LE BESOIN GRANDISSANT DE SÉCURISATION DES DONNÉES MÉDICALES DES ÉTABLISSEMENTS DE SANTÉ ET LE CADRE DE DÉVELOPPEMENT DES RÉPONSES APPORTÉES

Sonia Cordon

L'Institut Droit et Santé, de l'université de Paris | « Journal du Droit de la Santé et de l'Assurance - Maladie (JDSAM) »

2021/2 N° 29 | pages 63 à 66

ISSN 2269-9635
DOI 10.3917/jdsam.212.0063

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-journal-du-droit-de-la-sante-et-de-l-assurance-maladie-2021-2-page-63.htm

Les cyberattaques dans les établissements de santé : enjeux et protection

Actes du colloque en ligne en date du 17 mai 2021

Sonia Cordon
Stagiaire juriste à l'Institut Droit et Santé, Inserm UMR_S 1145, Faculté de droit, d'économie et de gestion, Université de Paris

Le besoin grandissant de sécurisation des données médicales des établissements de santé et le cadre de développement des réponses apportées

L'Association pour la sécurité des systèmes d'information de santé (APSSIS) a énoncé que « *Le coronavirus semble avoir largement inspiré les cybercriminels puisque le baromètre Signal Spam indique que le phishing aurait augmenté de 600 % sur le mois de mars* »[1].

Les établissements de santé ont été des cibles privilégiées des cyberattaques lors de la lutte contre l'épidémie de la Covid-19. Le Président de la Fédération Hospitalière de France, Frédéric Valletoux, explique parfaitement les raisons de cette situation en expliquant qu' « *On doit estimer que ce sont des proies faciles, qu'ils ont la tête ailleurs, qu'ils sont mobilisés par l'épidémie, la prise en charge des patients, par une activité débordante et que peut-être l'attention diminue quant aux précautions à avoir en matière de sécurité informatique* ». En effet, la situation de crise sanitaire a pu accentuer des faiblesses, déjà existantes qui peuvent être exploitées par les cybercriminels. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a, de son côté, mis en avant quelques faiblesses, notamment le manque de sensibilisation aux risques cyber, l'absence de maîtrise des systèmes d'information, l'augmentation de la surface d'attaque due au télétravail, le manque d'experts en cyber sécurité et le non-respect des mesures d'hygiène informatique[2].

De nombreux outils ont été mis en place dont la visée première est la sécurisation des données médicales **(I)**. Malgré ces derniers, une réponse nationale mettant le risque cyber en première ligne devient aujourd'hui nécessaire **(II)**.

I- Les moyens juridiques de sécurisation des données médicales

En première ligne, on retrouve le Règlement général sur la protection des données (RGPD)[3] qui remplace et abroge la Directive de 1995[4] sur la protection des données à caractère personnel. Le RGPD a pour objectif d'encadrer le traitement des données personnelles sur le territoire de l'Union européenne (UE). En raison des usages accrus du numérique et du développement du commerce en ligne, il y a aujourd'hui un besoin d'adaptation du contexte juridique pour suivre les évolutions technologiques de nos sociétés. À cet égard, le RGPD s'inscrit dans la continuité de la Loi française Informatique et Libertés datant de 1978[5] et vient renforcer le contrôle de l'utilisation qui peut être faite des données concernant les citoyens.

Ce nouveau Règlement vient harmoniser les règles en Europe avec un cadre juridique unique pour les professionnels ce qui leur permet un développement plus aisé de leurs activités numériques au sein de l'UE. Le Règlement peut concerner tout organisme, peu important sa taille, son pays d'implantation ou même son activité. En effet, dès lors qu'une organisation, tant publique que privée, traite de données personnelles et est soit établie sur le territoire de l'UE soit que son activité cible directement les résidents européens, le RGPD s'applique.

Au sein de ce RGPD, l'article 32 a plus spécifiquement trait à la sécurité du traitement et renforce l'obligation de sécurité à la charge du responsable du traitement. Les motivations de cet article proviennent de trois considérants différents. Tout d'abord, le considérant 39 du RGPD qui énonce que le traitement des données à caractère personnel devrait garantir une sécurité et une confidentialité appropriée. Ensuite, le considérant 49 explique la notion de « sécurité du réseau et des informations » en droit européen. Il présente cela comme « *La capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou*

1 - Apssis, Panorama des arnaques et attaques, juin 2020, https://www.apssis.com/actualite-ssi/429/covid-19-et-les-quarante-voleurs.html.

