Université de Lille

Faculté des sciences juridiques, politiques et sociales
Université de Lille

# Sujet : La sécurité numérique des établissements publics de santé : enjeux et perspectives de la protection des données personnelles

Mémoire présenté et soutenu par AUBINIÈRE Marie, étudiante en Master 2 Droit et Politiques de Santé

Sous la direction de Madame Johanne SAISON, Maître de conférences

*Année universitaire 2020-2021*

# REMERCIEMENTS

Je tiens à exprimer toute ma reconnaissance à ma directrice de mémoire, Madame Johanne SAISON pour avoir accepté de m'encadrer. Je la remercie de m'avoir orienté, encouragé et d'avoir suscité en moi un profond intérêt pour le droit hospitalier.

Je souhaite également remercier mon tuteur de stage au sein de la Direction des Ressources Matérielles du Centre Hospitalier Vallée de la Maurienne, Monsieur Philippe GIOVANANGELI. Je le remercie de m'avoir accompagné et conseillé tout au long de mon stage.

Par la même occasion, je remercie le DSIO du Centre Hospitalier Vallée de la Maurienne, Monsieur Alain JOYEUX. Je le remercie pour son retour d'expérience, ses conseils et le temps consacré à nos entretiens.

Au sein du GHT Savoie-Belley, je tiens à remercier le Responsable Sécurité des Systèmes d'Information, Monsieur André PILLON et le Délégué à la Protection des Données, Monsieur Thomas LADANT. Je les remercie pour leur disponibilité et leur retour d'expérience concernant la cyberattaque survenue à l'encontre du Centre Hospitalier d'Albertville-Moûtiers le lundi 21 décembre 2020.

Je tiens également à remercier le Responsable des Systèmes d'Information Santé à l'ARS Hauts-de-France, Monsieur Ronan ROUQUET. Je le remercie pour nos échanges sur la gestion de crise face à une cyberattaque, au niveau régional.

J'adresse mes remerciements particuliers au chef de projet en charge de la confidentialité des données médicales au sein du Centre Hospitalier Universitaire de Lille, Monsieur Jean-François DESCACQ. Je le remercie pour ses précieux conseils et son partage d'expériences sur la protection des données personnelles.

Enfin, je remercie mes parents, mon petit frère ainsi que mes ami(e)s pour leur soutien indéfectible.

# LISTE DES ABRÉVIATIONS

- ACSEL : Association pour le Commerce et les Services En Ligne
- ACSS : Accompagnement Cybersécurité des Structures de Santé
- AAI : Autorité Administrative Indépendante
- AFDS : Association Française des Directeurs des Soins
- AFDSD : Association Française de Droit de la Sécurité et de la Défense
- ANS : Agence du Numérique en Santé
- ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
- APMnews : Agence de Presse Médicale news
- APSSIS : Association Pour la Sécurité des Systèmes d'Information en Santé
- AQSSI : Autorité Qualifiée pour la Sécurité des Systèmes d'Information
- ARS : Agence Régionale de Santé
- ASIP Santé : Agence des Systèmes d'Information Partagées de santé
- ATIH : Agence Technique de l'Information sur l'Hospitalisation
- CALID : Centre d'Analyse en Lutte Informatique Défensive
- CEDH : Convention Européenne des Droits de l'Homme
- CH : Centre Hospitalier
- CHR : Centre Hospitalier Régional
- CJUE : Cour de Justice de l'Union Européenne
- CNIL : Commission Nationale de l'Informatique et des Libertés
- CORSSIS : COmité Régional Stratégique des Systèmes d'Information de Santé
- CP : Code Pénal
- CSP : Code de la Santé Publique
- DACG : Direction des Affaires Criminelles et des Grâces
- DGA-MI : Direction Générale de l'Armement - Maîtrise de l'Information
- DGOS : Direction Générale de l'Offre de Soins
- DGSI : Direction Générale de la Sécurité Intérieure
- DNS : Délégation ministérielle au Numérique en Santé
- DPII : Dossier Patient Informatisé et Interopérable
- DPO : *Data Protection Officer* (Délégué à la Protection des Données)
- DSIO : Directeur des Systèmes d'Information et de l'Organisation
- DSSIS : Délégation à la Stratégie des Systèmes d'Information de Santé

