie sanitaire parce que, si « *tout le monde*

*(1) Table ronde du 24 janvier 2017.*

*s'accorde sur le fait qu'il est possible de produire pour l'open data des données agrégées, qui fourniront, par exemple, la distribution des diagnostics au sein de groupes,* […] *lorsqu'on les propose aux journalistes, ils poussent de hauts cris, car ils estiment que l'information ne leur parvient que déjà filtrée et qu'on leur cache des choses. Le véritable enjeu, ce sont les bases de données qui conservent la granularité individuelle.* » (1)

Compte tenu de la fragilité juridique de l'anonymat des données, certains agrégats de catégorie 2° et tous les semi-agrégats qui identifient un professionnel de santé pourraient être produits par la CNAMTS ou son opérateur et livrés gratuitement aux demandeurs en application de l'article L. 1461-2. Cet intermédiaire protégerait l'utilisateur des agrégats des risques de poursuites judiciaires, implicitement évoqués par le rapport de la commission open data à propos des informations publiées sur les professionnels de santé : « *Si les données nominatives relatives aux professionnels de santé n'ont pas la même sensibilité que celles des patients, il n'en demeure pas moins qu'il existe des limites précises à leur publication :*

« – *La protection de la vie privée ;*

« – *Le respect de l'article 13 de la loi du 17 juillet 1978 qui précise les conditions de réutilisation de données personnelles détenues par une administration : "soit lorsque la personne intéressée y a consenti, soit si l'autorité détentrice est en mesure de les rendre anonymes, ou à défaut d'anonymisation si une disposition législative ou règlementaire le permet" ;*

« – *Le secret en matière commerciale et industrielle (art. 6 II de la loi du 17 juillet 1978), qui, selon la jurisprudence de la CADA, protège l'activité libérale des professionnels de santé.*

« *Il ressort assez clairement des échanges au sein de la commission que les données relatives aux honoraires (avec la question du choix de l'indicateur), à la nature et au volume de l'activité, aux pratiques de prescription et de façon plus générale à la qualité de la pratique constituent les champs prioritaires de publication des données.* » (2)

« […] *S'agissant de données relatives à la qualité des pratiques, il est nécessaire de permettre l'émergence consensuelle d'indicateurs porteurs de sens tant pour les professionnels que pour les patients. Pour ce faire, un lieu de concertation (par exemple au sein d'un groupe de travail* ad hoc *puis de l'instance d'expression des acteurs décrite [plus haut]) devrait être mis en place.*

« *Il est naturellement nécessaire que l'assurance maladie adresse aux professionnels de santé leurs données individuelles avant publication afin de leur permettre de rectifier d'éventuelles erreurs.* »

---

*(1) Audition du 13 décembre 2016.*

*(2) Commission open data en santé,* op. cit., *page 54.*

« […] *Les données relatives à l'activité et à la qualité des pratiques individuelles des professionnels de santé salariés constituent en revanche une zone largement inconnue des statistiques.* » (1)

En ne donnant pas directement accès aux données individuelles et en réalisant à la demande des agrégats, l'opérateur du SNDS éviterait aux consultants les procédures d'habilitation d'agents et de soumission des habilités au secret professionnel imposé par la loi.

M. Philippe Burnel avait d'ailleurs évoqué le passage d'un secret médical à un secret professionnel de statisticien exigé par la nature des bases de données de santé : « *En 2009, la loi portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires (HPST) prévoit que les agences régionales de santé (ARS) qu'elle créait pourraient avoir accès aux données SNIIRAM "dans des conditions garantissant l'anonymat des personnes", et sous l'autorité d'un médecin. Cette dernière mention, assez traditionnelle, est fondée sur l'idée que seuls les médecins peuvent accéder à des données médicales.*

« *Il s'agit, à mon sens, d'une interprétation un peu abusive du secret médical : le médecin a accès aux données médicales du malade non parce qu'il est médecin, mais parce qu'il le soigne. Or cette exigence pose problème, car le SNIIRAM est d'une telle complexité qu'il est nécessaire d'être statisticien pour en comprendre les données – pour bien faire, il faut donc être à la fois médecin et statisticien.* » (2)

En économisant aux consultants les coûts administratifs d'accès aux bases, l'opérateur du SNDS leur économise aussi en partie les coûts de formation aux structures de ces bases, indispensables pour être capables d'imaginer des agrégats pertinents et de les soumettre à l'appréciation de l'opérateur.

Mme Chantal Cases a justement expliqué que la maîtrise statistique des bases de données de santé supposait un long apprentissage : « *Jusqu'à il y a peu, les compétences étaient rares, et elles étaient localisées sur ces données. Je peux citer la caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS), qui a beaucoup développé l'exploitation des données ; l'IRDES ; certaines équipes de l'Institut national de la santé et de la recherche médicale (INSERM) – celle qui a lancé la cohorte Constances possède une très bonne connaissance de ces sujets.*

« *Je pense que l'ouverture de ces bases permettra à ces compétences de se disséminer et de se renforcer au fil des années. Un certain nombre d'équipes de l'INSERM ou de centres hospitaliers universitaires (CHU) ont commencé à travailler sur ces données, ainsi qu'il ressort des demandes actuellement adressées à l'IDS.*

---

*(1) Commission open data en santé,* op. cit., *page 55.*

*(2) Audition du 13 décembre 2016.*

« *Mais il faut un certain nombre de mois et d'années pour développer de réelles compétences permettant de travailler sur ces données. Par exemple, on a attendu dix bonnes années pour savoir exploiter utilement le PMSI. Et c'était un apprentissage nécessaire.* » (1)

L'exemple de l'INSEE prouve qu'un établissement public peut s'imposer comme une référence scientifique et statistique dans des domaines de recherches aussi vastes que ceux touchant à l'économie, en réalisant pour des tiers des agrégats statistiques qui les dispensent de demander un accès aux données individuelles protégées par un secret légal et même de reproduire les méthodes d'agrégation et de traitement appliquées par l'INSEE pour les vérifier.

Ce n'est pas, pour le moment, le modèle retenu pour l'INDS. Le législateur a préféré encourager le pluralisme par l'ouverture de la base à de nombreux accès permanents ainsi que la spécialisation de laboratoires et de bureaux d'études dans l'exploitation du SNDS.

Mme Chantal Cases n'envisage, elle aussi, pour l'INDS qu'un rôle administratif et d'accompagnement des utilisateurs : « *La loi rend l'architecture générale beaucoup plus lisible : la DREES est responsable du pilotage du système, la CNAMTS de la gestion des bases de données et le futur INDS aura pour tâche de faciliter les accès aux données et les échanges avec les utilisateurs. Le nouveau paysage est donc assez clair. À cela s'ajouteront des "bulles d'accès", autrement dit des plateformes de mise à disposition des données ; l'INSERM, notamment, en prévoit une, qui assistera les chercheurs dans la préparation de leurs projets.* » (2)

Toutefois, l'INDS étant un destinataire obligé des résultats d'exploitation du SNDS, il pourrait mettre ceux produits par les personnes publiques disposant d'un accès permanent ou pour les nécessités publiques mentionnées par l'article L. 1461-5 à la disposition du public et de la presse contre un abonnement équivalent à celui facturé par une agence de presse pour ses services de dépêches.

L'INDS pourrait aussi jouer le rôle d'un distributeur en ligne d'articles scientifiques doublé d'une société de droits d'auteurs privés. Mais ce n'est que si les agrégats sont commentés par une analyse à valeur ajoutée et réalisés rapidement et fréquemment qu'ils pourraient être vendus par l'INDS à un prix supérieur à celui d'une redevance de mise à disposition d'une base de données.

#### *e. Le CASD offre un exemple de plateforme permettant la mise à disposition, accompagnée et contrôlée, de bases publiques de données*

À la recherche d'un modèle économique pour l'exploitation du SNDS, la Cour des comptes estime que, « *au-delà du financement des frais techniques de*

*(1) Audition du 20 décembre 2016.*

*(2) Audition du 20 décembre 2016.*

*mise à disposition, l'accompagnement des utilisateurs devrait également faire l'objet d'une tarification spéciale.*

« *La création, souhaitable, de plateformes ou de structures chargées d'accompagner les utilisateurs dans la procédure de demandes d'accès aux SNDS, de les aider à définir des algorithmes, de les former aux traitements de ces données complexes ou de leur apporter une assistance technique, doit s'accompagner de règles claires de financement de leurs travaux.*

« *Ces plateformes, structures publiques comme privées, pourraient également, dans un cadre à définir avec la CNAMTS et la DREES, réaliser tout ou partie des extractions demandées. Cette perspective rejoint le projet d'infrastructure de recherche, CépiDc, porté par l'INSERM.* »

Le Centre d'accès sécurisé aux données (CASD) a été créé par l'INSEE pour permettre aux chercheurs de traiter des données confidentielles dans des conditions élevées de sécurité et de protection de la confidentialité, après l'ouverture, par la loi dite « des archives » de juillet 2008, de ses bases de données.