2 - Rapport franco-allemand « *Common Situational Picture* », 3ème édition, 2020.

3 - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

4 - Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995.

5 - Loi nº 78-17 du 6 janvier 1978.

malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données à caractère personnel conservées ou transmises (...) ». Enfin, le dernier considérant est le 83 qui demande une approche de la sécurité par les risques de la part du responsable de traitement ou du sous-traitant.

Le RGPD ne fait pas seulement de la prévention car il permet à la Commission nationale de l'informatique et des libertés (CNIL) de prononcer des sanctions administratives à l'encontre des responsables de traitements qui manquent à leur obligation de sécurité. À cet égard, il faut préciser que les établissements de santé ne sont pas protégés contre ces amendes et y sont donc confrontés comme tout autre organisme. En effet, la première amende prononcée après le RGPD dans l'UE a concerné un centre hospitalier portugais pour manquement aux principes d'intégrité, de confidentialité et de minimisation des données[6]. Le centre hospitalier a été condamné par l'homologue portugais de la CNIL, le CNPD (Comissão Nacional de Proteção de Dados) à hauteur de 400 000 euros. Évidemment, l'obligation de sécurité des responsables de traitement ne constitue pas une obligation de résultat, néanmoins elle est aujourd'hui une obligation de moyens renforcés. En ce sens, une telle obligation nécessite l'adoption de mesures de sécurité conformes à l'état de l'art et adaptées au niveau de sensibilité des données collectées, très haut en matière de données de santé.

Les obligations de sécurité sont, par ailleurs, spécifiquement renforcées pour les prestataires de soins de santé[7] car, étant considérés comme des opérateurs de service essentiels (OSE), ils sont soumis à la Directive NIS[8]. Sont concernés par ce renforcement, les prestataires de soins de santé, définis comme « *Toute personne physique ou morale ou toute autre entité qui dispense légalement des soins de santé sur le territoire d'un État membre* »[9].

À côté de ce Règlement, le Code de la santé publique, en son article L.1111-8, énonce que toute entreprise qui héberge des données personnelles de santé pour le compte d'un tiers est soumise à l'obligation d'une Certification HDS (hébergeurs de données de santé). Cette procédure repose sur une évaluation de conformité au référentiel de certification[10]. Un organisme certificateur, choisi par l'hébergeur et accrédité par le COFRAC (Comité français d'accréditation), ou un équivalent européen, va procéder à un audit en deux étapes afin d'évaluer la conformité de l'hébergeur au référentiel de certification. Contrairement à l'ancienne procédure d'agrément, la démarche de certification applicable depuis le 1er janvier 2019 se fait désormais aux frais de l'organisme demandeur. Pendant trois mois après la fin des étapes de l'audit, l'hébergeur peut corriger les manquements aux exigences du référentiel et faire auditer ses modifications. Si ce délai est dépassé, la procédure d'audit devra être entièrement réalisée à nouveau. Dans le cas où le certificat est délivré, la certification dure trois ans avec un renouvellement tous les ans par l'organisme certificateur après un audit de surveillance.

En dehors de ces outils règlementaires, différents organismes ou même entités ont édicté des guides et des recommandations de bonnes pratiques ayant vocation à une meilleure sécurisation des données. C'est notamment le cas de l'ANSSI ainsi que la CNIL[11]. En effet, l'ANSSI propose, en partenariat avec la Confédération des petites et moyennes entreprises, un guide de bonnes pratiques de l'informatique[12] qui contient douze règles essentielles pour sécuriser les équipements numériques. On peut citer notamment la mise à jour régulière des logiciels, le choix avec soin de ses mots de passe, la sécurisation de l'accès WI-FI de l'entreprise etc...

