ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Compte rendu

Commission des affaires sociales

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

Auditions, ouverte à la presse, sur les données médicales personnelles inter-régimes détenues par l'assurance maladie, versées au SNIIRAM puis au Système national des données de santé (SNDS) *(M. Pierre Morange, rapporteur)* :

Mardi
7 février 2017
Séance de 10 heures 30

Compte rendu n° 11

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 7 février 2017

La séance est ouverte à dix heures trente-cinq.

(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, du 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.

M. le président Pierre Morange, rapporteur. Nous poursuivons nos travaux sur les données médicales personnelles versées au Système national d'information inter-régimes de l'assurance maladie (SNIIRAM), puis au Système national des données de santé (SNDS). Nous avons le plaisir d'accueillir le général Arnaud Martin, haut fonctionnaire adjoint de défense et de sécurité au pôle « défense et sécurité » du 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

Nous sommes, en quelque sorte, au milieu du gué du processus d'ouverture des données de santé. La Cour des comptes a publié un rapport sur la question en mars 2016, à la suite de l'adoption de la loi du 26 janvier 2016 de modernisation de notre système de santé, dont l'article 193 porte sur la mise à disposition des données de santé. Pour sa part, la MECSS a traité une partie du sujet au travers des auditions qu'elle a menées, sachant que nous avançons en marchant, puisque plusieurs décrets d'application doivent encore être pris – certains décrets ont été publiés le 26 décembre 2016. Compte tenu des échéances électorales, la MECSS rédigera un pré-rapport qu'elle présentera à la commission des affaires sociales d'ici la fin du mois, avant la suspension des travaux du Parlement. Notre ambition est que le rapport définitif soit rédigé pour la fin de l'année 2017 ou le début de l'année 2018, mais tout dépendra des futurs représentants désignés par le peuple.

Le sujet est très vaste, non seulement parce que le SNDS sera l'une des bases de données les plus importantes d'Europe, voire du monde – il sera enrichi par les données du Centre d'épidémiologie sur les causes médicales de décès (CépiDc), par un échantillon des données de remboursement des assurances complémentaire et, à terme, par des données médico-sociales, – mais aussi en raison des problèmes soulevés : prise en compte des évolutions technologiques, articulation avec les objets connectés – dont le nombre sera multiplié par cinquante au cours des cinq prochaines années –, protection contre la piraterie informatique. Cette dernière n'est plus seulement théorique, ainsi que l'ont signalé différents ministères. Avez-vous eu connaissance d'éventuelles attaques informatiques dans le domaine de compétence du ministère des affaires sociales et de la santé ?

La Cour des comptes a subdivisé ce sujet en quatre grands thèmes.

Premier thème : la sécurité des méthodologies utilisées ou, en d'autres termes, la qualité du « coffre-fort informatique » renfermant ces données. À cet égard, quel est votre sentiment sur la solidité de l'algorithme FOIN (fonction d'occultation des identifiants nominatifs) ? Que pensez-vous des préconisations de la Cour des comptes visant à élever le niveau de sécurité, notamment de sa recommandation de reconnaître à la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS) la qualité d'opérateur d'importance vitale ?

Deuxième thème : la confidentialité des données, qui passe par leur pseudonymisation et leur cryptage. Les techniques de chaînage ne présentent-elles pas quelques faiblesses ?

Troisième thème : l'exploitation des données. Elle demeure insuffisante, d'où les nouvelles dispositions de la loi de modernisation de notre système de santé. La procédure proposée vous semble-t-elle suffisamment solide et efficiente ? Que pensez-vous notamment du contrôle *a posteriori* ? Disposons-nous des moyens humains, techniques et financiers nécessaires à cette fin ?

Quatrième thème : le modèle économique. Cette question est sans doute à la marge de votre domaine de compétence, mais elle renvoie au problème de la sécurisation de l'accès à des données très sensibles, notamment au moyen d'un certain nombre de pare-feu.

M. Arnaud Martin, haut fonctionnaire adjoint de défense et de sécurité au pôle « défense et sécurité » du secrétariat général des ministères chargés des affaires sociales. En préambule, je réaffirme que les ministères sociaux, notamment celui des affaires sociales et de la santé, prennent bien en compte tous les enjeux relatifs à la sécurité des systèmes d'information, notamment des bases de données de santé. La question est traitée au plus haut niveau du ministère. Philippe Loudenot, spécialiste de ce dossier, qu'il suit depuis de nombreuses années, sera en mesure de vous apporter un éclairage sur toutes les questions de nature technique.

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.

M. le président Pierre Morange, rapporteur. Si j'ai bien saisi le sens de votre propos, votre réserve porte non seulement sur la forme – vous n'êtes pas favorables au classement de la CNAMTS parmi les OIV –, mais aussi sur le fond : le niveau de sécurité qui doit être celui d'un OIV ne vous semble pas forcément le plus adapté pour répondre à l'exigence de sécurité des données de santé.

