ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Compte rendu

Commission des affaires sociales

Mission d'évaluation et de contrôle des lois de financement de la sécurité sociale

Mardi
24 janvier 2017
Séance de 14 heures

Compte rendu n° 08

SESSION ORDINAIRE 2016-2017

Présidence de M. Pierre Morange, ***coprésident***

ASSEMBLÉE NATIONALE

COMMISSION DES AFFAIRES SOCIALES

MISSION D'ÉVALUATION ET DE CONTRÔLE DES LOIS DE FINANCEMENT DE LA SÉCURITÉ SOCIALE

Mardi 24 janvier 2017

La séance est ouverte à quatorze heures.

(Présidence de M. Pierre Morange, coprésident de la Mission)

La Mission d'évaluation et de contrôle des lois de financement de la sécurité sociale (MECSS) procède à l'audition, ouverte à la presse, de M. Edouard Geffray, secrétaire général, de M. Thomas Dautieu, directeur-adjoint à la direction de la conformité, et de Mme Tiphaine Inglebert, conseillère pour les questions institutionnelles et parlementaires de la Commission nationale de l'informatique et des libertés (CNIL).

M. le coprésident Pierre Morange, rapporteur. La mission d'évaluation et de contrôle des lois de financement de la Sécurité sociale poursuit ses travaux sur l'accès aux données médicales personnelles détenues par l'assurance maladie en accueillant, cet après-midi, M. Édouard Geffray, secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL), accompagné de M. Thomas Dautieu, directeur adjoint à la direction de la conformité, et de Mme Tiphaine Inglebert, conseillère pour les questions institutionnelles et parlementaires.

Madame, messieurs, je vous souhaite la bienvenue et vous prie d'excuser l'absence de Mme Gisèle Biémouret, coprésidente de la mission, qui est retenue par d'autres obligations liées à sa charge.

La CNIL est particulièrement concernée par l'article 193 de la loi de modernisation de notre système de santé, dont je rappelle qu'il vise à répondre à un certain nombre d'interrogations portant sur les données de santé gérées par l'assurance maladie, qu'il s'agisse de leur sécurité, de leur confidentialité, de l'amélioration des procédures d'accès et de gestion de ces données ou de l'efficience du modèle économique du Système national des données de santé (SNDS). Par ailleurs, la transposition dans notre droit de la réglementation européenne en la matière suscite des interrogations, de même que la gouvernance du dispositif, du fait de la multiplicité des opérateurs.

Je souhaiterais donc que vous nous fassiez une présentation aussi exhaustive et synthétique que possible de ces sujets d'autant plus complexes que nous devons anticiper le défi que représentent, d'une part, l'accumulation et l'agrégation de données dont le nombre augmente à une vitesse exponentielle, d'autre part, les risques de piratage informatique auxquels elles sont soumises.

M. Édouard Geffray, secrétaire général de la Commission nationale de l'informatique et des libertés. Je me propose de vous présenter, tout d'abord, un panorama général de la situation, avant de répondre aux questions que vous nous avez adressées. L'histoire des relations entre la CNIL et le Système national d'information inter-régimes de l'assurance maladie (SNIIRAM) – qui deviendra bientôt le SNDS – est, non pas, comme on le croit parfois, celle d'un blocage, mais celle de l'ouverture progressive et raisonnée d'une base de données considérable, extrêmement riche, précise et individualisée, qui suscite, de ce fait,

des appétits légitimes – dès lors qu'il s'agit de servir l'intérêt public – et d'autres moins légitimes.

La CNIL a toujours accompagné l'ouverture de l'accès du SNIIRAM à la recherche. Cette ouverture s'est faite, d'abord, par l'extension du périmètre des recherches que l'on pourrait qualifier de plein droits, dans le cadre du fameux arrêté SNIIRAM de juillet 2013 modifié relatif à sa mise en œuvre . Celui-ci a, en effet, été régulièrement aménagé, après avis de la CNIL, laquelle a systématiquement conclu à la possibilité de cette extension moyennant des conditions particulières. Au-delà de ces accès de plein droit, la CNIL délivre ponctuellement des autorisations d'accès au SNIIRAM. Le nombre de ces autorisations est moins important qu'on pourrait le penser puisque, depuis 2012, nous avons reçu environ 180 demandes qui ont toutes été acceptées.