- EMA : *European Medicines Agency* (Agence Européenne des Médicaments, AEM)
- EPS : Etablissement Public de Santé
- EUROPOL : *European Police Office* (Office Européen de la Police)
- FSSI : Fonctionnaire chargé de la Sécurité des Systèmes d'Information
- GIP : Groupement d'Intérêt Public
- GIP ACYMA : Groupement d'Intérêt Public Action contre la CYberMAlveillance
- GHT : Groupement Hospitalier de Territoire
- HADS : Hébergeur Agréé de Données de Santé
- HFDS : Haut Fonctionnaire de Défense et de Sécurité
- INRIA : Institut National de Recherche en Informatique et en Automatique
- JORF : Journal Officiel de la République Française
- LEJEP : Laboratoire d'Etudes Juridiques et Politiques
- NTIC : Nouvelles Technologies de l'Information et de la Communication
- OCLCTIC : Office Central de Lutte contre la Criminalité lié aux Technologies de l'Information et de la Communication
- OMS : Organisation Mondiale de la Santé
- OSE : Opérateurs de Services Essentiels
- PGSSI-S : Politique Générale de Sécurité des Systèmes d'Information de Santé
- RELIMS : Répertoire des Editeurs de Logiciels et des Intégrateurs du Monde de la Santé
- RGPD : Règlement Général sur la Protection des Données
- RSSI : Responsable de la Sécurité des Systèmes d'Information
- SGDSN : Secrétariat Général de la Défense et de la Sécurité Nationale
- SI : Système d'Information
- SI-DEP : Système d'Information de Dépistage Populationnel
- SIH : Système d'Information Hospitalier
- TICsanté : Technologies d'Information et de Communication dans la santé
- UE : Union Européenne
- VAC-SI : Système d'Information Vaccin Covid

# SOMMAIRE

# INTRODUCTION

*« L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique ».* Telle était la conviction d'Albert Einstein, célèbre mathématicien et physicien du XXème siècle. Cette conviction est d'autant plus vraie aujourd'hui. La fulgurante émergence des nouvelles technologies de l'information et des communications (NTIC) quelques décennies plus tard, s'est faite au dépens de l'homme et de sa sécurité. Au fil des années, les outils numériques ont envahi autant la sphère professionnelle que personnelle. Cette société de plus en plus hyperconnectée efface alors progressivement la frontière entre la vie privée et la vie publique, mettant en danger la sécurité matérielle, morale voire physique de l'Homme. Cette mise en danger se manifeste, par exemple, par un harcèlement scolaire qui se poursuit sur les réseaux sociaux, par la publication d'images ou de propos compromettants, par l'espionnage d'acteurs privés et publics, ou encore par le piratage des outils numériques. Cette compromission de la sécurité de chacun est plus que jamais un enjeu sociétal, politique et juridique à comprendre pour protéger numériquement la société française.

Par ailleurs, la sécurité des systèmes et des données informatiques d'un Etat ou d'une entreprise[1] est assurée via divers moyens. Cette sécurité, désignée plus communément sous l'appellation de cybersécurité, englobe la cyberdéfense, la cyberprotection et la cyberrésilience[2]. La cyberdéfense implique l'instauration de diverses mesures, techniques et non techniques permettant à un Etat de défendre les systèmes d'informations (SI) jugés essentiels dans le cyberespace, face à un acte de cybermalveillance[3]. Cette cyberdéfense est complétée par la cyberprotection, soit par un ensemble de mesures techniques, physiques et organisationnelles instaurées de telle sorte que le système puisse faire face aux cyberattaques. Pilotée par le Centre de cyberdéfense de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), cette cyberprotection permet d'éviter toute atteinte à la disponibilité, la confidentialité et l'intégrité des informations ou des services. Enfin, la cyberrésilience est évoquée comme étant la capacité des systèmes à continuer de fonctionner en mode dégradé suite à un acte cybermalveillant. Ces trois constitutives de la cybersécurité apparaissent alors comme des priorités nationales pour assurer la sécurité des SI.