M. Arnaud Martin. 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.

M. le président Pierre Morange, rapporteur. Quel est votre sentiment, monsieur Loudenot, en ce qui concerne la qualité du « coffre-fort informatique » ? Que pensez-vous des remarques de la Cour des comptes à propos de l'obsolescence de certains algorithmes ? Compte tenu de la sensibilité des données de santé, quel est votre avis sur les différents modèles de sécurité informatique, notamment sur celui du Centre d'accès sécurisé aux données (CASD) ? Le CASD suit une procédure différente de celle de la CNAMTS, bien qu'il exploite lui aussi des données de santé, celles du programme de médicalisation des systèmes d'information (PMSI).

M. Philippe Loudenot, fonctionnaire de sécurité des systèmes d'information pour les ministères chargés des affaires sociales. 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 CNAMTS a d'ores et déjà inscrit à son programme de travail la modification et l'évolution de l'algorithme de chiffrement.

Concernant la méthodologie qui a été appliquée, un travail commun a été lancé d'entrée de jeu avec la direction de la recherche, des études, de l'évaluation et des statistiques (DREES), c'est-à-dire avec M. Franck Von Lennep et ses équipes. Nous nous sommes appuyés sur un marché interministériel en matière de sécurité des systèmes d'information, afin de disposer d'une analyse des risques et d'engager nos travaux de manière cohérente. Ces travaux, qui ont été menés tout au long de l'année 2016 et se sont achevés au début de l'année 2017, nous ont permis d'établir un référentiel de sécurité, en prenant en compte tant le point de vue des techniciens que celui des utilisateurs « métiers », qui est le plus important, car il s'agit de déterminer ce que l'on veut protéger et à quel niveau.

Dans la mesure où le SNIIRAM, le SNDS et le PMSI comportent des données nominatives, ces travaux ont été supervisés par la Commission nationale de l'informatique et des libertés (CNIL). Celle-ci nous a aidés dans la phase initiale, puis s'est mise en retrait – ce

qui est tout à fait normal, car elle ne peut pas être à la fois juge et partie. Enfin, elle a porté un jugement sur le projet d'arrêté fixant le référentiel de sécurité que j'ai évoqué. Tous les éléments pertinents ont été pris en compte, y compris le règlement européen sur la protection des données personnelles, qui sera appliqué dès 2018. Il n'était pas question de le mettre de côté temporairement ; il reste néanmoins quelques ajustements à faire.

Dans ce référentiel, nous sommes notamment passés du contrôle déclaratif au contrôle *a posteriori*, ce qui est, selon moi, une excellente chose en matière de sécurité. Cela permet d'aller voir à un moment donné ce qui se passe réellement sur le terrain et, le cas échéant, si quelqu'un se fait prendre « la main dans le pot de confitures », de le sanctionner comme il se doit.

M. le président Pierre Morange, rapporteur. Selon vous, les moyens sont-ils suffisamment étoffés pour relever le défi du contrôle *a posteriori* ?

M. Philippe Loudenot. Nous avons mis en place un comité d'audit, dont je vais assurer la présidence, et dans lequel siégeront des représentants de la DREES, de la CNAMTS, de l'ANSSI, de la CNIL et, je présume, de l'Institut national des données de santé (INDS). Tous les travaux seront menés en parfaite intelligence.

S'agissant des moyens, le seul organisme disposant de réels pouvoirs de sanction est la CNIL. Ces pouvoirs seront renforcés par le règlement européen.

M. le président Pierre Morange, rapporteur. Selon certains, la notion d'intérêt général est envisagée de manière plus restrictive dans le règlement européen que dans la réglementation française, laquelle est encore en devenir, ainsi que je l'ai évoqué dans mon propos liminaire.

D'autre part, les moyens de la CNIL sont, on le sait, relativement limités, et la question des moyens ouvre sur celle du financement et du modèle économique. Vous allez sans doute me dire que ces questions ne relèvent pas de votre domaine de compétence, mais cela ne vous interdit pas d'y réfléchir, notamment au regard des modèles existant ailleurs en Europe. Quel dispositif vous semblerait le plus pertinent ou le plus efficient ? En tant que spécialiste de la sécurité informatique, avez-vous fait une extrapolation, tenant compte de la masse des données, du nombre de personnes intéressées – physiques ou morales – et des évolutions technologiques en matière de traitement des données dématérialisées, afin de déterminer les moyens nécessaires pour assurer un contrôle *a posteriori* efficace, c'est-à-dire dissuasif, car réactif et à même d'évaluer la pertinence des demandes d'accès aux données et d'empêcher un éventuel dévoiement de leur esprit initial ?