M. le coprésident Pierre Morange, rapporteur. Les organismes agréés, qui disposent à ce titre d'un accès permanent au SNDS, sont-ils soumis au contrôle de la CNIL ?

M. Édouard Geffray. À l'avenir, la CNIL n'exercera plus de contrôles *a priori* ; elle devra donc développer les contrôles *a posteriori* alors que, jusqu'à présent, son effort portait, pour des raisons de moyens, sur l'amont plutôt que sur l'aval.

M. le coprésident Pierre Morange, rapporteur. Votre réponse me conduit à vous interroger sur les moyens de la CNIL, dont j'ai cru comprendre qu'ils étaient quelque peu contingentés. On peut en effet espérer qu'ils soient beaucoup plus importants dès lors que, pour améliorer les procédures, le contrôle s'exercera *a posteriori*. Quels devraient-ils être, selon vous ?

M. Édouard Geffray. Nous pouvons toujours réorienter des agents de la CNIL vers d'autres missions. C'est ce que nous faisons actuellement dans le cadre du contrôle du SNIIRAM, qui a été inscrit au programme des contrôles annuels de l'année 2017. Cependant – et notre présidente s'en est récemment ouverte à la commission des lois lors de son audition –, la situation de la CNIL est actuellement extrêmement tendue en termes de moyens. De fait, nous traitons annuellement 100 000 déclarations, 3 000 autorisations, 8 000 à 9 000 plaintes et 6 000 demandes de droit d'accès indirect. Par ailleurs, 18 000 organismes ont désigné un correspondant informatique et libertés (CIL) et nous avons effectué 550 contrôles sur place ou en ligne, ainsi que 100 mises en demeure. Le volume de notre activité – qui concerne aussi bien la santé que les « GAFA », acronyme pour Google, Apple, Facebook, Amazon, ou la sécurité publique – est donc considérable ! Aujourd'hui, pour traiter l'ensemble de ces dossiers, le régulateur dispose d'environ 195 équivalents temps plein travaillé (ETPT), soit 195 agents permanents. Comme je le disais, nous pouvons, pour répondre aux demandes des citoyens ou du législateur, réaffecter ponctuellement certains agents, mais cela reviendra bientôt à déshabiller Pierre pour habiller Paul.

M. le coprésident Pierre Morange, rapporteur. Quel est le nombre des agents spécifiquement affectés au domaine de la santé ?

M. Édouard Geffray. Le service de la santé, qui a été récemment renforcé, compte huit agents. Outre l'amont, c'est-à-dire notamment les autorisations de recherche, ce service se consacre à l'accompagnement et à la mise en conformité, qui consistent à répondre aux demandes de conseil des organismes ou des chercheurs qui souhaitent se mettre en conformité avec la loi « Informatique et libertés ». Pour ce qui est de l'aval, c'est-à-dire les contrôles-sanctions, les fonctions étant moins spécialisées, nous réorientons des agents en fonction de

l'activité. Dans le cadre du contrôle du SNIIRAM, par exemple, nous allons mobiliser trois ou quatre agents. J'ajoute, pour être complet, que le service des contrôles de la CNIL comprend 22 équivalents temps plein et effectue 550 contrôles par an, dont, l'année dernière, Microsoft, Facebook et Google…

M. le coprésident Pierre Morange, rapporteur. Quel serait selon vous, le nombre d'agents nécessaires pour que la CNIL soit véritablement opérationnelle en matière de contrôles *a posteriori* ?

M. Édouard Geffray. Le dernier plan triennal d'orientations stratégiques et opérationnelles de la CNIL, qui portait sur les années 2015 à 2017, s'est traduit, en moyenne, par six créations de poste par an, sachant que les projections que nous avions effectuées pour anticiper l'augmentation de notre activité n'incluaient pas toutes les missions nouvelles qui nous ont été confiées depuis par le législateur. À titre personnel, j'estime que le futur plan triennal, pour les années 2017 à 2019, devrait au moins maintenir cette tendance car, aujourd'hui, nous parvenons à « tenir » grâce à ces cinq créations de poste par an. Je précise, à titre d'exemple, que notre homologue britannique emploie 360 agents.

Encore une fois, les contrôles *a posteriori* nous offrent davantage de souplesse : nous pouvons décider de les concentrer sur tel secteur plutôt que sur tel autre et remobiliser ainsi ponctuellement des moyens. Mais, si nous voulons atteindre un niveau d'exigence suffisamment élevé et universel, il est évident que nous aurons besoin de renforcer ces équipes.