La CNIL, a quant à elle récemment fait un rappel des précautions à mettre en œuvre pour être en conformité avec les règlementations. Il faut d'ailleurs savoir que la CNIL a annoncé faire de la cybersécurité sur les données de santé l'une de ses thématiques prioritaires de son contrôle en 2021[13].

En outre, des entreprises se sont également penchées sur cette question de la sécurité des données de santé, telle la Société hospitalière d'assurance mutuelle (SHAM) qui propose un livre blanc centré spécifiquement sur la cybersécurité au sein des établissements de santé[14]. Le but de la création de ce libre blanc est d'expliquer les principes fondamentaux ainsi que les enjeux de la cybersécurité. En effet, la SHAM vient ici décrypter le risque Cyber pour permettre aux professionnels au sein d'établissements de santé de savoir gérer un tel risque de par l'analyse des risques, l'étude des solutions de prévention ainsi que la question de la gestion et l'assurance du risque résiduel.

Ces différents outils et recommandations révèlent une prise de conscience collective de l'enjeu de la sécurisation des données. Néanmoins, de tels outils ne sont aujourd'hui plus suffisants face à la montée du risque cyber, l'action de l'État est nécessaire.

6 - JusJornal, N.º 33, Secção Proteção de dados / Temas de hoje , Dezembro 2018, Editora Wolters Kluwer.

7 - Article 3, g) de la Directive 2011/24/UE du Parlement Européen et du Conseil du 9 mars 2011.

8 - Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

9 - Article 3, g) de la Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011.

10 - https://esante.gouv.fr/sites/default/files/media_entity/documents/20200610-ANS-ReferentielCertificationHDS-v1.6.pdf.

11 - https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf.

12 - https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf.

13 - Site de la CNIL, « *Cybersécurité, données de santé, cookies : les thématiques prioritaires de contrôle en 2021* ».

14 - Livre Blanc «Cybersécurité, nouveau défi des établissements de la santé et médico-sociaux».

II- L'action de l'État, complémentaire des dispositifs préexistants de sécurisation des données médicales

Face à la hausse des cyberattaques en France, et notamment des attaques par *ransomware*[15] qui ont quadruplées en 2020 en passant de 54 à 192 attaques (dont 11 % visaient des hôpitaux), l'État s'est retrouvé dans l'obligation d'agir[16]. À cet effet, le Président de la République a notamment annoncé un plan de lutte contre la cybercriminalité à hauteur d'un milliard d'euros **(A)**. Néanmoins, l'action de l'État sur le plan national, bien qu'elle permette une globalisation des mesures prises, n'est pas la seule à jouer un rôle **(B)**.

A. La prise de mesures à dimension nationale

Le 18 février 2021, le Président de la République Emmanuel Macron a annoncé un plan de lutte contre la cybercriminalité d'un milliard d'euros appliqué d'ici 2025[17]. Ce plan s'articule autour de cinq axes : 1. Le développement de solutions nationales de cybersécurité et l'augmentation du chiffre d'affaires de ce secteur ; 2. Le renforcement des liens et synergies entre les acteurs de la cybersécurité ; 3. La mise en place des actions de sensibilisation pour promouvoir les solutions nationales ; 4. Le soutien en fonds propres dédié aux startups ; 5. Le renforcement d'un volet formation dans le but de doubler les emplois de la filière afin de passer de 37 000 à 75 000 postes[18].

Le plan vise à déployer des solutions nouvelles et innovantes de sécurité par la mise en place de projets de recherche et de développement en collaboration entre le public et le privé (515 millions d'euros seront déployés à cet effet). En outre, courant 2021, verra également le jour un campus cybersécurité de 20 000 m² à la Défense dont le coût s'élève à 148 millions d'euros[19]. L'intérêt de ce dernier est de favoriser les collaborations entre les acteurs dans le domaine puisqu'il va réunir plus d'un millier d'experts[20].