M. Philippe Loudenot. D'expérience, il me semble qu'un véritable contrôle *a posteriori* offre beaucoup plus de souplesse et se révèle beaucoup moins chronophage et coûteux, notamment en moyens humains, que le contrôle *a priori*. Alors que le contrôle *a priori* mobilise un certain nombre de personnes au même moment pour traiter un dossier, le contrôle *a posteriori* consiste à réaliser des audits à un instant « t », avec des membres de la CNIL, en demandant le cas échéant l'appui de l'ANSSI ou en recourant à un marché interministériel en matière de sécurité des systèmes d'information.

Autre avantage : le contrôle *a priori* reste trop souvent un contrôle déclaratif, sans que personne ne procède à des vérifications par la suite ; avec le contrôle *a posteriori*, nous disposerons d'une image photographique de la réalité sur le terrain.

La CNIL dispose en son sein d'une équipe dédiée au secteur de la santé. Il ne m'appartient pas de m'exprimer en son nom.

M. le président Pierre Morange, rapporteur. La CNIL a souhaité un renforcement de ses moyens et de ses effectifs. Jusqu'à présent prévalait une sorte de principe « de l'entonnoir » : pour accéder aux données, il n'y avait pas d'autre solution que d'obtenir une autorisation de la CNIL, et les délais d'instruction étaient un peu étirés – pour le dire en termes diplomatiques. Mais l'entrée en vigueur de l'article 193 de la loi de modernisation de notre système de santé va améliorer la fluidité des procédures : le contrôle *a posteriori* permettra de gérer un nombre beaucoup plus important de dossiers de recherche, publique ou privée, l'objectif étant de développer l'exploitation des données, que chacun s'accorde à trouver insuffisante aujourd'hui. De votre point de vue, les moyens actuels sont-ils suffisants ? On pourrait imaginer, par exemple, que vous soyez favorable à un doublement des effectifs. Il s'agit d'une question importante pour les représentants de la Nation que nous sommes : il nous reviendra, le cas échéant, d'appeler l'attention de l'exécutif sur la nécessité de renforcer les moyens pour remplir cette mission.

M. Philippe Loudenot. S'agissant des contrôles en matière de sécurité des systèmes d'information ou d'utilisation de ces systèmes, nous faisons le même constat dans la plupart des ministères : de nombreux services ont été débordés par des événements, cyberattaques ou actes de cybercriminalité, et tout le monde essaie de renforcer ses troupes. Ainsi que l'a rappelé le général Martin, le ministère des affaires sociales et de la santé met tout en œuvre pour élever le niveau de sécurité de l'ensemble de son périmètre. J'en veux pour preuve l'article 110 de la loi de modernisation de notre système de santé, issu d'un amendement déposé par M. Gérard Bapt : la santé est le seul secteur ministériel où il sera bientôt obligatoire de déclarer les incidents de sécurité affectant les systèmes d'information. Auparavant, cette déclaration obligatoire ne concernait que les OIV et les opérateurs visés par les « paquets télécom » européens. Cette disposition s'appliquera à tous les établissements de santé dès le 1er octobre prochain. En ce qui concerne la CNAMTS, tout est prévu dans les textes relatifs au comité d'audit, qui seront publiés prochainement.

En ce qui concerne les moyens humains nécessaires à la CNIL et à l'ANSSI, la souplesse du contrôle *a posteriori* devrait permettre, dans un premier temps, de réaliser au mieux les contrôles. Cela étant, les services concernés seraient tous ravis de voir leurs effectifs non pas nécessairement doubler, mais augmenter sérieusement.

M. le président Pierre Morange, rapporteur. Vous devriez faire de la politique, monsieur Loudenot ! *(Sourires.)*

J'en viens aux actes de piraterie informatique. Le ministre de la défense a déclaré que 24 000 attaques informatiques avaient été déjouées en 2016, soit le double de l'année précédente. La presse a relaté de nombreuses affaires, notamment le piratage de 500 millions de comptes d'utilisateurs de l'opérateur Yahoo. Avez-vous des chiffres à nous communiquer en ce qui concerne les attaques informatiques dans le domaine sanitaire et social ? Progressent-elles d'une année sur l'autre ?

M. Philippe Loudenot. Il y a trois ans, le service du haut fonctionnaire de défense et de sécurité a mis en place une boîte d'alerte, ce qui n'était pas obligatoire alors. En 2015, nous avons recensé 1 300 incidents de tout type. Il s'est agi, je le répète, de déclarations volontaires. Nous sommes en train de consolider les chiffres pour 2016.

J’ignore la manière dont le ministère de la défense a fait ses calculs. Pour ma part, j’ai tendance à factoriser certains incidents. Prenons l’exemple de l’« Armageddon informatique » qui avait été annoncé sur internet à la suite de l’attentat contre *Charlie Hebdo*. De nombreux sites internet ont subi des attaques, et il y a deux façons de les comptabiliser : soit l’on compte le nombre de sites attaqués les uns après les autres, soit l’on compte le nombre de serveurs, qui hébergent chacun un certain nombre de sites. Je préfère ce deuxième chiffre, beaucoup plus parlant que le total des incidents qui se produisent.