J'en reviens à l'histoire des relations entre la CNIL et le SNIIRAM. Le niveau de sécurité suscite des interrogations, qui ont du reste été soulignées par la Cour des comptes.

M. le coprésident Pierre Morange, rapporteur. Quel est votre avis à ce sujet ?

M. Édouard Geffray. La CNIL a toujours clairement affirmé que le niveau de sécurité du SNDS devait être amélioré. Nous l'avons d'ailleurs indiqué à la Cour des comptes, laquelle est parvenue aux mêmes conclusions par ses propres moyens. Cette situation explique en partie qu'historiquement, l'ensemble de l'écosystème ait touché à cet outil avec prudence. Nous sommes en effet dans un monde où les questions de sécurité prennent des proportions considérables. Ainsi, nous effectuons 500 contrôles par an et, dans 85 % des cas, nous sommes amenés à émettre des recommandations, des injonctions ou des mises en demeure relatives à la sécurité informatique. Nous devons donc être collectivement attentifs à cette question, d'autant plus que la France est un peu faible dans ce domaine. S'agissant d'une base de données telle que celle du SNIIRAM, dont on connaît la richesse et la sensibilité, nous ne pouvons pas prendre le risque de subir un jour une attaque informatique majeure.

Une triple réponse doit être apportée. La première consiste dans une amélioration de l'architecture et de la sécurisation technique du SNDS qui, à ma connaissance, est en cours puisqu'un projet de texte nous a été transmis. Le contrôle que nous effectuons actuellement au SNIIRAM porte d'ailleurs notamment sur le volet « sécurité ».

La deuxième réponse, d'ordre juridique, est apportée par la loi de modernisation de notre système de santé et ses textes d'application. Ce cadre juridique est toutefois encore en devenir puisque tous les décrets n'ont pas paru : le Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (CEREES) n'est pas encore opérationnel

et nous n'avons pas expérimenté la nouvelle procédure. Il serait donc hasardeux de porter un jugement définitif sur celle-ci.

M. le coprésident Pierre Morange, rapporteur. Je rappelle que, pour renforcer sa sécurité informatique, la Cour des comptes préconise d'élever le SNDS au rang d'opérateur d'importance vitale. Quel est votre sentiment sur cette proposition ? Je rappelle que le directeur général de la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS) est mesuré sur le sujet ; il considère que les incidences ne sont pas les mêmes pour cette base de données que pour des industries stratégiques telles que l'électricité ou la défense. Il s'agit néanmoins de données importantes et sensibles qui peuvent être utilisées à des fins lucratives dans le cadre, soit d'un piratage, soit d'une exploitation assurantielle dont l'enjeu pourrait être une remise en cause du principe de mutualisation du risque par la déclinaison d'une offre dépendant du profil de chaque patient.

M. Édouard Geffray. Je distinguerai deux éléments. 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 !

M. le coprésident Pierre Morange, rapporteur. Le ministre de la défense a indiqué qu'au cours de l'année 2016, 24 000 attaques informatiques avaient été déjouées. Avez-vous connaissance d'éléments similaires dans le domaine de la protection sanitaire et sociale ?

M. Édouard Geffray. 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.

M. le coprésident Pierre Morange, rapporteur. Pourriez-vous préciser le cadre juridique tel qu'il est défini par la réglementation française et la réglementation européenne, qui est plus restrictive ?

M. Édouard Geffray. 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.

M. le coprésident Pierre Morange, rapporteur. Actuellement, les producteurs de données fournissent des données à un opérateur qui peut éventuellement les réaffecter à des tiers. Or, cette pratique est totalement orthogonale à la réglementation européenne.

M. Édouard Geffray. Pas forcément, en ce sens que 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. Concrètement, 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…

La troisième réponse relève de la régulation : que fait la CNIL dans cet environnement ? Outre son action en aval, c'est-à-dire les contrôles *a posteriori*, elle est chargée de délivrer des autorisations, d'une part, en matière de recherche dans le domaine de la santé, d'autre part, aux organismes qui ne sont pas considérés par la loi comme ayant un accès de plein droit aux données du SNDS mais qui peuvent, pour un motif d'intérêt public, mener des recherches à partir de ces données.