Entendus le 10 janvier 2017, MM. Kamel Gadouche, directeur du CASD, et Philippe Cunéo, directeur général du Groupe des écoles nationales d'économie et statistique (GENES), ont présenté leur offre commerciale de services en la comparant aux préconisations de la Cour.

M. Cunéo a essentiellement mis en avant le rôle d'intermédiation assumé par le CASD et les conséquences en termes de relations contractuelles avec les détenteurs des données comme avec les utilisateurs : « *En ce qui concerne les relations contractuelles avec les différents acteurs, il faut garder à l'esprit que le CASD ne réalise aucune étude et que sa mission quasi unique est de mettre à disposition des utilisateurs les données qui lui ont été confiées. Nous sommes, en quelque sorte, un tiers de confiance, ce qui signifie que nous sommes liés contractuellement avec les détenteurs des données, par l'intermédiaire d'une convention qui spécifie les modalités de mise à disposition de ces données ainsi que les modalités d'habilitation. En tant que tel, le CASD ne procède à aucune habilitation, lesquelles dépendent soit du producteur de données soit de la loi, par exemple de la loi de 1951.*

« *En aval, nous sommes liés aux utilisateurs par un triple contrat : en premier lieu, un contrat d'hébergement, qui stipule que le boîtier d'accès ne peut être connecté n'importe où et que l'accès à la bulle doit se faire à partir de l'établissement signataire du contrat, qui garantit des conditions d'hébergement très strictement définies – boîtier installé dans un bureau fermé, écran visible par le seul utilisateur… En second lieu, est signé un contrat de financement, que nous avons déjà évoqué, et, enfin, un contrat d'utilisation, qui spécifie les conditions de consultation auxquelles doit se conformer l'utilisateur.* »

M. Gadouche a apporté des informations détaillées sur les paramètres financiers des consultations effectuées *via* le CASD : « *Pour en revenir à la question du coût et de son estimation, le rapport de la Cour des comptes distingue, d'une part, le volet gestion et alimentation du SNDS, d'autre part, le volet diffusion. En ce qui nous concerne, la production et l'alimentation sont gérées par les détenteurs des données. Ce qui nous est transmis, ce sont des copies des bases, à charge pour nous de les installer dans une bulle sécurisée pour les mettre à disposition.*

« *Le coût de cette opération croît de façon linéaire avec le nombre d'utilisateurs, dont nous n'avons pas encore, en l'occurrence, d'idée précise, pas davantage que nous ne savons quels seront les usages qui seront faits du système. Cela étant, pour vous donner un ordre de grandeur, l'accès d'un millier d'utilisateurs coûte aujourd'hui 2 millions d'euros, sachant qu'une part de cette somme correspond aux importants investissements de départ et qu'elle devrait décroître après 2020.*

« […] *Notre grille tarifaire est affichée sur notre site. La contribution moyenne demandée est de 800 euros par an et par utilisateur – mais, comme je vous l'ai indiqué, ce montant a été établi en tenant compte de la subvention que nous recevons pour financer ce projet dit équipement d'excellence.* »

M. Cunéo a ensuite ajouté que, « *Sans subvention, le montant demandé devrait être de 1 200 euros par utilisateur. Nous avons fait savoir aux chercheurs que c'est ce que nous leur demanderons à partir de 2019 si la subvention au titre de l'équipement d'excellence n'est pas renouvelée.* »

Le directeur du CASD a apporté aux questions du rapporteur une réponse écrite circonstanciée détaillant le contenu du contrat-cadre passé avec les consultants des bases : « *Pour pouvoir avoir accès aux données du CASD, l'utilisateur et les organismes concernés doivent signer un ensemble contractuel qui se compose :*

« *– D'un contrat-cadre de prestation dit "hébergeur – financeur" en vertu duquel l'entité signataire se voit dotée de la capacité à héberger un ou plusieurs points d'accès au CASD (SD-Box) via l'émission de bons d'hébergement (il y a autant de bons d'hébergement émis que de SD-Box hébergées) ; et/ou à financer l'accès et les services nécessaires au traitement des données dans le cadre d'un "projet" via l'émission de bons de commande. Ce document régit les relations contractuelles entre le GENES et son Cocontractant, et fixe les devoirs et obligations de chacune des parties – notamment en termes financiers, matériels, administratifs, de confidentialité, etc. Toute entité émettant ou ayant émis au moins un bon d'hébergement dans le cadre de ce contrat-cadre est qualifiée d'Hébergeur. Elle est qualifiée de "Financeur" dès lors qu'elle émet ou a émis un bon de commande dans le cadre de ce contrat-cadre. Une entité peut être à la fois "Hébergeur" et "Financeur".*

« *– De “Conditions d’utilisation du CASD”, destinées à chacun des membres du projet, qui précisent en particulier les modalités d’usage du service et du matériel, les obligations et responsabilités des utilisateurs notamment en termes de sécurité et de confidentialité, mais aussi les engagements du CASD à leur égard en termes de services, d’assistance et de support technique. Il y a autant de “Conditions d’utilisation” signées que d’utilisateurs impliqués sur un projet.*

« *Il n’y a pas de méthodologie de recherche convenues avec les utilisateurs qui restent libres de réaliser les traitements qu’ils souhaitent à condition qu’ils s’exécutent dans l’environnement sécurisé.* »

Cette absence de méthodologie distingue le contrat-cadre proposé par le CASD de la convention cadre proposée par la CNIL.

### *f. Les redevances demandées pour la consultation du PMSI couvrent en partie les charges d’exploitation de cette base*

Le PMSI, auparavant distribué gratuitement par échange de CD-Rom aux personnes publiques, est mis à la disposition de recherches à but lucratif par l’ATIH, qui en est dépositaire, et par l’intermédiaire technique du CASD.

Dans sa réponse écrite aux questions du rapporteur, M. Kamel Gadouche décrit les conditions contractuelles et le coût de l’abonnement qu’il propose : « *Il existe aujourd’hui un contrat entre l’ATIH et le Genes (CASD) dans le cadre d’un marché à procédure adaptée (MAPA) pour l’année 2017. Le renouvellement du marché avec l’ATIH est conditionné à la publication du référentiel de données de santé (et donc à son contenu). Il n’y a pas de convention entre le Genes et la CNAM-TS.*

« *Le service de mise à disposition des données (et non les données) est facturé par le CASD à l’utilisateur final. La facturation annuelle moyenne aujourd’hui est de 788 € par utilisateur. Cette facturation sert à couvrir partiellement les frais d’exploitation, l’autre partie étant couverte par le financement Equipex et les contributions des partenaires du projet.*

« *Les tarifs sont fixés à l’issue d’une étude détaillée des coûts complets de mise à disposition. Nous ne pratiquons pas de marge commerciale.* »

Selon le rapport de la Cour des comptes, les utilisateurs intéressés par le PMSI « *s’acquittent d’une redevance, forfaitaire – et minime – jusqu’à quatre heures de travail effectuées pour répondre à leur commande (250 € en 2015) ; s’y ajoute 0,34 centime par tranche de 999 cellules.* »

La Cour ne précise pas si cet accès est facturé et ouvert par le CASD ou directement par l’ATIH, en particulier auprès des médecins responsables de l’information médicale.