La grande majorité des alertes pour lesquelles nous avons apporté un appui aux établissements concernaient des incidents qui auraient pu être évités si l’on avait fait preuve d’un minimum de bon sens. Depuis 2014, nous avons affaire essentiellement à des campagnes de cryptovirus. Ceux-ci entrent dans les systèmes par manque d’attention de la part des utilisateurs. Par exemple, un établissement nous a appelés après avoir été infecté par un virus parce qu’un utilisateur avait cliqué sur un lien dans un message en italien, langue qu’il ne comprenait pourtant pas. Il y a toute une acculturation de l’usager à faire, quel que soit son niveau. Il faut le former aux bonnes pratiques ou, pour reprendre les termes de l’ANSSI, aux « mesures d’hygiène » à mettre en œuvre pour la sécurité des systèmes d’information. Travaillant dans le domaine de la santé, j’ajouterai qu’il faut aussi le former à la prophylaxie, c’est-à-dire lui apprendre pourquoi il doit se tenir informé et utiliser les bonnes pratiques.

M. le président Pierre Morange, rapporteur. Avez-vous établi une typologie des incidents ? Par exemple, certains des 1 300 incidents que vous avez évoqués ont-ils été causés par des *ransomwares* – logiciels de rançon ? Ou bien les avez-vous comptés séparément ?

Pour parvenir au chiffre de 1 300 incidents, avez-vous utilisé le premier ou le deuxième des modes de calcul que vous avez évoqués ?

M. Philippe Loudenot. Le deuxième.

M. le président Pierre Morange, rapporteur. À quel chiffre parviendrait-on si on appliquait le premier mode de calcul ?

M. Philippe Loudenot. Je ne suis pas en mesure de vous le dire.

Reprenons l’exemple des attaques qui ont suivi l’attentat contre *Charlie Hebdo*. Dès l’annonce sur internet de cette « tempête informatique », nous avions adressé un message d’alerte à tous nos établissements, médicaux et sociaux. Et nous nous sommes retrouvés avec une situation un peu ambiguë : certains ont annoncé que les établissements relevant du ministère de la santé avaient été attaqués, alors que tel n’était pas le cas ; en réalité, plusieurs responsables, sachant leur site internet un peu fragile, avaient tout simplement décidé de le déconnecter, ce qui a fait augmenter certains chiffres de manière inhabituelle.

Nous avons répertorié trois grands types d’incidents : dans 18 % des cas signalés en 2015, il s’est agi d’attaques malveillantes, visant à commettre un vol, à nuire ou à empêcher les gens de travailler.

Ensuite, il y a ce que j’appelle les « attaques par opportunisme ». Certains établissements de santé disposent de systèmes fortement exposés sur internet, dont la sécurité n’est pas suffisamment prise en compte. Dès lors, la première attaque, virale ou autre, passe sans difficulté.

M. le président Pierre Morange, rapporteur. Quelle est la motivation de ces « attaques par opportunisme » ? Est-ce tout simplement du vandalisme informatique, le goût de nuire, sans espoir de « retour sur investissement » grâce à une exploitation des données détournées au profit de tiers ?

M. Philippe Loudenot. C'est en effet du vandalisme informatique, ou le goût de la lumière. Et pour nous, c'est le fait, malheureusement, de se trouver sur la mauvaise trajectoire au mauvais moment. Il s'agit souvent d'incidents sans gravité auxquels nous remédions très rapidement de manière satisfaisante.

M. le président Pierre Morange, rapporteur. Quel est le pourcentage de ces attaques par opportunisme ou de ce vandalisme ?

M. Philippe Loudenot. Environ 60 %. Le reste des incidents correspond à un mésusage des systèmes d'information. Dans notre domaine, on dit communément que « le premier virus est entre la chaise et le clavier ». D'où la nécessité, je l'ai dit, d'une acculturation de l'usager : il faut le former aux gestes hygiéniques en matière d'utilisation des systèmes d'information. Actuellement, les utilisateurs consultent des sites internet qui ne présentent pas un intérêt professionnel évident, ou cliquent sur tel ou tel lien lorsqu'ils reçoivent un message électronique inhabituel. Il y a un gros travail de sensibilisation à mener auprès de l'ensemble des directions et des équipes, en expliquant les « gestes qui sauvent ».

M. le président Pierre Morange, rapporteur. De ce point de vue, de quels pouvoirs pédagogiques de sanction les employeurs disposent-ils dans les cas de non-respect des procédures, qui suscitent un danger et constituent de ce fait des failles de sécurité ?