---

[1] *Définition de la cybersécurité*, Dictionnaire Le Robert.

[2] « L'excellence cybersécurité dans Rennes Métropole », *Territoire de Confiance*, novembre 2019, Observatoire Economie.

[3] *Définition de la cyberdéfense*, glossaire en ligne sur le site de l'ANSSI.

Au delà de ces termes, certains spécialistes, comme Laurane Raimondo[4], estiment que l'expression *« sécurité numérique »* est plus appropriée. La cybersécurité se serait qu'une partie de la sécurité numérique. La sécurité numérique serait un terme plus englobant, traduisant mieux les défis qui se posent et incluant l'humain. La mise en place de cette sécurité numérique permet, en autre, une résistance à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises[5]. En autre, le cyberespace symbolise l'espace de communication formé par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques[6]. La sécurité numérique dans le cyberespace est assurée via des techniques spécifiques de sécurisation des SI. En plus de ces techniques, la sécurisation des SI s'inscrit dans une lutte menée par les Etats contre la cybercriminalité, soit à l'encontre des actes contrevenant aux traités internationaux et aux lois nationales au sein du cyberespace[7]. Ces infractions pénales commises via le réseau Internet ciblent les réseaux ou les SI. En outre, les délinquants peuvent utiliser ces derniers dans la perspective de commettre des infractions spécifiques au cyberespace, ou de faciliter des infractions existant avant l'arrivée d'Internet (extorsion d'argent, usurpation d'identité)[8].

Au niveau international, la cybercriminalité est encadrée par la Convention sur la cybercriminalité du Conseil d'Europe signée le 23 novembre 2001. Cette convention dite Convention de Budapest est le premier traité international relatif aux infractions pénales commises via Internet et d'autres réseaux informatiques. En matière de cybercriminalité, ce traité se révèle être le seul instrument international contraignant[9]. Par ailleurs, suite aux cyberattaques contre l'Estonie[10], le Conseil de l'Europe a approuvé le 25 juin 2013 la création d'un Centre Européen de Lutte contre la Cybercriminalité au sein d'Europol.

---

[4] Chercheuse associée (cyberdéfense, espace exo-atmosphérique et données personnelles) au sein du Centre Lyonnais d'Etudes de Sécurité Internationale et de Défense, Université de Lyon.

[5] *Définition de la cybersécurité*, glossaire en ligne sur le site de l'ANSSI.

[6] *Définition du cyberespace*, glossaire en ligne sur le site de l'ANSSI.

[7] *Définition de la cybercriminalité*, glossaire en ligne sur le site de l'ANSSI.

[8] CHOPIN (Frédérique), « Cybercriminalité », *Répertoire de droit pénal et de procédure pénale*, janvier 2020, page 4.

[9] Convention sur la cybercriminalité, 23 novembre 2011, site du Conseil de l'Europe.

[10] BERTHELET (Pierre), « Aperçus de la lutte contre la cybercriminalité dans l'Union Européenne », *Revue de Science criminelle et de droit pénal comparé 2018/1 n°1*, janvier 2018, page 64.

En France, la première loi relative à la cybercriminalité est la loi n°88-19 du 5 janvier 1988 relative à la fraude informatique[11] dite loi Godfrain qui insère, dans le Titre II du Livre III du Code Pénal, le Chapitre III *« De certaines infractions en matière informatique »* (articles 462-2 à 462-9). Suite à cette loi, la Convention de Budapest citée précédemment est ratifiée et entre en vigueur en droit interne, le 1er mai 2006, via la loi n°2005-493 du 19 mai 2005 autorisant l'approbation de la Convention sur la cybercriminalité[12].

La lutte contre la cybercriminalité se poursuit jusqu'à aujourd'hui au travers de diverses lois et ordonnances. Le Code Pénal (CP) est successivement modifié pour intégrer des dispositions relatives à la répression des atteintes aux données personnelles (articles 226-16 à 226-24 du CP), ou encore aux systèmes de traitements automatisés de données (articles 323-1 à 323-8 du CP). De plus, certaines infractions comme l'escroquerie (articles 313-1 et suivants du CP) et l'usurpation d'identité[13] (article 226-14-1 du CP) sont appliquées à la délinquance informatique.