### *g. Le choix du CASD pour diffuser le SNDS aux personnes privées ne s'est pas imposé au ministère de la santé*

Selon la réponse écrite du directeur du CASD aux questions du rapporteur, le logiciel dont le CASD est propriétaire et pour lequel un brevet a été déposé est utilisé dans plusieurs domaines parmi lesquels :

« *CASD "Données Publiques", hébergé au GENES (au sein des locaux de l'INSEE), permettant à près de 1000 utilisateurs français et étrangers de travailler sur des données confidentielles des administrations françaises, en particulier : les données de l'INSEE, du Ministère de la Justice, du Ministère de l'Agriculture, … du Ministère du Travail, les données fiscales sur les personnes physiques et les entreprises et les données de santé (Memento et PMSI).*

« *CASD "Recherche Publique Européenne" : le CASD a développé un pilote de réseaux d'accès sécurisés – utilisant la technologie CASD – avec l'Allemagne, la Grande-Bretagne, le Portugal, la Hongrie. Les gisements de données ciblés sont ceux de la Statistique Publique Européenne (http://www.safe-centre.info/) et plus généralement les données à caractère socio-économique utiles aux recherches en économie et sciences sociales (http://www.dwbproject.org/).*

« *CASD "Usages privés", dont l'objectif est de permettre à des entreprises ou établissements publics d'utiliser la technologie du CASD pour leurs propres besoins. À titre d'exemple, cette version du CASD a été utilisée par la Banque Postale, la Banque Publique d'Investissement ou encore Generali pour faire travailler des consultants et experts (externes à l'entreprise donc) sur leurs données clientèle.*

« *Parmi les pistes de développement en cours d'étude : le CASD en mode "Dataroom" pour permettre d'accéder à des données et documents sensibles – sans risque de fuite – dans le cadre d'une opération de* due-diligence, *le CASD en mode interne pour permettre à des personnels internes à l'entreprise de travailler à distance sur des données confidentielles, sans utiliser des solutions logicielles de type Citrix, coûteuses à maintenir et dont le niveau de sécurité n'est pas suffisant., etc.* »

M. Gadouche précise que cependant, « *le ministère de la santé n'a* a priori *pas voulu adopter le dispositif CASD existant pour différentes raisons selon nous :*

« *– En premier lieu parce qu'il a voulu au préalable procéder à une analyse des risques afin de préciser les besoins plutôt que d'adopter d'emblée un outil existant (ce qui est bien sûr légitime) ;*

« *– Parce qu'il a considéré aussi que la sécurité du dispositif ne se limitait pas au segment final de la mise à disposition des données (ce qui est là aussi exact) et que le référentiel à paraître devrait donc évaluer l'ensemble des risques ; Mais il nous semble qu'il aurait été opportun de considérer séparément*

*ces deux segments distincts : production de données et diffusion sécurisée de données à des utilisateurs extérieurs ;*

« *– Parce que les organismes gestionnaires des données (en particulier la CNAMTS et l'ATIH) ont déjà expérimenté ou mis en œuvre des dispositifs techniques de mise à disposition des données auxquels ils ne souhaitent pas renoncer, ce dont nous ne remettons pas en cause non plus la légitimité ;*

« *– Parce que les rédacteurs du projet de référentiel de sécurité voient aussi dans le CASD un dispositif trop exigeant (au regard des besoins de sécurité) et donc trop contraignant pour les utilisateurs.*

« *Nous contestons cette analyse, en particulier parce qu'elle ne distingue pas la fonction de production de données et la fonction de diffusion sécurisée. Cette dernière fonction fait précisément partie intégrante de la mission du CASD et donne satisfaction aux utilisateurs du CASD.*

« *De plus, pour la diffusion sécurisée des données, certaines procédures techniques ou organisationnelles du CASD peuvent être ajustées en fonction des besoins des producteurs de données et sont toujours spécifiées dans les conventions ou contrats correspondants.*

« *Il est vrai que pour la fonction de production, les adaptations nécessaires, que ce soit du côté du CASD ou du côté des utilisateurs, sont plus importantes.*

« *– Parce que, enfin, ils jugent le CASD trop coûteux pour les utilisateurs alors qu'une réflexion sur le modèle économique des données de santé laisse penser, à notre sens, qu'au contraire cette opinion est loin d'être avérée, notamment si on prend en compte les coûts cachés induits par la multiplication de dispositifs, les audits réguliers* ex post*…* »

***h. Les principaux utilisateurs privés intéressés par le SNDS sont réservés sur l'acquittement d'une redevance***

Lors de la table ronde réunissant les assureurs, les mutuelles et les complémentaires santé organisée le 6 décembre 2016, de nombreuses réticences à l'acquittement d'une redevance se sont exprimées. Mme Cécile Malguid a notamment estimé que la complexité du dispositif retenu ne devait pas aboutir à voir vidée de son sens la notion de « droit d'accès aux données » : « *La FFA a alors fait valoir que, si nous devions un jour payer un droit d'accès aux données, il faudrait que celui-ci soit bien réel. Or, si la loi permet une ouverture, il faut bien voir que, du point de vue des opérateurs, l'accès aux données reste excessivement complexe et le fonctionnement de l'institut des données de santé (INDS) ne garantit pas…* […] *J'ajoute que la loi précise que les organismes complémentaires vont contribuer à ce système pour un coût dont il faudra tenir compte dans le modèle économique*. »

Intervenant au cours de la table ronde réunissant les laboratoires et industriels de la santé organisée le 24 janvier 2017, M. Philippe Lamoureux, directeur général du LEEM, est convenu de la légitimité d'une participation au financement du système tout en récusant l'idée d'y satisfaire par le biais d'une taxe : « *les entreprises du médicament que je représente ici ne sont pas favorables à l'instauration d'une énième redevance ; nous payons déjà onze taxes spécifiques, et la fiscalité spécifique française est la plus lourde d'Europe. Il ne faut donc pas l'accroître. Nous ne sommes pas non plus favorables au paiement d'une redevance lorsque les recherches sont réalisées à la demande de la puissance publique.*

« *En revanche, nous ne sommes nullement opposés à l'idée de participer au financement du système : l'utilisation de la base doit être payante, dans des conditions qui restent à imaginer – on peut penser, par exemple, à un système de forfait par tranche. La vertu du système de paiement à l'utilisation serait d'assurer la proportionnalité entre les ressources de l'INDS et l'utilisation de la base de données. Cela constituerait donc une réponse à la question des moyens, alors qu'un système de taxe serait au contraire forcément sur- ou sous-dimensionné.* »

M. Christophe Roussel a appelé, pour sa part, à établir un système qui corresponde bien aux besoins des utilisateurs, notamment pour les secteurs où opèrent surtout des TPE et des PME : « *Pour que le système fonctionne, il doit répondre aux besoins des industriels. Le parcours d'accès aux données est aujourd'hui complexe – certains ont parlé d'usine à gaz – et le comité stratégique de filière s'est attelé à sa simplification. Par ailleurs, vous évoquiez le modèle économique du nouveau système : l'idée d'un paiement à chaque demande peut convenir dans certains cas.*

« *Mais, j'y insiste, notre secteur est essentiellement composé de PME et de TPE : si l'industriel qui a besoin d'accéder de façon répétée à des informations doit verser un forfait à chaque fois, il lui sera bien difficile d'utiliser les données, et le système sera inopérant. Il faut donc vérifier que les délais et les coûts correspondent bien aux besoins réels et aux capacités des différents types d'acteurs.* »

Bien au fait de la problématique, M. Vincent Bildstein a souligné l'effet bénéfique en termes de coûts que l'on peut attendre du passage obligé par des bureaux d'études : *« L'autorisation d'accès donnée aux bureaux d'études permettra aussi de mutualiser les coûts du dispositif – ils étaient importants pour le PMSI et, étant donné l'augmentation du volume de données recueilli et leur complexité, ils le seront davantage encore pour le SNIIRAM. Cela réduira le coût d'accès potentiel pour les plus petits des acteurs intéressés, qui ne pourraient assumer individuellement l'infrastructure technique et humaine nécessaire.* »

M. Christian Babusiaux avait cependant remarqué que : « *s'il est instauré une tarification des accès aux données* [effectués] *par des assureurs ou par des*

*laboratoires pharmaceutiques, par exemple, cela signifierait qu'ils pourraient en tirer un profit commercial et justifierait leur cotisation. À mon sens, nous devons nous garder de mettre le doigt dans cet engrenage.* » (1)

Nonobstant ces avis très divers, le rapporteur est convaincu que les réflexions et travaux préliminaires sont suffisamment avancés et que le modèle du CASD est suffisamment éclairant pour que des décisions soient prises dans un délai rapproché, qui permettront sinon de garantir la viabilité économique intrinsèque du SNDS, du moins de couvrir dans des proportions raisonnables une partie de ses coûts, selon des modalités respectueuses à la fois des besoins des gestionnaires et des attentes des utilisateurs.