M. Arnaud Martin. Le discours que nous tenons sur ce point vise à faire comprendre aux dirigeants d'établissement et à l'ensemble du monde des affaires sociales et de la santé que les systèmes d'information constituent désormais un enjeu de gouvernance. L'effort de pédagogie doit se poursuivre dans ce domaine, car les responsables, confrontés à d'autres difficultés dans un environnement fort complexe, n'ont pas encore tous conscience de cette question et n'en prennent la mesure, hélas, que lorsqu'un incident survient. Il est donc indispensable de continuer à tenir ce discours.

S'il est tenu compte de cet enjeu de gouvernance, les responsables des structures concernées déclineront la politique des ministères chargés des affaires sociales en matière de sécurité des systèmes d'information. Nous avons élaboré en novembre un plan d'action visant à relayer cette politique de sécurité, qui comprend des mesures très simples dont la seule mise en œuvre suffirait à résoudre un certain nombre de problèmes – liés aux mésusages, par exemple.

S'agissant des objets connectés et d'autres questions émergentes dans le domaine de la santé, il nous faut aller vite, même s'il est toujours difficile de progresser au même rythme que les technologies, qui prennent désormais une place indispensable au fonctionnement du secteur de la santé.

Les enjeux sont donc importants. L'expérience montre qu'il faut aussi insister sur leur dimension financière. En octobre, les systèmes d'information de plusieurs établissements de santé anglais ont été bloqués, d'où une perte d'activité pouvant atteindre une semaine, ce qui n'est pas neutre. Il y a donc un enjeu financier important, au-delà des dangers auxquels les patients eux-mêmes peuvent être exposés – que nous ne sous-estimons naturellement pas.

M. le président Pierre Morange, rapporteur. Plusieurs publications ont en effet présenté des modèles d'attaques informatiques qui mettent la santé des patients en danger, ciblant des pompes à perfusion ou des stimulateurs cardiaques par exemple.

M. Gérard Bapt. Seule une minorité de centres hospitaliers universitaires (CHU) dispose à l'heure actuelle d'agents délégués aux questions de sécurité, d'où une importante marge de progrès. Cela étant, ce domaine semble être encore en friche, ce qui doit nous permettre d'avancer en parallèle sur tous les plans. La mise en place des groupements hospitaliers de territoire (GHT) pourrait à mon sens être l'occasion…

M. le président Pierre Morange, rapporteur. Grâce à la mutualisation des ressources, notamment.

M. Gérard Bapt. … de former des agents – sinon à plein temps, du moins dans le cadre de leurs responsabilités – de sorte qu'ils soient capables d'alerter les directions générales au sujet de la sécurité des systèmes d'information.

M. le président Pierre Morange, rapporteur. La pédagogie étant l'art de la répétition, quels moyens faudrait-il déployer pour répandre cette culture de la sécurité et, surtout, à quel niveau ? Faut-il cibler les GHT, ou y ajouter les agences régionales de santé (ARS), qui sont tout de même responsables de l'organisation de l'offre de soins à l'échelle de la région et qui, à ce titre, doivent naturellement, compte tenu des risques, assurer la sécurité des moyens mis à la disposition de la santé de nos concitoyens ? La question n'est pas uniquement d'ordre budgétaire. Au-delà de cet ouvrage de pédagogie qu'il faudra inlassablement remettre sur le métier en réexaminant les moyens à lui affecter, existe-t-il un arsenal réglementaire qui puisse le compléter par un mécanisme plus dissuasif de sanction en cas de faute ou de non-respect – même involontaire – des procédures ?

M. Arnaud Martin. Commençons par décliner la politique générale de sécurité des systèmes d'information au niveau des établissements de santé.

M. le président Pierre Morange, rapporteur. Existe-t-il un plan structuré assorti d'un échéancier, permettant de vérifier que l'ensemble des préconisations sont bien mises en œuvre ? Il s'agit d'un domaine extrêmement évolutif, où le champ des possibles se démultiplie chaque jour. Quelles sont donc les déclinaisons concrètes des préconisations, étant entendu qu'il faut en la matière demeurer humble et modeste ?

M. Arnaud Martin. L'économie générale du dispositif a été précisée et ne pose aucun problème. Nous croyons beaucoup à la mutualisation : si l'Assistance publique-Hôpitaux de Paris (AP-HP) n'a aucun mal à se doter d'un responsable de la sécurité des systèmes d'information (RSSI), la question est en revanche plus compliquée sur d'autres territoires de santé et la possibilité de mutualiser un responsable entre plusieurs établissements est prometteuse.