Protéger les données personnelles apparaît indispensable. La protection de ces données, est encadrée au niveau européen par le Règlement Général sur la Protection des Données, dit RGPD[14]. Depuis le 25 mai 2018, cette réglementation européenne est obligatoire et entérine la loi Informatique et Libertés du 6 janvier 1978[15]. Le RGPD refond et renforce les droits et la protection des données à caractère personnel des personnes physiques. Ce règlement s'inscrit dans le souhait d'une gouvernance des données personnelles, en conciliant l'évolution technologique et la sécurité juridique. Pour atteindre ce souhait, ce règlement incite à l'élaboration de Codes de conduite, de labels et de mécanismes de certifications.

---

[11] Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique, *JORF*, 6 janvier 1988, page 231.

[12] Loi n°2005-493 du 19 mai 2005 autorisant l'approbation de la Convention sur la cybercriminalité et du protocole additionnel à cette Convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, *JORF*, n°116, 20 mai 2005, page 8729, texte n°2.

[13] Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, *JORF* n°0062, 15 mai 2011.

[14] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (dit Règlement Général sur la Protection des Données), entré en vigueur dans toute l'Union Européenne le 25 mai 2018.

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

La protection des données personnelles décrite par le RGPD s'applique autant aux traitements de données personnelles informatisés que sur des fichiers sur support papier[16]. En cas de violation des données personnelles, l'article 33 du RGPD précise la procédure à suivre, avec une notification à l'autorité de contrôle compétente dans les meilleurs délais. La protection des données personnelles se déroule, en autre, sous l'autorité de la Commission Nationale de l'Informatique et des Libertés (CNIL). Créée en 1978[17], cette AAI exerce un rôle d'alerte, de conseil et d'information vers tous les publics tout en disposant d'un pouvoir de contrôle et de sanction[18].

Encadrer légalement et réprimer pénalement ces cyberattaques ne suffit pas. En effet, ces comportements illégaux mettent en danger la sécurité des systèmes informatiques visés et des données traitées par ces systèmes. Cette mise en danger est d'autant plus accentuée par la qualité de données traitées. En effet, le caractère essentiel des SI s'apprécie au regard des données stockées, recueillies et traitées. Par ailleurs, de manière générale, les SI comportent bien souvent des données dites personnelles. Ces données sont des informations relatives à une personne physique identifiée ou identifiable[19]. L'identification est soit directe (nom, prénom), soit indirecte (numéro de Sécurité Sociale, plaque d'immatriculation, numéro de téléphone). L'identification peut se faire soit à partir d'une seule donnée, soit via le croisement de plusieurs données.

Depuis quelques années, cette préoccupation sécuritaire concerne plus particulièrement les outils informatiques (ordinateurs, téléphonie) utilisés au sein des établissements publics de santé (EPS). Définis par l'article L.6111-1 du Code de la Santé Publique (CSP), les EPS apparaissent comme les premiers concernés par cette protection des données personnelles. En effet, une quantité importante de données personnelles, dites données de santé, y sont traitées. Ces données se révèlent être confidentielles et sensibles puisqu'elles concernent la santé d'une personne et constituent autant des informations directes qu'indirectes, permettant d'identifier une personne physique de manière unique.

---

[16] *Fiche d'information relative au RGPD et son application*, juin 2018, site du gouvernement.fr.

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

[18] RAIMONDO (Laurane), *La protection des données personnelles, 100 Questions/Réponses, Pour comprendre et mieux se protéger*, janvier 2021, page 188.

[19] *Définition d'une donnée personnelle*, glossaire de la CNIL, site de la cnil.fr.