*(1) Audition du 17 janvier 2017.*

## CONCLUSION

Contrairement à l'habitude de la MECSS, le présent rapport ne formule pas de propositions ou de recommandations – tout au plus quelques conseils. La raison en est simple.

Comme le rapporteur l'a indiqué précédemment, la construction du système public de données de santé n'est pas encore achevée. Bon nombre de décisions restent encore à prendre – ce qui aurait pu justifier une attitude plus hardie – mais, surtout, bon nombre de paramètres restent encore inconnus.

Par ailleurs, la MECSS n'a pu consacrer que quelques semaines à ce sujet complexe, touffu, et aux nombreuses implications. Plusieurs dimensions du sujet n'ont été qu'effleurées ou n'ont pas pu être abordées.

Le rapporteur a donc fait le choix de préparer un simple rapport d'étape, le traitement intégral du sujet étant renvoyé à la prochaine législature, sous réserve que la MECSS l'inscrive à nouveau à son programme de travail. Cela lui a paru être une façon pertinente de mettre à profit le caractère transpartisan de la MECSS, qui est le gage de la continuité de son action et de la qualité de ses travaux.

*
* *

La mission d'évaluation et de contrôle des lois de financement de la sécurité sociale a *adopté* le présent rapport, à l'unanimité, lors de sa réunion du 21 février 2017.

## TRAVAUX DE LA COMMISSION

*Dans sa séance du 21 février 2017, la commission des Affaires sociales examine le rapport d'information de M. Pierre Morange en conclusion des travaux de la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale (MECSS) sur les données médicales personnelles inter-régimes détenues par l'assurance maladie, versées au SNIIRAM puis au Système national des données de santé (SNDS).*

**Mme la présidente Catherine Lemorton.** Nous allons examiner le rapport d'information de M. Pierre Morange sur les données médicales personnelles inter-régimes détenues par l'assurance maladie versées au Système national d'informations inter-régimes de l'assurance maladie (SNIIRAM) puis au Système national des données de santé (SNDS).

Avant de vous donner la parole, monsieur Morange, je tiens à saluer votre action à la tête de la Mission d'évaluation et de contrôle des lois de financement de la sécurité sociale (MECSS), dont les rapports sont toujours fort intéressants et qui a le mérite de prendre le temps de travailler dans le calme. Depuis 2007, vous avez assumé la coprésidence de cette mission, d'abord avec Jean Mallot, puis avec Jean-Marc Germain et, aujourd'hui, avec Gisèle Biémouret. Je vous remercie pour le soutien constant que vous avez apporté à ses rapporteurs, soutien dont j'ai moi-même bénéficié lorsque, chargée, en 2008, d'un rapport sur le médicament – je ne reviendrai pas sur ce débat, qui fut presque un combat –, je me suis retrouvée aux prises avec un laboratoire pharmaceutique.

**M. Pierre Morange, coprésident de la Mission d'évaluation et de contrôle des lois de financement de la sécurité sociale (MECSS), rapporteur.** Merci, madame la présidente. Je veux tout d'abord remercier, au nom de Gisèle Biémouret, coprésidente, et des membres de la MECSS, la commission des affaires sociales ainsi que les administrateurs, qui m'ont accompagné dans ces travaux.

Je reconnais que l'intitulé de ce rapport d'information – pour lequel nous avons sollicité l'avis de la Cour des comptes, laquelle nous a remis les conclusions de ses travaux en mai 2016 – est quelque peu aride et qu'il pourrait dissuader les meilleures volontés de s'intéresser au sujet. Il présente comme particularité de ne pas comporter de recommandations puisqu'il s'agit d'un rapport d'étape : de fait, nous sommes au milieu du gué.

Permettez-moi de rappeler tout d'abord quelques chiffres. Le Système national des données de santé, qui regroupe les données du Programme de médicalisation des systèmes d'information (PMSI) et du SNIIRAM, est issu de l'article 193 de la loi de modernisation de notre système de santé. Il est d'ores et

déjà le plus important fichier de données médicales d'Europe, voire du monde, et il sera encore enrichi, au cours de l'année 2017, par les données du CépiDC, le Centre d'épidémiologie sur les causes médicales de décès. Au stock des données déjà détenues par la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) s'ajoutera, chaque année, un flux constitué de 1,2 milliard de feuilles de soins, 500 millions d'actes médicaux et 11 millions de séjours hospitaliers. L'ensemble a une profondeur historique de quinze à vingt ans selon les données. Le CépiDC compte, quant à lui, 20 millions d'enregistrements.

Un tel réservoir d'informations suscite de nombreuses interrogations sur la sécurité – quelle est la qualité du coffre-fort informatique ? –, la confidentialité des données, les procédures d'accès à ces données, les moyens humains, techniques et financiers nécessaires à leur exploitation et, enfin, l'enjeu économique que représente le financement du dispositif. Tels sont les défis que l'article 193 de la loi de modernisation de notre système de santé nous invite à relever.

La première partie du rapport présente l'état des lieux de ce qui est encore, à l'heure actuelle, un dispositif en construction. Une plus grande ouverture des données personnelles de santé permettrait de renforcer la démocratie sanitaire, d'améliorer la vigilance sanitaire, d'assurer un pilotage plus efficient de la politique de santé publique et du système de soins – selon la Cour des comptes, l'exploitation des données du SNIIRAM est susceptible d'engendrer 840 millions d'euros d'économies. Elle permettrait aussi de favoriser le progrès de la recherche médicale en facilitant la reproductibilité de la preuve et la constitution de cohortes significatives – je pense par exemple à la recherche sur les maladies orphelines ou l'oncologie pédiatrique, qui concernent des populations restreintes.

L'article 193 vise à concilier les objectifs *a priori* contradictoires que sont une plus grande ouverture au public des données personnelles de santé et la préservation de la vie privée, y compris la garantie du secret médical.

En ce qui concerne les données elles-mêmes, il faut noter que le SNDS rassemblera des données sanitaires et médico-sociales. Ainsi que je l'ai indiqué, il intégrera, outre les deux grandes bases médico-administratives déjà en interaction, le PMSI et le SNIIRAM, et la base CépiDC, les données transmises à la Caisse nationale de solidarité pour l'autonomie (CNSA) par les maisons départementales des personnes handicapées (MDPH). Notre collègue Martine Carillon-Couvreur a démontré dans son excellent rapport, déposé en janvier 2015, que la collecte des informations et des données auprès des établissements de soins et des MDPH était notoirement insuffisante. Les personnes auditionnées estiment néanmoins que, dans ce domaine, l'objectif pourrait être atteint, dans le meilleur des cas, dans un délai de deux à trois ans. J'ajoute que le SNDS comportera également un échantillon représentatif des données de remboursement transmises par des organismes d'assurance maladie complémentaire. Ceux-ci le feront cependant dans un cadre, non pas légal, mais conventionnel. Il faudra donc trouver les moyens de les inciter à participer activement à cette transmission.

Pour concilier les objectifs *a priori* contradictoires que sont la plus grande ouverture au public des données personnelles de santé et la préservation de la vie privée, le nouveau dispositif définit des droits d'accès différenciés selon les données et les opérateurs. Les données agrégées, qui ne présentent aucun risque de ré-identification, seront ouvertes à tous sans restriction et à titre gratuit, comme les données relatives à l'activité des professionnels de santé. En revanche, les données qui peuvent être directement ou indirectement identifiantes seront accessibles sous conditions et uniquement pour des recherches, évaluations ou études dont il faudra démontrer qu'elles présentent un « intérêt public » – notion dont la définition juridique doit être précisée.

Par ailleurs, les organismes chargés d'une mission de service public, dont la liste sera arrêtée par décret en Conseil d'État, bénéficieront d'un accès privilégié et permanent. Quant aux opérateurs privés, ils devront respecter des contraintes renforcées. Je rappelle que, grâce au travail parlementaire, l'utilisation des données du SNDS est expressément proscrite dans deux cas : l'extraction des données aux fins d'exclusion de garantie ou d'adaptation de la tarification des contrats d'assurance, d'une part ; aux fins de ciblage territorial ou professionnel du démarchage des prescripteurs de médicaments, d'autre part. Enfin, pour les opérateurs privés, le traitement des données devra être effectué par un tiers, laboratoire de recherche ou bureau d'études, public ou privé.