M. le président Pierre Morange, rapporteur. Est-ce déjà possible au niveau des ARS ?

M. Arnaud Martin. Dans les ARS, la montée en capacité se fera au fil de l'application de l'article 110 précité : à partir du 1er octobre, les incidents relatifs aux systèmes d'information remonteront *via* les ARS, lesquelles se dotent actuellement avec notre appui des moyens qui leur permettront de qualifier la nature des incidents et, s'ils sont graves, de les faire remonter jusqu'au ministère de la santé. Le dispositif, qui s'appuiera sur l'Agence des

systèmes d'information partagés de santé (ASIP Santé), permettra d'analyser les incidents et, s'ils ont des conséquences sanitaires, d'en informer le réseau de santé et d'aider les établissements concernés. En clair, les ARS ne possédaient jusqu'à présent aucune compétence réelle en la matière mais elles vont s'en doter – ce qui présentera les difficultés inhérentes à toute prise de responsabilité dans un domaine échappant à leur cœur de métier. Il va de soi que nous appuierons le renforcement des compétences des ARS qui se produira dans les mois et années à venir en vertu de la loi.

M. le président Pierre Morange, rapporteur. Une telle approche serait sans doute adaptée sur le terrain dans les GHT, dont le dimensionnement territorial varie selon les cas. L'échelon régional, cependant, qui monte en puissance, devrait avoir une vision assez horizontale de ces sujets partagés. Avez-vous estimé les ressources humaines qu'il faudrait déployer pour ce faire ? Faut-il selon vous doter chaque ARS, nonobstant les caractéristiques démographiques de chaque région, d'une équipe de deux ou trois personnes, par exemple ? Un format particulier de structure minimale capable d'assurer ces missions a-t-il été dessiné ?

M. Philippe Loudenot. Non, cette estimation n'a pas été faite. Le secteur de la santé englobe plusieurs cas de figure. La CNAMTS et les différents opérateurs indépendants de la direction de la sécurité sociale (DSS) disposent tous d'équipes de sécurité de très haut niveau, avec lesquelles nous entretenons des relations régulières. Les rares incidents – tous mineurs – qui se sont produits ont tous été traités dans des délais extrêmement rapides. Dans les établissements de santé, en revanche, la mutualisation envisagée me semble très judicieuse. Les ARS vont gagner en maturité et un plan de formation a été proposé à leurs agents afin qu'ils puissent bénéficier des formations dispensées par l'ANSSI en matière de sécurité des systèmes d'information ; ce chantier est ouvert. Les niveaux de maturité varient selon les établissements de santé.

M. le président Pierre Morange, rapporteur. En effet, le caractère très hétérogène du parc informatique hospitalier français est bien connu. L'ancienne idée selon laquelle il fallait homogénéiser ce parc a vécu ; en l'absence de vision planificatrice des équipements, elle a été supplantée par la notion d'interopérabilité des systèmes. De surcroît, les niveaux de sécurité varient, certains étant des plus rustiques – et constituant autant de portes d'entrée pour une attaque. Compte tenu de l'efficience et de la solidité des équipes de la CNAMTS – sans entrer pour autant dans le vieux débat de la répartition des compétences entre la CNAMTS et les ARS, qui a suscité sinon de la concurrence, en tout cas une certaine compétition et des chevauchements – et du caractère stratégique de cette question pour la santé, voire la sécurité budgétaire de la nation, avez-vous entrepris un travail de coordination ou de coopération permettant le partage d'expériences ? En effet, les ARS ne maîtrisent pas encore ce sujet avec autant de finesse que la CNAMTS.

M. Philippe Loudenot. Cela fait partie de l'action conduite depuis trois ans, sachant que le service du haut fonctionnaire de sécurité informatique a l'avantage de compter dans son périmètre de compétences quatre secteurs ministériels : la santé, le travail et le sport, ainsi que les droits des femmes. Il m'est ainsi arrivé de présenter des sujets de santé aux équipes de sécurité de Pôle Emploi, en bénéficiant d'une vision non pas fermée mais, au contraire, complètement ouverte dans un domaine qu'*a priori*, elles ne connaissaient pas. En matière de sécurité des systèmes d'information, les métiers finaux sont certes différents mais les objectifs initiaux, eux, sont identiques : il s'agit de protéger la disponibilité, l'intégrité et la confidentialité de nos systèmes et des informations qu'ils contiennent. Il nous faut faire comprendre aux acteurs de la santé que la difficulté n'est pas seulement d'ordre technique : la

technique est un outil qu'il ne faut employer qu'après une analyse de risque. La question à poser est la suivante : que veut-on protéger et à quel niveau ?

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…

M. le président Pierre Morange, rapporteur. Il a la faveur de la CNIL.

M. Philippe Loudenot. En effet ; 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.

M. le président Pierre Morange, rapporteur. La gestion technique du SNDS est confiée à la CNAMTS, qui est tout à la fois productrice et hébergeur de données, même si certains estiment qu'il serait plus judicieux de séparer les deux fonctions. Concernant la fonction de stockage, un modèle similaire à celui du CASD aurait pu être envisagé, ne serait-ce que pour faciliter les échanges et les procédures. Ce n'est semble-t-il pas le cas, puisque les analyses sont différentes. Quel est votre sentiment à ce sujet – sans faire aucun procès d'intention ?