Dans ce dernier cas, le schéma habituel est un schéma d'autorisation individuelle. Concrètement, une entreprise ou un organisme soumettra son projet de recherche à l'Institut national des données de santé (INDS) puis le CEREES l'examinera et enfin la CNIL s'assurera que les conditions de protection des données sont suffisantes et lui accordera ou non l'autorisation. Nous souhaitons donc construire autant que possible des actes-cadres, appelés méthodologies de référence ou autorisations uniques. Ces deux outils juridiques permettent aux organismes traitant tel type de données dans telles conditions d'éviter de suivre une procédure individualisée à la CNIL dès lors qu'ils s'engagent à agir en conformité avec le cadre défini, leur activité pouvant bien entendu être contrôlée.

M. le coprésident Pierre Morange, rapporteur. Quelle est la valeur de cet engagement au plan juridique ?

M. Édouard Geffray. Cet engagement est contraignant car s'il apparaît, lors d'un contrôle *a posteriori*, que l'entité ne le respecte pas, nous sommes en droit de lui infliger une

sanction dont le montant maximal, actuellement de 3 millions d'euros, sera porté, lorsque le règlement européen entrera en vigueur, à 20 millions d'euros ou 4 % de son chiffre d'affaires mondial.

Nous avons d'ores et déjà adopté, en août dernier, deux méthodologies de référence ; le 31 décembre, soit quatre mois plus tard, nous avions reçu presque 600 engagements de conformité à ces deux méthodologies. Ainsi, non seulement nous évitons aux opérateurs de suivre la procédure d'autorisation individuelle, longue à instruire, mais nous dégageons des moyens qui nous permettent de concentrer une ressource rare sur les cas plus atypiques ou qui auraient fait l'objet d'une appréciation plus réservée du CEREES, par exemple.

Ces trois réponses – sécurité, évolution du cadre juridique et simplification des procédures par le régulateur – doivent être conjuguées si nous voulons répondre à la volonté du législateur et nous assurer que les données seront traitées dans un cadre sûr pour nos concitoyens.

J'en viens au questionnaire que vous nous avez adressé.

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.

M. le coprésident Pierre Morange, rapporteur. Au-delà du débat sur la définition de l'intérêt public, qui est à géométrie variable, les dérogations que vous évoquez doivent être analysées à la lumière du respect du secret professionnel. Où placer le curseur, dès lors que la réutilisation des données se fait à l'insu de leurs producteurs ?

M. Édouard Geffray. 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. En outre, nous avons insisté pour qu'il soit possible de sanctionner un ré-utilisateur qui utiliserait des données qui ne sont pas

directement identifiantes aux fins de ré-identifier des personnes. Il nous semble en effet nécessaire de sécuriser et l'amont et l'aval : en amont, l'entité qui met les données à disposition doit le faire dans un cadre protecteur ; en aval, il faut pouvoir interdire au ré-utilisateur de se servir de ces données pour retrouver l'identité d'une personne qui, par exemple, a été hospitalisée pour un panaris du 3 au 5 juin 2015.

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.

Par ailleurs, les données du SNDS ont, par nature, un caractère personnel, dans la mesure où elles sont relatives à des personnes directement ou, en l'espèce, indirectement indentifiables. Selon nous, il n'y a pas de débat juridique sur ce point, au demeurant important car il détermine notre champ de compétence. Ainsi, lorsque nous contrôlerons le SNDS, nous contrôlerons l'ensemble du SNDS. Cependant, ces données personnelles telles qu'elles sont mises à disposition sont plus ou moins individualisées. Si elles prennent la forme d'agrégats, elles ne sont pas individualisables et la sécurité est maximale ; si elles sont individualisables, elles doivent faire l'objet d'une protection renforcée.

J'en viens à l'appréciation de l'intérêt scientifique. En fait, la question sous-jacente est celle de savoir si la CNIL se prononce sur l'intérêt scientifique du projet. La réponse est : *a priori* non ; cela n'entre pas dans notre champ de compétence. C'est au Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé (CCTIRS) aujourd'hui, au CEREES demain, de se prononcer sur ce point. La CNIL, quant à elle, définira, en tenant compte de l'appréciation portée par le comité, les conditions de traitement des données. Elle peut ainsi, le cas échéant, fixer des bornes. Je pense à un projet portant sur l'étude du génome d'une certaine catégorie de population définie par son origine. L'intérêt scientifique du projet avait été reconnu ; la CNIL a précisé que ces travaux ne pouvaient être utilisés pour établir que telle personne appartenait à telle population. L'intérêt scientifique ne relève donc pas de la CNIL, qui se prononce, en revanche, sur l'intérêt sociétal, lequel commande de ne pas sortir des frontières de la science en permettant à d'autres d'utiliser des données à mauvais escient, notamment dans des perspectives extrêmement dolosives.