L'article 193 de la loi de modernisation de notre système de santé traite ces questions, mais nous avons souhaité clarifier le nouveau dispositif, si touffu que nous serons bientôt conduits à remettre l'ouvrage sur le métier. De fait, nous avons été amenés, au fil des auditions, à nous intéresser à quatre thèmes, qui fondent la seconde partie du rapport : la solidité du socle juridique du SNDS, la sécurité informatique du dispositif, la gouvernance du système et son modèle économique.

Le socle juridique du SNDS devra être suffisamment solide si l'on veut tirer parti de toutes les potentialités, par exemple si l'on souhaite intégrer à terme les données issues des objets connectés, qui connaîtront une croissance exponentielle au cours des quelques années à venir ; cela rendra le problème plus complexe encore. Il convient aussi de cerner la notion d'« intérêt public », clef d'entrée du SNDS pour les organismes ne disposant pas d'un accès permanent ; la doctrine ainsi établie devra guider les décisions du futur Institut national des données de santé qui devra rendre un avis sur chaque demande d'accès déposée.

Outre cela, plusieurs textes définissent les finalités du système gouvernant l'ouverture des données personnelles de santé, dont l'article 8 de la loi du 6 janvier 1978 relative à l'informatique et aux libertés ; leur ensemble étant quelque peu confus, il conviendrait de les harmoniser. C'est d'autant plus nécessaire qu'un règlement européen, adopté au printemps 2016 et qui entrera en vigueur en mai 2018, obligera à repenser certains fondements du SNDS. Une mission d'information de la commission des lois examine, d'ailleurs, depuis quelques semaines, les incidences sur la législation française des nouvelles normes

européennes en matière de protection des données personnelles. Déjà, la Commission nationale de l'informatique et des libertés (CNIL) a informé la MECSS que le Parlement devrait être saisi, probablement dès l'été 2017, d'un nouveau projet de loi « Informatique et libertés » qui, visant à tirer toutes les conséquences du règlement européen, traitera notamment des données de santé.

Paradoxalement, ce chantier législatif semble donc être inachevé alors même que les décrets d'application de la loi de modernisation de notre système de santé ne sont pas encore tous publiés – les derniers décrets parus pour le sujet qui nous concerne l'ont été le 26 décembre 2016 et ceux qui traitent de l'articulation entre PMSI et SNIIRAM au sein du SNDS doivent paraître le 1er avril 2017. Aussi le secrétaire général de la CNIL a-t-il indiqué : « *Actuellement, nous en sommes réduits à nous demander si un régime juridique dont nous ne connaissons pas encore tous les contours est bien compatible avec un texte dont la clarté n'est pas évidente…* ». Enfin, l'accès aux données stockées dans le SNDS emporte l'obligation légale de publication des recherches menées à bien grâce à leur utilisation. Cela pose un problème de droit de propriété intellectuelle, source de contentieux potentiels, qui n'a pas encore trouvé réponse.

L'exigence de sécurité informatique est double : il faut assurer, d'une part, la protection contre les risques d'intrusion et, d'autre part, la protection contre les risques liés à la ré-identification des données personnelles préalablement pseudonymisées.

S'agissant du risque d'intrusion, la Cour des comptes recommande d'ériger la CNAMTS en « opérateur d'importance vitale » au sens du code de la défense. La plupart de nos interlocuteurs ne partagent pas cet avis. La MECSS estime que l'important est moins la qualification juridique de l'opérateur que les garanties et le niveau de sécurité offerts par la gestion du futur SNDS ; on pourrait donc envisager de classer la CNAMTS au nombre des « opérateurs de service essentiel » au sens du droit européen des réseaux et des systèmes d'information.

Pour prévenir le risque de ré-identification, il est nécessaire de modifier l'algorithme de cryptage des données personnelles, considérées comme obsolescent par la Cour et par nombre de spécialistes. La CNAMTS assure de la robustesse de cet algorithme pendant encore quelques années, néanmoins, l'engagement des opérations nécessaires à son remplacement est prévu dans la future convention d'objectifs et de gestion entre l'État et la CNAMTS.

J'en viens à la gouvernance du dispositif. La loi visait à la simplifier pour faciliter les procédures et réduire le délai d'autorisation d'accès aux données, actuellement compris entre douze et quinze mois, et parfois dix-huit mois. Or le dispositif demeure complexe : le pilotage stratégique du SNDS est assuré par la direction de la recherche, des études, de l'évaluation et des statistiques (DREES) et l'INDS, la gestion technique par la CNAMTS, et la CNIL accordera ou n'accordera pas les autorisations d'accéder aux données. À cette organisation déjà passablement touffue, dans laquelle les compétences des divers acteurs restent

insuffisamment définies, se greffent plusieurs comités – comité de pilotage stratégique du SNDS, comité des utilisateurs, comité des services, comité d'audit et de contrôle – qui sont autant d'acteurs secondaires dont on mesure mal l'articulation avec les acteurs principaux. Ce n'est pas un procès d'intention mais un constat : nous sommes au milieu du gué et le rapport d'étape qui vous est soumis aujourd'hui devrait être la base de nouveaux travaux parlementaires.

Enfin, le modèle économique du nouveau système d'information n'est ni chiffré ni bien défini. Dans le rapport sur la gouvernance et l'utilisation des données de santé qu'il a remis en 2013 à la ministre des affaires sociales de la santé, M. Pierre-Louis Bras en évaluait le coût à 20 millions d'euros, un montant dérisoire rapporté aux plus de 200 milliards d'euros consacrés aux dépenses de santé. Il faut accélérer la mise en œuvre du nouveau système, donc lui consacrer les moyens humains supplémentaires nécessaires. L'effectif actuel de l'Institut des données de santé (IDS), qui deviendra l'INDS, est de neuf personnes ; elles devraient être douze, à terme, pour faire face à l'augmentation continue du volume des données collectées et à l'accroissement du nombre de demandes d'accès. Le principe d'instituer une redevance, ou une taxe, pour l'utilisation de ces données par les opérateurs privés n'a pas été tranché. Cela conditionne pourtant la viabilité du dispositif.

Contrairement à l'habitude, le rapport, adopté par la MECSS ce matin, ne présente pas de recommandations. Beaucoup de décisions restent à prendre, ce qui aurait pu justifier une attitude plus hardie, mais bon nombre de paramètres demeurant inconnus, la sagesse commande de ne vous présenter qu'un rapport d'étape, en laissant à la prochaine législature le soin de parachever cet ouvrage, une fois parus tous les décrets d'application et après avoir mesuré l'impact du règlement européen transposé dans une nouvelle loi « Informatique et libertés ». La synthèse ainsi permise devrait permettre de refonder l'article 193 de la loi de modernisation de notre système de santé pour établir un dispositif satisfaisant en termes de sécurité et de confidentialité des données, crédible sur le plan économique et à même, pour ces raisons, de faire face à des enjeux stratégiques pour la politique nationale de santé.

**Mme Martine Carrillon-Couvreur.** Au nom du groupe Socialiste, écologiste et républicain, je salue le travail accompli par Pierre Morange, qui préside la MECSS avec notre collègue Gisèle Biémouret. J'ai eu l'honneur de participer un temps à la réflexion de la Mission, dont notre commission a toujours suivi les travaux avec une grande attention. Ce n'est pas sans émotion que je prends la parole devant vous ce soir pour la dernière fois puisque je ne me représenterai pas à la députation ; j'ai mesuré tout ce que la MECSS apporte à nos débats et je puis témoigner qu'elle nous apprend beaucoup.

Je tiens à saluer la constance de notre rapporteur et sa parfaite cohérence ; il n'a cessé de souligner l'importance du sujet dont nous débattons. Comme il y invite, les importants travaux réalisés sur l'ouverture de l'accès aux données de santé devront être poursuivis par la future MECSS. Le SNDS rassemblera à terme

les données médicales et médico-sociales ; l'accès à ces données différentes des autres suppose une procédure spécifique. L'article 193 de la loi de modernisation de notre système de santé a amorcé une évolution bienvenue mais il faudra aller plus loin. Le rapport a le grand mérite d'apporter tous les éléments nécessaires à l'achèvement ultérieur de ces travaux et de préparer l'élaboration de décrets que notre réflexion devrait enrichir. En particulier, la gouvernance du dispositif, complexe et alourdie par l'adjonction de plusieurs comités, demande à être encore débroussaillée pour faciliter l'ouverture de l'accès aux données. Sur un plan général, les travaux de la MECSS ont souvent mis l'accent sur de tels travers, qui entravent le fonctionnement des organismes intervenant dans le champ de la protection sociale ; ils devront être corrigés.