M. Philippe Loudenot. Le Secrétariat général pour la modernisation de l'action publique (SGMAP) accompagne également le projet du SNDS et travaille à ce titre sur différentes solutions. Il s'en présente au moins six. Il faudra envisager un modèle économique pour chacune d'entre elles, puisque c'est le nerf de la guerre.

M. le président Pierre Morange, rapporteur. Il va de soi que cette réflexion est nécessaire et qu'elle doit s'appuyer sur des références au niveau européen. La réglementation européenne étant plus stricte que la réglementation française, quel est votre sentiment, général Martin, sur l'action à conduire pour atteindre ces objectifs en matière de sécurité, de confidentialité et de procédures ?

M. Arnaud Martin. Je me garderai de formuler un avis sur le volet technique, sur lequel je ne suis pas compétent, mais je dirai ceci : il est essentiel que l'analyse des risques permette à l'ensemble des acteurs de déterminer quels types de solutions répondent au niveau de risque à traiter, ensuite ces options seront mises en concurrence. Les choses avancent vite, en effet : l'ANSSI met au point ses solutions, de même que la DREES.

M. le président Pierre Morange, rapporteur. Quels sont les avantages et inconvénients respectifs des six solutions évoquées ?

M. Philippe 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. 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 ?

M. le président Pierre Morange, rapporteur. Quand les conclusions de l'analyse de risque seront-elles rendues ?

M. Philippe Loudenot. Elles l'ont été et ont permis d'établir le référentiel de sécurité qui a été présenté à la CNIL, qui l'a approuvé en y apportant quelques compléments en matière de contrôle – une fonction essentielle à la sécurisation de tout système d'information. La protection des données ne se décrète pas ; elle doit se démontrer.

M. le président Pierre Morange, rapporteur. Y a-t-il un modèle – économique ou de sécurité – européen qui vous semble plus pertinent que les autres ?

M. Philippe Loudenot. En matière de sécurité des systèmes d'information, les approches varient. Pendant des années, nous avons préconisé le modèle de l'analyse de risque visant à aboutir systématiquement à un choix technique figé. D'autres approches plus « souples » consistent à effectuer une analyse de risque tout en s'interrogeant sur l'objet et la méthode de la protection. La cybersécurité et la sécurité des systèmes d'information présentent la difficulté d'être toujours considérées comme des sources de coûts par les dirigeants et comme des sources de blocage par les professionnels ; elles ne sont jamais présentées comme un facteur de création de valeur. Autrefois, il fallait démontrer la qualité en l'opposant à la non-qualité ; aujourd'hui, le maintien en condition opérationnelle d'un système ne suffit pas à le sécuriser. Permettez-moi cette analogie : pour les passionnés de voitures, la 2CV est un très beau véhicule ; sur le plan opérationnel, elle roule, mais en termes de sécurité elle est une catastrophe. Aujourd'hui, elle ne passerait plus aucun test technique et serait interdite à la vente. La mise en place d'un système de sécurité et l'application d'abaques ne supprime pas la nécessité de procéder à des vérifications régulières. La Cour des comptes, se prononçant sur la fonction d'occultation des informations nominatives – l'algorithme FOIN –, avait ainsi relevé la fragilité de l'une des briques du système ; la CNAMTS, qui en était consciente, l'a fait évoluer. Cette évolution, cependant, a un coût qu'il faut anticiper dès l'origine. Il est toujours plus difficile de récupérer ce coût et, de ce fait, de devoir conduire de nouvelles études pour envisager l'avenir.

M. le président Pierre Morange, rapporteur. Le remplacement de cette fameuse « brique » coûterait environ, nous a-t-on dit, 20 millions d'euros : est-ce le cas ?

M. Philippe Loudenot. Je ne dispose pas des éléments financiers permettant de le confirmer. Cela étant, il y a deux manières d'établir ce coût : soit il correspond à un bouleversement d'ensemble du système, à la manière d'un *big bang* concernant tous les établissements censés utiliser ces moyens de chiffrement, soit il s'agira d'une évolution au fil de l'eau – même si tous les établissements devront *in fine* basculer. Plutôt que de se lancer tête baissée dans des études pour remplacer cette brique à tout prix, préférer une méthode progressive de projet serait beaucoup moins douloureux en termes financiers et techniques.