En ce qui concerne l'articulation entre les différents acteurs, je rappelle que la CNIL délivre une autorisation à la personne qui va consulter la base du SNDS : soit cette autorisation est respectée, soit elle ne l'est pas et la personne peut alors être sanctionnée. Il n'y a donc ni négociation, ni convention. Une fois qu'elle a obtenu cette autorisation, l'entité se tourne vers le SNDS et le responsable de traitement, c'est-à-dire la CNAMTS. Celle-ci, je le précise, travaille actuellement à la rédaction d'une convention avec l'INSERM, qui assurera une partie de la gestion des droits d'accès. Concrètement, il ouvrira telle boîte pour accéder à tel type de données.

Quant à la question de savoir si le CEREES doit avoir la personnalité juridique, je ne crois pas que ce soit une obligation légale. Il peut en effet être rattaché à la personne morale qu'est l'État, à l'instar de la CNIL, par exemple.

M. le coprésident Pierre Morange, rapporteur. Qu'en est-il de l'accès au SNDS des assurés, des patients et des professionnels de santé personnellement désignés par les données de santé ? Ont-ils un droit de consultation et de rectification, voire d'opposition au traitement des données qui les concernent ?

M. Édouard Geffray. L'alimentation du SNDS est de plein droit. Bien entendu, tout un chacun peut exercer ses droits d'accès et de rectification. Quant au droit d'opposition, il ne peut pas être exercé s'agissant des traitements nécessaires à l'accomplissement des missions des services de l'État, des établissements publics ou des organismes chargés d'une mission de service public, c'est-à-dire les opérateurs bénéficiant d'un accès permanent au SNDS. En d'autres termes, le droit d'accès et de rectification est universel ; le droit d'opposition ne peut être exercé qu'en cas de traitement à des fins de recherche, d'étude ou d'évaluation, prévu au III de l'article L. 1461-1 du code de la santé publique, c'est-à-dire aux traitements soumis à autorisation de la CNIL.

M. le coprésident Pierre Morange, rapporteur. Cela suppose cependant que la personne concernée soit informée de l'existence d'une telle étude.

M. Édouard Geffray. L'effectivité des droits se heurte, en effet, parfois au déficit d'information. C'est un obstacle qui, hélas !, n'est pas anecdotique dans le domaine de l'informatique et des libertés. En tout état de cause, cette règle permet de préserver l'intégrité de la base, indispensable à la mise en œuvre de la politique de santé, tout en permettant aux individus d'exercer leurs droits lorsque l'usage de leurs données, quoique d'intérêt public, est davantage privatif.

M. le coprésident Pierre Morange, rapporteur. Le règlement européen exige la restitution d'une information qui, de fait, n'est pas partagée. Cette zone d'ombre devra impérativement être éclairée.

M. Édouard Geffray. De manière générale, l'information soulève en effet un véritable problème.

M. Gérard Bapt. Un article de la loi de modernisation du système de santé dispose que tous les incidents de sécurité doivent être rapportés à l'ARS, qui les agrège au niveau national. Les incidents peuvent concerner le système d'information lui-même ou résulter d'une effraction qui donne accès à des données personnelles. Dans le second cas, la CNIL sera-t-elle saisie de ces incidents ?

M. Édouard Geffray. Dans le cadre juridique actuel, non. À compter du 25 mai 2018 et de l'entrée en vigueur du règlement européen, toute faille de sécurité, qu'il s'agisse d'une défaillance du système lui-même, d'une effraction ou du comportement négligent d'un agent – dont je précise qu'il est à l'origine de 43 % des failles de sécurité –, devra être notifiée à la CNIL. En outre, s'il apparaît que cette faille a un effet sur la vie privée des personnes, elle leur sera obligatoirement notifiée également. C'est pourquoi il est important que le niveau de sécurité du SNDS, notamment le chiffrement des données, soit extrêmement élevé. En effet, si les données sont rendues quasiment illisibles, le hacker renoncera à les décrypter et le risque pour la personne sera donc quasiment nul : il ne sera pas nécessaire de lui notifier la faille. En revanche, si les bases sont stockées dans des conditions de chiffrement précaires ou dépassées – ce que nous constatons, hélas !, régulièrement lors de nos contrôles – et que le pirate est en mesure de voir les données en clair, il faudra notifier l'information aux personnes concernées.