Le rapport mentionne l'obligation légale de verser au SNDS les données des maisons départementales des personnes handicapées. Le rapport d'information sur la mise en œuvre des missions de la Caisse nationale de solidarité pour l'autonomie (CNSA), que j'ai présenté en janvier 2015, montrait que, dix ans après la création de la Caisse, il n'existait pas de système partagé d'accès aux données médico-sociales. La prise de conscience s'est faite, mais comment envisagez-vous les choses sur ce plan ?

Les travaux dont vous avez été un artisan très engagé, monsieur Morange, doivent se poursuivre. Beaucoup reste à faire dans le domaine médico-social pour améliorer l'évaluation de l'activité et des coûts et favoriser l'optimisation de l'offre de soins. Ce chantier législatif inachevé doit se poursuivre et j'invite à la vigilance notre commission, dont je remercie la présidente et le rapporteur.

**Mme la présidente Catherine Lemorton.** Je vous remercie pour le travail que vous avez accompli dans notre assemblée au bénéfice de tous ceux que nos travaux concernent.

**M. Dominique Tian.** Au nom du groupe Les Républicains, je remercie à mon tour Pierre Morange. Pour avoir participé aux travaux de la MECSS alors qu'il la présidait avec Jean Mallot, j'ai constaté leur volonté de parvenir à des recommandations communes que les gouvernements devraient, en principe, s'empresser de suivre – malheureusement, on connaît les limites de l'exercice. Le recueil des données de santé passionne notre rapporteur de longue date, comme en attestent les travaux qu'il a conduits avec Jean-Pierre Door sur le dossier médical partagé. Cette fois, nous parlons d'*open data* et les enjeux sont considérables. La France disposant de bases médico-administratives de santé sans équivalent, nous devrions être premiers en la matière, mais tels sont les problèmes de gouvernance du dispositif, qu'il n'en est rien.

Dans son numéro de janvier 2017, le magazine *Mutations* de la Mutualité française publie l'entretien croisé de Didier Sicard, professeur de médecine et président d'honneur du Comité consultatif national d'éthique, et de Nicolas Revel, directeur général de la CNAMTS, à propos de l'exploitation des données de santé. M. Sicard y voit « *un enjeu scientifique et économique majeur* » mais il est d'avis

que la France est *« très en retard culturellement* » à ce sujet, l'Assurance maladie se faisant « *la gardienne un peu jalouse* » de l'utilisation qui peut être faite des données du SNIIRAM. Il en résulte que si la loi autorise les opérateurs de toutes sortes à accéder à ces données, la culture du partage n'existe pas, de par « *une peur de la rupture de confidentialité qui relève bien souvent du fantasme* ».

M. Sicard poursuit en disant : « *L'idée que les données de santé anonymisées mises en commun puissent avoir une fonction de santé publique n'a pas encore fait son chemin. Les données de santé ne sont pas au centre des stratégies, elles sont considérées comme secondaires. Dans des institutions comme la Haute Autorité de santé, qui ont pourtant un accès permanent au SNIIRAM, il n'y a pas de cellule dédiée à l'exploitation des données. Ce qui me frappe, c'est l'absence de curiosité et le conservatisme du monde médical. La France n'est pas un pays de santé publique et elle n'a pas encore pris le tournant numérique* ». Que les délais de réponse aux demandes d'autorisation d'accès soient trop longs – il y faut parfois près de deux ans – est « *décourageant et dissuasif* » pour les chercheurs. Aussi M. Sicard souhaite-t-il que l'assurance maladie « *s'engage dans un partenariat plus dynamique et plus collaboratif avec la communauté médicale et scientifique* ».

Or le rapport qui nous est présenté aujourd'hui semble indiquer que le dispositif qui a été conçu pour remédier à cette lacune se traduit par un nouveau système très compliqué et qui ne fonctionne pas. On ne peut donc manquer de s'interroger : la voie et l'opérateur choisis sont-ils les bons ? Des mesures correctrices ne s'imposent-elles pas, alors que nous prenons du retard ? La Cour des comptes s'en inquiète également, mais les solutions qu'elle recommande n'étant pas exactement celles du rapporteur – que je félicite pour son excellent travail –, le débat doit se poursuivre.

**M. Bernard Perrut.** Je salue l'habituelle qualité des travaux menés par Pierre Morange dans le cadre de la MECSS, cette fois pour traiter d'un sujet complexe aux implications majeures. L'avis est partagé : il est de l'intérêt de tous que les données de santé soient rendues plus accessibles. Cela ne peut se faire, cependant, sans précautions particulières puisqu'il s'agit de données à caractère personnel qui révèlent des indications sur l'état de santé des individus. À cela s'ajoutent les contraintes juridiques rappelées par le rapporteur et la nécessité de droits d'accès différenciés et de contrôle de l'exploitation.

Tout cela est décrit de manière exhaustive. Le rapport qui nous est présenté clôt donc une première étape de la réflexion de la MECSS sur un dispositif qui ne fonctionnera qu'après que tous les décrets nécessaires auront été publiés et une fois arrêtée la convention constitutive du groupement d'intérêt public du futur INDS. Quelle vision en avez-vous, et dans quel délai, selon vous, ces conditions seront-elles remplies ?

Le rapport évoque aussi la gouvernance du dispositif, son articulation avec le règlement européen bientôt en vigueur, la protection de la sécurité et de la

confidentialité des données de santé ainsi que le modèle économique de l'exploitation des données du SNDS. Ce vaste spectre dit assez la complexité du sujet. Une réponse définitive ne peut être donnée aujourd'hui ; il faudra donc poursuivre ce grand œuvre en traçant le bon chemin.

**Mme la présidente Catherine Lemorton.** Je note, monsieur le rapporteur, que tout en vous félicitant de la présence de l'Union nationale des professions de santé au sein du futur groupement d'intérêt public dont les contours exacts restent à définir, vous exprimez une réserve : que l'intérêt corporatiste ne l'emporte sur l'intérêt général. M. Christian Babusiaux, ancien président de l'IDS, que vous avez entendu, s'inquiète également de l'introduction des laboratoires pharmaceutiques dans le processus d'autorisation d'accès aux données de santé.

**M. le rapporteur.** Je vous remercie, chers collègues, pour ce concert d'éloges. En cette fin de législature, j'exprime le vœu ardent que la MECSS, dont la composition transpartisane lui permet de se dispenser des querelles idéologiques pour se concentrer sur l'analyse du rapport coût-efficacité de notre système de sécurité sociale, continue, au cours de la législature à venir, de formuler des recommandations unanimes. Si notre commission autorise la publication du rapport, les recommandations qu'il contient, adoptées ce matin par la Mission, y gagneront encore en puissance, en crédibilité et en légitimité, et nos concitoyens trouveront dans ces travaux une nouvelle réponse tangible à leurs interrogations sur l'utilité des travaux parlementaires.

Nous cherchons précisément, madame Carrillon-Couvreur, à définir un modèle pertinent de partage des données personnelles médicales et médico-sociales, celui qui permettra de passer outre la mosaïque des structures, des forteresses qui se sont constituées, des corporatismes et des fonctionnements claniques dont nos concitoyens pâtissent, tant dans la prestations des soins que par la mauvaise utilisation des fonds publics induite.

Dans votre rapport d'information sur la mise en œuvre des missions de la CNSA dix ans après sa création, vous aviez fait le constat attristé que l'ambition initiale formulée pour l'institution – restaurer l'équité en matière médico-sociale sur l'ensemble du territoire – était contrariée par le retard considérable de ses systèmes d'information. Cela rendait ce géant aveugle et sourd, faute de disposer des données qui lui permettraient de définir une stratégie apte à répondre à la double tragédie de la dépendance et du handicap. Nous avons une sorte de génie pour bâtir des cathédrales dont le fonctionnement laisse ensuite pantois. Même si les données de santé et les données médico-sociales sont hétérogènes et éparpillées, l'interopérabilité s'impose pour réduire les délais d'accès, au bénéfice des patients souffrants ou handicapés dont on souhaite améliorer le sort. La prise en charge, dans le domaine médico-social, a été longtemps faite par les associations ; l'État ne s'est saisi que tardivement de la question. Une prise en charge globale est pourtant nécessaire, liant les aspects sanitaires et médico-sociaux de la condition des personnes.