M. Arnaud Martin. Il faut reconnaître que, dans le secteur de la santé comme dans d'autres secteurs, le maintien de conditions de sécurité a souvent été délaissé. Or, l'approche globale de la mise en conformité en matière de sécurité n'a pas toujours été prise en compte – permettez-moi cet euphémisme – alors que les technologies évoluent très vite et que les systèmes de sécurité doivent répondre à des demandes croissantes. Ce retard nous rattrape. Il y a là un enjeu de gouvernance. Les responsables des projets informatiques doivent inciter les décideurs à chiffrer le volet sécurité, non seulement au départ – analyse de risque et audit initial – mais aussi sur la durée, et à ne pas minorer cet enjeu. Les économies réalisées à l'instant « t » finissent par se payer si une attaque survient quelques années plus tard, comme on l'a constaté dans plusieurs secteurs. Hélas, les perspectives de court terme auxquelles nous nous heurtons nous empêchent de nous projeter en raison des coûts initiaux d'une action plus durable. J'appelle l'attention des décideurs sur ce point : il faut prendre en compte ce volet de sécurité dès la mise en œuvre d'un projet.

M. le président Pierre Morange, rapporteur. Existe-t-il des estimations financières en la matière ?

M. Arnaud Martin. Nous pourrons nous rapprocher des structures concernées pour affiner l'estimation de ce volet.

M. le président Pierre Morange, rapporteur. Il nous serait utile d'avoir cette estimation, non pas pour instruire un quelconque procès d'intention mais pour éclairer la représentation nationale, de sorte qu'elle puisse insister auprès du pouvoir exécutif – qui en est nul doute convaincu – sur l'importance de ce suivi et de la ligne budgétaire qui doit y être affectée, sachant que celle-ci ne doit pas être centralisée mais qu'elle doit plutôt irriguer l'ensemble des systèmes spécialisés qui structurent le secteur de la santé dans le pays.

Dans le domaine, si vaste et évolutif, des systèmes de sécurité et du modèle économique qui permettrait d'en assurer la pérennité, auriez-vous, compte tenu de notre législation actuelle, de la réglementation européenne et de la diversité des risques que vous êtes les premiers à combattre, des préconisations à soumettre à la MECSS, qui nécessiteraient par exemple de prendre des mesures législatives ou de donner une orientation particulière aux décrets d'application ?

M. Philippe Loudenot. Je forme le vœu que les directions chargées de faire face aux risques juridiques n'occultent pas les questions de cybersécurité et de sécurité des systèmes d'information. L'anticipation au démarrage des projets coûte beaucoup moins cher que les rectifications apportées *a posteriori*, en catastrophe et sans réflexion. Les textes réglementaires existent, qu'il s'agisse des textes de la CNIL, du règlement européen sur la protection des données personnelles ou encore de la politique de l'État en matière de sécurité des systèmes d'information, qui impose d'homologuer ces systèmes et qui a été déclinée dans les politiques de sécurité des systèmes de chaque ministère chargé des affaires sociales, publiées par arrêté. Différents textes imposent donc aux dirigeants de veiller à la prise en compte *ex ante* de la sécurité informatique.

La difficulté principale tient aux projets réalisés rapidement pour satisfaire un supérieur hiérarchique, alors qu'il faudrait procéder à une gestion de projets réfléchie en tenant compte des questions de sécurité, pour ce qui concerne l'analyse de risque mais aussi le cycle de vie tout entier du projet, depuis son lancement jusqu'à son extinction. Pour autant, les textes en vigueur suffisent puisque la plupart exigent de tenir compte du volet sécurité. Il existe cependant un fossé profond entre les textes existants et leur appropriation par les

professionnels sur le terrain, d'où le travail de sensibilisation – voire d'évangélisation – du service du haut fonctionnaire de sécurité informatique auprès des dirigeants, qui consiste notamment à faire de régulières piqûres de rappel, car les questions de sécurité sont de ces sujets que l'on a tendance à oublier. Il est vrai que la plupart de ces dirigeants sont rompus à la gestion des risques financiers, sanitaires ou concernant les ressources humaines, mais la cybersécurité et la sécurité des systèmes d'information sont aussi une nouveauté pour eux. C'est sans relâche qu'il faut faire passer ce message.

M. le président Pierre Morange, rapporteur. Il faut donc que l'ensemble des acteurs du secteur sanitaire et social, jusqu'au niveau le plus fin, s'approprient ces questions.

M. Arnaud Martin. En clair, aucun système d'information ne devrait être mis en production sans homologation et sans prise en compte de l'analyse de risque. De ce point de vue, la Haute Autorité de santé (HAS) conduit des audits dans différentes structures ; sur ces sujets, un travail collectif est à faire – comme c'est de plus en plus le cas. Il faut s'assurer que ce travail a été accompli avant d'habiliter une structure. Je crois aux aiguillons de ce type beaucoup plus qu'aux sanctions. Les moyens informatiques et les contrôles *a posteriori* permettent désormais de faire remonter les signaux faibles avec plus d'efficacité. Un travail de pédagogie est nécessaire en la matière. Le secteur est si vaste qu'il est difficile, en effet, de faire progresser toutes les structures ensemble.

M. le président Pierre Morange, rapporteur. Je vous remercie. Sans doute la MECSS vous interrogera-t-elle de nouveau en fin d'année avant de finaliser son rapport.

La séance est levée à onze heures quarante.