M. le coprésident Pierre Morange, rapporteur. Deux questions, pour terminer. Pourquoi est-ce la CNIL et non le comité du secret statistique qui définit les agrégations qui rendent les données du SNDS anonymes ? À ce propos, le Centre d'accès sécurisé aux données (CASD) a un modèle informatique particulier qui présente un niveau de sécurité pertinent. Ce modèle vous semble-t-il devoir être partagé ? Par ailleurs, quel est votre sentiment sur l'efficience du modèle économique de gestion de ces données ? Nous avons évoqué la nécessité d'augmenter le nombre des agents de la CNIL pour répondre aux objectifs de la loi. Or, il est évident que les dotations budgétaires doivent être complétées par un mode de rémunération lié à l'accès à ces données.

M. Édouard Geffray. Il m'est plus facile de répondre à votre première question qu'à la seconde. Tout d'abord, le comité du secret statistique n'est compétent qu'en matière de statistique publique. La compétence de la CNIL, quant à elle, dépend du caractère anonyme ou non des données, qui détermine le champ d'application de la loi « Informatique et libertés ». Si les données ne sont pas anonymes – quand bien même seraient-elles « pseudonymisées », hachées, etc. –, elles entrent dans le champ de cette loi et relèvent de donc de la CNIL ; si elles sont complètement anonymes, elles en sont exclues. C'est pourquoi le législateur a toujours confié le soin à la CNIL de déterminer le caractère anonyme ou non des données. Du reste, la loi pour une République numérique de 2016 l'a également chargée d'homologuer des méthodologies d'anonymisation. Pour répondre à votre première question, nous avons des liens très étroits avec le comité du secret statistique, mais nous n'avons ni le même métier ni le même champ d'intervention.

Quant au CASD, c'est un système dont la CNIL a dit publiquement qu'il était conforme à la loi « Informatique et libertés ». Il n'a pas forcément vocation à être le réceptacle de toutes les données mais, dans son concept et sa mécanique, il est objectivement intéressant de par les conditions de sécurité qu'il garantit, puisqu'il fonctionne *grosso modo* sur le modèle de la chambre noire du photographe : il permet de ne sortir que la photographie, toutes les pellicules restant à l'intérieur.

Enfin, la question de l'efficience du modèle économique renvoie à celle, plus large, de la gratuité de la donnée publique. Le problème n'est pas propre à la santé ; il concerne tout l'open data. La CNIL n'a pas, en tant que telle, à se prononcer sur le sujet. Toutefois, il est nécessaire de trouver un équilibre entre, d'un côté, l'open data et les avantages qu'il présente pour le renouvellement des modalités de contrôle de l'action publique – qui est l'un des principes fondamentaux de notre contrat social – et, de l'autre, le coût de la mise à disposition de ces données, dont d'autres vont tirer un bénéfice commercial. Selon la théorie économique, ces derniers étant ensuite amenés à payer des impôts, le bénéfice serait *in fine* infiniment plus important que le coût de la mise à disposition initiale. Je n'ai pas lu d'ouvrages qui permettent de le démontrer, mais il faut envisager l'équilibre de manière globale. Quoi qu'il en soit, ce n'est pas à moi de dire ce qui est rentable ou non en la matière.

M. le coprésident Pierre Morange, rapporteur. Je vous remercie pour la précision de vos réponses, que vous pourrez compléter par écrit. À ce propos, je rappelle que la MECSS souhaite que ses travaux soient opérationnels. Par conséquent, nous serons très attentifs aux préconisations ou aux propositions pragmatiques que vous pourriez nous soumettre.

Pour conclure, je précise que nous présenterons, au mois de février, un prérapport à la commission des affaires sociales. En effet, les décrets d'application de la loi de modernisation du système de santé n'étant pas encore tous parus, le rapport ne pourra être finalisé que sous la prochaine législature.

La séance est levée à quinze heures.