L'entretien entre Didier Sicard et Nicolas Revel auquel vous vous êtes référé, Monsieur Tian, reflète le constat partagé de la lenteur de l'accès aux données de santé. Le législateur a voulu combler cette lacune en se donnant pour objectif de réduire à trois ou quatre mois la durée moyenne du délai de réponse à une demande d'accès, qui est actuellement d'une quinzaine de mois. Mais, pour les raisons que j'ai évoquées, quelques interrogations demeurent sur la fluidité réelle du dispositif mis en place sur le fondement de la loi de modernisation de notre système de santé.

L'augmentation considérable prévisible du volume de données collectées va aiguiser les appétits des opérateurs publics et des opérateurs privés qui concourent à l'« intérêt public » – notion dont il faudra préciser la portée juridique. Le risque d'un effet « entonnoir » demeure : si l'on substitue au contrôle *a priori*, l'une des causes d'embolisation du système, un contrôle *a posteriori* pour fluidifier le traitement des demandes d'autorisation d'accès, des moyens supplémentaires seront nécessaires, et ce sujet n'est pas traité.

Alors, comment faire, m'ont demandé MM. Tian et Perrut ? La commission des lois s'est saisie de cette question particulièrement évolutive. Deux options sont possibles. La première consiste en une révision générale du dispositif ; la seconde, plus immédiatement applicable, en des rectifications lors de l'élaboration des décrets d'application, ou par ordonnance pour ce qui concerne la transposition en droit interne du règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel qui sera applicable en 2018, afin de préciser les exigences de sécurité et de respect de la confidentialité des données de santé et de mentionner expressément qu'elles ne sauraient être exploitées à des fins mercantiles mais qu'elles doivent servir à l'élaboration de la politique de santé publique.

Ainsi parviendra-t-on, conformément au vœu exprimé par M. Dominique Tian, à une utilisation moins « *précautionneuse* », selon le terme choisi par la Cour des comptes, du trésor national que représente l'immense masse de données de santé dont nous disposons.

J'indique que ce rapport d'étape sera enrichi d'un glossaire des sigles employés et complété par quelques mots indiquant que la présente MECSS passe le relais à ses successeurs.

**Mme la présidente Catherine Lemorton.** Monsieur le rapporteur, je vous remercie.

*

* *

*La Commission autorise, à l'unanimité, la publication du rapport de la MECSS sur les données médicales personnelles inter-régimes détenues par l'assurance maladie, versées au SNIIRAM puis au Système national des données de santé (SNDS).*

# ANNEXES

## ANNEXE 1 : COMPOSITION DE LA MISSION

***Coprésidents***

Mme Gisèle BIÉMOURET (SRC) *(depuis le 8 octobre 2014)*

M. Pierre MORANGE (UMP)

***Membres***

***Groupe Socialiste, écologiste et républicain***

Mme Martine CARRILLON-COUVREUR

Mme Joëlle HUILLIER *(depuis le 8 octobre 2014)*

Mme Bernadette LACLAIS *(depuis le 8 octobre 2014)*

***Groupe Les Républicains***

M. Jean-Pierre DOOR

Mme Isabelle LE CALLENNEC

Mme Bérengère POLETTI

M. Dominique TIAN

***Groupe Union des démocrates et indépendants***

M. Francis VERCAMER

***Groupe Radical, républicain, démocrate et progressiste***

Mme Dominique ORLIAC

***Groupe Gauche démocrate et républicaine***

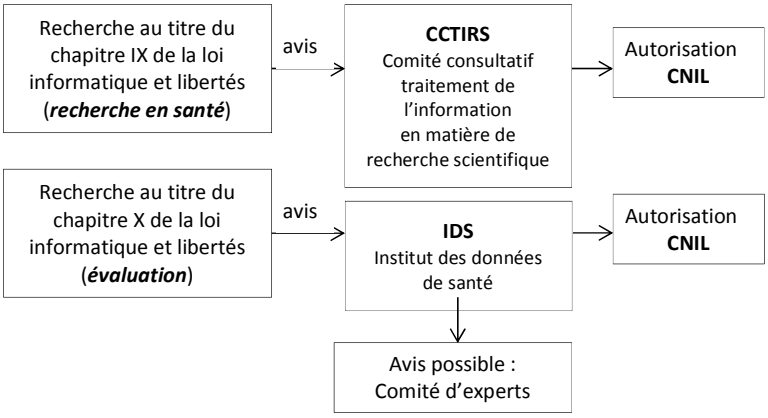
M. Jean-Philippe NILOR

***Non inscrit***

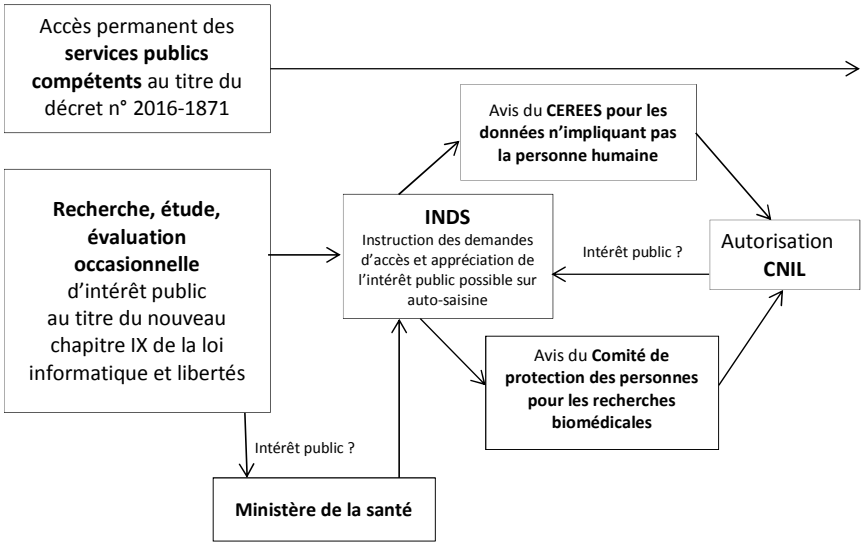
M. Jean-Louis ROUMÉGAS

## ANNEXE 2 : L'ACCÈS AUX DONNÉES DE SANTÉ

**Le dispositif actuel d'accès aux données :** 2 guichets




**Le dispositif à venir :** un guichet d'accès pour les recherches occasionnelles d'intérêt public et un accès permanent réservé aux services publics compétents en santé



## ANNEXE 3 : GLOSSAIRE DES SIGLES

| | |
|---|---|
| ALD | Affection de longue durée |
| AMM | Autorisation de mise sur le marché |
| ANSM | Agence nationale de sécurité du médicament et des produits de santé |
| ANSP | Agence nationale de santé publique |
| ANSSI | Agence nationale de la sécurité des systèmes d'information |
| ARS | Agence régionale de santé |
| ATIH | Agence technique de l'information sur l'hospitalisation |
| CADA | Commission d'accès aux documents administratifs |
| CASD | Centre d'accès sécurisé aux données |
| CCMSA | Caisse centrale de la Mutualité sociale agricole |
| CEREES | Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé |
| CIDS | Commission interministérielle de défense et de sécurité |
| CISS | Collectif interassociatif sur la santé |
| CMU-C | Couverture maladie universelle complémentaire |
| CNAMTS | Caisse nationale de l'assurance maladie des travailleurs salariés |
| CNIL | Commission nationale de l'informatique et des libertés |
| COG | Convention d'objectifs et de gestion |
| COPIIR | Comité d'orientation et de pilotage de l'information interrégimes |
| CPP | Comité de protection des personnes |
| CRIST | Centre de réponse aux incidents de sécurité informatique |
| DARES | Direction de l'animation de la recherche, des études et des statistiques |
| DCIR | *Datamart* de consommation interrégimes |
| DNS | Directive nationales de sécurité |
| DREES | Direction de la recherche, des études, de l'évaluation et des statistiques |
| DSSIS | Délégation / délégué à la stratégie des systèmes d'information de santé |
| EGB | Échantillon généraliste de bénéficiaires |
| EHPAD | Établissement d'hébergement pour personnes âgées dépendantes |
| ETP | Équivalent temps plein |
| FFA | Fédération française de l'assurance |
| FNMF | Fédération nationale de la mutualité française |
| GENES | Groupe des écoles nationales d'économie et de statistique |
| GIP | Groupement d'intérêt public |