En ce qui concerne le secteur santé et médicosocial en lui-même, c'est le 22 février que le Ministre de la Santé, Olivier Véran, et le secrétaire d'État chargé de la Transition numérique et des Communications, Cédric O, se sont chargés de détailler le plan présenté. Ces derniers ont énoncé qu'il était prévu de déployer 350 millions d'euros pour renforcer la cybersécurité des établissements sanitaires et médico-sociaux. De plus, sur une enveloppe de 136 millions d'euros attribuée à l'ANSSI pour renforcer la cybersécurité de l'État, 25 millions seront spécifiquement dédiés aux établissements de santé. Une réserve est cependant posée, les établissements allocataires de ressources devront consacrer entre 5 et 10 % de leur budget à la cybersécurité pour bénéficier d'un soutien de la part de l'État[21]. Grâce à un tel financement, il sera possible de déployer le service national de cybersurveillance en santé qui se réalisera avec le concours de l'Agence du Numérique en santé. Le déploiement d'un tel service entre dans le cadre de la feuille de route 2019-2022 en santé « accélérer le virage numérique » dont l'enjeu est l'intensification de la sécurité et de l'interopérabilité du numérique en santé.

Afin de continuer vers un renforcement des exigences de sécurité informatique, il a été annoncé à la fin du mois de février, par le Ministre des Solidarités et la Santé et le secrétaire d'État chargé de la Transition numérique et des Communications électroniques, que 135 Groupements Hospitaliers de Territoire seront, fin mai 2021, intégrés à la liste des opérateurs de service essentiels. L'intérêt étant d'apporter des règles de sécurité informatiques plus strictes mais également de les contraindre à appliquer les meilleures pratiques de cybersécurité aux systèmes d'information actuels. Le contrôle du bon respect des règles sera du ressort de l'ANSSI mais ce sont les Agences régionales de santé (ARS) qui devront accompagner les établissements pour se conformer à ces mesures[22].

Dans un communiqué du 30 mars 2021, le secrétaire d'État chargé de la Transition numérique et des Communications électronique a également lancé un appel à manifestation d'intérêts. Son objectif est de retenir trois projets qui visent des solutions innovantes pour répondre aux besoins de cybersécurité dans les collectivités territoriales, les établissements de santé et les infrastructures portuaires. Cependant, de telles actions ont déjà été menées dans les territoires.

B. Les solutions innovantes à dimension locale

À côté des projets nationaux, des projets locaux s'inscrivent dans la lutte contre la cybercriminalité au sein des établissements de santé à travers la mise en place de solutions innovantes.

Tel est notamment le cas dans la région des Pays de la Loire qui amorce des pistes d'actions collectives face aux enjeux actuels de la sécurité numérique. En effet, après l'organisation d'un temps d'échange le 12 mars 2021 en collaboration avec les structures sanitaires et médico-sociales de la région, ont été dévoilés des objectifs et des mesures que la région souhaite mettre en place pour préparer chaque établissement aux cyberattaques. Comme l'exprime le Directeur général de l'ARS Pays de la Loire, Jean-Jacques Coiplet « *Cette menace nous concerne tous, quels que soient la taille, le rôle, le positionnement des établissements dont*

15 - Attaques par rançongiciel.

16 - Agence nationale de la sécurité des systèmes d'information, « *État de la menace rançongicel à l'encontre des entreprises et institutions* », 4 mars 2021.

17 - Visio-conférence en direct de l'Élysée avec la direction de l'hôpital de Villefranche-Sur-Saône.

18 - Lionel Costes, Lamyline, Droit de l'immatériel, n°179 « *Cybersécurité : présentation par Emmanuel Macron d'un plan d'un milliard d'euro* ».

19 - Cécile Rabeux, Hospimedia, 17 février 2021, « *Le Gouvernement consacre 1 Md€ supplémentaires à sa stratégie contre la cybercriminalité* ».

20 - Géraldine Tribault, Hospimedia, 18 février 2021, « *Emmanuel Macron souhaite que la cybersécurité passe à un niveau supérieur* ».

21 - Revue hospitalière de France, n°599, mars-avril 2021, « *La cybersécurité allie technologie et facteurs humains* ».

22 - Communiqué de presse de Olivier Véran, 22 février 2021.

nous avons la responsabilité ». Pour contrer cette menace, il entend veiller à l'intégration de manière systématique des enjeux de cybersécurité dans les cahiers des charges – que ce soit à vocation régionale, départementale ou même infra-territoriale. En effet, il est nécessaire que la cybersécurité devienne, au même titre que la qualité des soins ou même la prévention des risques, un enjeu de politique d'établissement. Selon le directeur, l'enjeu doit être inscrit dans l'agenda des instances dirigeantes un minimum de deux fois par an pour obtenir un arbitrage éclairé des risques.