| | |
|---|---|
| HAD | Hospitalisation à domicile |
| HAS | Haute autorité de santé |
| IDS | Institut des données de santé |
| INDS | Institut national des données de santé |
| INED | Institut national d'études démographiques |
| INSERM | Institut national de la santé et de la recherche médicale |
| IRDES | Institut de recherche et documentation en économie de la santé |
| LEEM | Les Entreprises du Médicament |
| LIL | Loi « Informatique et Libertés » [loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés] |
| MCO | Médecine-chirurgie-obstétrique |
| MDPH | Maisons départementales de personnes handicapées |
| MSA | Mutualité sociale agricole |
| NIR | Numéro d'inscription au répertoire [national d'identification des personnes physiques] |
| OIV | Opérateur d'importance vitale |
| ONDAM | Objectif national de dépenses d'assurance maladie |
| OSE | Opérateur de services essentiels |
| PIV | Point d'importance vitale |
| PMSI | Programme de médicalisation des systèmes d'information |
| PPP | Plan particulier de protection |
| PRADO | Programmes d'accompagnement des retours à domicile après hospitalisation |
| PSO | Plan de sécurité opérateur |
| RSA | Résumé de sortie anonyme |
| RSI | Régime social des indépendants |
| SAIV | Secteur d'activités d'importance vitale |
| SGMAP | Secrétariat général pour la modernisation de l'action publique |
| SIIV | Système d'informations d'importance vitale |
| SNDS | Système national des données de santé |
| SNIIRAM | Système national d'information inter-régimes de l'assurance maladie |
| SNITEM | Syndicat national de l'industrie des technologies médicales |
| SSR | Soins de suite et de réadaptation |
| UNOCAM | Union nationale des organismes complémentaires d'assurance maladie |
| UNPS | Union nationale des professionnels de santé |

## ANNEXE 4 : LISTE DES PERSONNES AUDITIONNÉES

L'ensemble des comptes rendus des auditions de la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale sont disponibles sur le portail de la MECSS :

http://www2.assemblee-nationale.fr/14/commissions-permanentes/commission-des-affaires-sociales/mecss/mission-d-evaluation-et-de-controle-des-lois-de-financement-de-la-securite-sociale

### Audition du 3 mai 2016

- Présentation de la communication de la Cour des comptes à la MECSS : M. Antoine Durrleman, président de la sixième chambre de la Cour des comptes, M. Didier Selles, conseiller-maitre, président de section, M. François de la Gueronnière et M. Alain Gillette, conseillers-maitres, Mme Delphine Rouilleault, auditrice, et Mme Clélia Delpech

### Audition du 6 décembre 2016

– Table ronde réunissant les assureurs, les mutuelles, les complémentaires santés :

- Mme Évelyne Guillet, directeur santé, Mme Florence Atger, chargée de mission santé, et Mme Miriana Clerc, directrice communication et relations institutionnelles du Centre technique des institutions de prévoyance (CTIP) ;
- Mme Véronique Cazals, directrice santé, Mme Cécile Malguid, sous-directrice santé, M. Jean-Paul Laborde, directeur des affaires parlementaires, et Mme Annabelle Jacquemin-Guillaume, conseillère parlementaire, direction des affaires parlementaires de la Fédération française de l'assurance (FFA) ;
- Mme Agnès Bocognano, directrice déléguée santé à la direction santé, M. Mathieu Cousineau, responsable Pôle métier assurances à la direction santé, et M. Valentin Jeufrault, chargé d'affaires publiques à la direction des affaires publiques de la Fédération nationale de la mutualité française (FNMF) ;
- M. Maurice Ronat, président, et M. Éric Badonnel, secrétaire général administratif de l'Union nationale des organismes d'assurance maladie complémentaire (UNOCAM)

### Auditions du 13 décembre 2016

- M. Philippe Burnel, délégué à la stratégie des systèmes d'information de santé (DSSIS), secrétariat général du ministère des affaires sociales et de la santé
- Dr Dominique Blum, praticien hospitalier

### Auditions du 20 décembre 2016

- Union nationale des professionnels de la santé – Dr William Joubert, secrétaire général, et M. Patrick Corne**,** membre de l'UNPS

- Direction de la recherche, des études, de l'évaluation et des statistiques (DREES) – M. Franck Von Lennep, directeur, et Mme Mylène Girard**,** chef de la mission « accès aux données de santé »
- Institut des données de santé (IDS) – Mme Chantal Cases, présidente, Mme Yvanie Caille, directrice générale, et Mme Valérie Edel, directrice adjointe

Audition du 10 janvier 2017

- Centre d'accès sécurisé aux données (CASD) – M. Kamel Gadouche, directeur, et M. Philippe Cunéo, directeur général du Groupe des écoles nationales d'économie et statistique (GENES)

Audition du 17 janvier 2017 matin

– Table ronde réunissant les acteurs de l'assurance maladie :

- M. Nicolas Revel, directeur général, M. Claude Gissot, directeur de la direction de la stratégie, des études et des statistiques, et Mme Véronika Levendof, responsable des relations avec le Parlement de la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) ;
- M. Alain Pelc, directeur chargé des études, des répertoires et des statistiques, M. Marc Rondeau, médecin conseiller technique national en charge de l'expertise médico-sociale individuelle, et M. Christophe Simon, chargé des relations parlementaires de la Caisse centrale de la Mutualité sociale agricole (CCMSA) ;
    - M. Olivier Aynaud, administrateur, et M. Pascal Perrot, médecin-conseil national et directeur de la gestion des risques et de l'action sociale à la caisse nationale du régime social des indépendants (RSI)

Audition du 17 janvier 2017 après midi

- M. Christian Babusiaux, ancien président de l'Institut des données de santé

Audition du 24 janvier 2017 matin

– Table ronde réunissant les laboratoires et industriels de la santé :

- M. Philippe Lamoureux, directeur général, M. Thomas Borel, directeur des affaires scientifiques du LEEM (Les Entreprises du Médicaments), M. Philippe Maugendre, directeur des relations gouvernementales de SANOFI ; Mme Muriel Carroll, directrice des affaires publiques du LEEM ;
- M. François-Régis Moulines, directeur des affaires gouvernementales et communication du syndicat national de l'industrie des technologies médicales (SNITEM) ; M. Christophe Roussel, membre du groupe affaires publiques du SNITEM et directeur du développement chez 3M France, département des systèmes d'information de santé/marchés de la santé ;
- M. Vincent Bildstein, président de IMS Health France ; Mme Michèle Arnoé, directrice innovation et croissance, et M. Étienne Lepoutre, directeur de Head of Real-World Insights France

Audition du 24 janvier 2017 après midi

- Commission nationale de l'informatique et des libertés (CNIL) – M. Édouard Geffray, secrétaire général, M. Thomas Dautieu, directeur-adjoint à la

direction de la conformité, et Mme Tiphaine Inglebert, conseillère pour les questions institutionnelles et parlementaires

Audition du 31 janvier 2017 matin

– Table ronde réunissant les réunissant les agences sanitaires :

- M. Dominique Martin, directeur général, Mme Carole Le-Saulnier, directrice des affaires juridiques et réglementaires, et M. Mahmoud Zureik, directeur scientifique et de la stratégie européenne de l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) ;
- Dr Jean-Claude Desenclos de l'Agence nationale de santé publique

Audition du 31 janvier 2017 après midi

- Dr Jacques Lucas, vice-président du Conseil national de l'Ordre des Médecins, délégué général aux systèmes d'information en santé ;

Audition du 7 février 2017

- Général Arnaud Martin, Haut fonctionnaire de défense et de sécurité / Pôle Sécurité défense – Secrétariat général des ministères chargés des affaires sociales, et M. Philippe Loudenot, fonctionnaire de sécurité des systèmes d'information (FSSI) pour les ministères chargés des affaires sociales ;