Au-delà de cela, deux initiatives innovantes ont pu être mises en avant. Tout d'abord, la création d'un réseau de responsables sécurité des systèmes d'information volontaires dans le but de favoriser l'entraide lors d'une crise au sein d'un établissement de la région. Si l'établissement se voit exposé à un risque de cyberattaque, alors le réseau sera à disposition des équipes de direction de l'établissement en question. Puis, une autre initiative porte sur le fonctionnement courant des établissements par l'émergence d'un « pool régional de compétences sécurité des systèmes d'information mutualisées »[23]. L'intérêt de ce dernier sera avant tout d'accompagner les projets de modernisation dans le cadre du Ségur de la santé mais également d'appuyer les structures en compétences.

L'ARS souligne l'importance à accompagner les établissements en difficulté, notamment à travers le partage de bonnes pratiques, le déploiement de formations, de webinaires, par le groupement de coopération sanitaire e-santé Pays de la Loire. La stratégie « collective » de la région Pays de la Loire permet d'inclure divers acteurs notamment les partenaires locaux dont le délégué régional de l'ANSSI, le référent cybersécurité du conseil régional, la gendarmerie, ainsi que les conseils départementaux. L'ARS Pays de la Loire sera la première à adhérer à l'APSSIS située en Sarthe.

Un autre projet a vu le jour dont le but est de protéger les systèmes de santé des menaces, notamment cyber : le programme européen SAFECARE[24]. Ce programme est développé avec l'Assistance publique des hôpitaux de Marseille (l'AP-HM) avec la collaboration de vingt et un partenaires publics ou privés issus de dix États membres de l'UE. L'enjeu d'un tel projet est d'augmenter et d'accélérer l'entraide aux échelons régional, national et européen. En effet, la qualité des systèmes d'information d'un établissement de santé est conditionnée à la capacité à communiquer rapidement des informations fiables. Pour répondre aux cinq objectifs qu'il s'est fixé, à savoir la surveillance et le signalement des événements indésirables de sécurité, la détection des signaux faibles, l'aide à la décision des opérateurs, le conseil des décideurs dans la gestion de crise et l'accompagnement de la gestion de crise, le projet matérialise un partage nécessaire de la sécurité opérationnelle cyber avec divers acteurs tels que la police, les instituts scientifiques etc.

Le maître mot du programme SAFECARE est la maîtrise des risques en temps réel, obtenue grâce à un entraînement et une entraide. Ce projet sera le premier système global de supervision en matière de sécurité des systèmes d'information en santé qui permettra une visualisation de l'état des risques et leur propagation à court terme. Enfin, il permet la mobilisation des ressources appropriées, que ce soit dans le cadre d'un entraînement de simulation ou en réponse à un vrai problème. Le projet est européen et financé par la Commission européenne mais sera piloté localement, à Marseille, à l'AP-HM.

Si l'on peut se féliciter de ces diverses initiatives, nationales ou locales, on peut néanmoins s'inquiéter d'une telle hausse de la cybercriminalité dans le domaine de la santé en raison d'une baisse de moralité des hackeurs qui semblent s'affranchir de toute limite quant au choix de leur cible pour parvenir à leurs fins. Au risque de perdre trop gros, les établissements de santé ont désormais un devoir de s'investir pleinement dans le domaine de la sécurisation de leurs systèmes d'information, dans la formation du personnel au risque cyber et dans l'anticipation des cyberattaques qui peuvent toucher tous les établissements, quelle que soit leur taille.

Sonia Cordon

23 - Perrine Debacker, Hospimedia, 14 avril 2021, « *L'ARS Pays de la Loire veut jouer collectif contre les cyberattaques d'établissements* ».

24 - Philippe Tourron, Revue Hospitalière de France, n°599, mars-avril 2021, « *Cyberguerre, Une innovation pour nous protéger : SAFECARE* ».