En effet, au sens du RGPD[20] et de la loi Informatique et Libertés du 6 janvier 1978[21], une donnée de santé est une donnée relative à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins) qui révèle des informations sur l'état de santé de cette personne. Ces données sont contenues dans un fichier. Le fichier organise les données dans un ensemble stable et structuré de données à caractère personnel. Les données d'un fichier sont accessibles selon des critères déterminés préalablement. La détermination des critères doit permettre un accès aisé aux données[22]. Les données personnelles peuvent faire l'objet d'un traitement. Le traitement de ces données correspond à une ou plusieurs opérations, via divers procédés, effectuées à partir des données. Les données peuvent alors être collectées, enregistrées, conservées, adaptées, modifiées, extraites, utilisées, communiquées par transmission, diffusées ou détruites. Le traitement doit nécessairement avoir une finalité déterminée antérieurement au recueil des données et à leur exploitation[23].

Selon l'article L.1112-1 III du CSP, *« Les établissements sont tenus de protéger la confidentialité des informations qu'ils détiennent sur les personnes qu'ils accueillent ».* Cette obligation implique que les informations détenues par les établissements ne soient pas disponibles ou divulguées à des personnes, ou des entités non autorisées. Cependant, depuis quelques années, les établissements de santé se retrouvent être la cible de cyberattaques, au travers soit de hameçonnages (mail de *phishing* visant à pirater des comptes), soit de *ransonwares*. En 2016, près de 90% des attaques *ransonware* dans le monde ont visé des établissements de santé[24], et depuis, cette menace numérique n'a pas cessé. Ces attaques consistent le plus souvent au recours à des rançongiciels, c'est-à-dire via un programme malveillant qui infecte un poste de travail. L'installation incongrue du programme a pour cause majoritaire, l'ouverture d'un courrier électronique piégé par un utilisateur du SIH[25].

---

[20] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, dit Règlement Général sur la Protection des Données, entré en vigueur dans toute l'Union Européenne le 25 mai 2018.

[21] Loi n°78-17 du 6 janvier 1978 modifiée par la loi n° 2018-493 du 20 juin 2018.

[22] *Définition d'un fichier*, glossaire de la CNIL, site de la cnil.fr.

[23] *Définition d'un traitement de données personnelles*, glossaire de la CNIL, site de la cnil.fr.

[24] QUILLIOU-RIOUAL (Mikael), QUILLIOU-RIOUAL (Morgane), *18. Accompagner les professionnels aux bons usages des TIC, Communication professionnelle et travail en équipe pluridisciplinaire en ESSMS en 29 notions*, 2020, page 211, collection Aide Mémoire, éditeur Dunod.

[25] *Définition d'un rançongiciel*, glossaire en ligne sur le site de l'ANSSI.

Une fois le fichier malveillant ouvert, le fichier bloque ou chiffre les données du poste piraté. Le rétablissement de l'accès aux données est conditionné par le paiement d'une rançon[26]. L'infection peut s'étendre au reste du SIH de l'établissement de santé soit à l'ensemble des moyens humains, techniques et organisationnels visant à assurer la circulation de l'information[27]. Par exemple, le blocage peut concerner les serveurs, les ordinateurs, la téléphonie ou encore la régulation de la température d'une salle opératoire.

Cette recrudescence des cyberattaques bouleverse la perception du numérique au sein des EPS. Jusque dans les années 2000, la préoccupation principale de ces établissements était de soigner dans le cadre d'une relation de confiance entre le patient et le professionnel de santé. La menace numérique était alors un fait rarissime. A cette époque, la France était à la pointe du numérique et les cyberattaques étaient majoritairement à l'encontre de banques.

Progressivement, les EPS sont devenus une des cibles privilégiées des cybercriminels. La prise de conscience de la sensibilité et de la protection des données personnelles détenues par les EPS a donné lieu à un programme Hôpital Numérique en 2013. Ce programme a été renforcé par le RGPD en 2018 notamment l'article 32. Cet article relatif à la sécurité du traitement des données personnelles sous-entend que les directeurs d'établissements sont tenus de prendre des mesures de sécurité du fait de la sensibilité des données traitées.

Dans l'atteinte des prérequis de ce programme, et du plan d'action sur la sécurité des SI, une Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) a été élaborée par l'Agence des Systèmes d'Information Partagées de santé (ASIP Santé). Plus récemment, le projet de transformation de notre système de santé dit *« Ma Santé 2022 »* place l'individu au coeur du système de santé. Le patient devient acteur de santé et apparaît comme le premier bénéficiaire des services numériques en santé. Dans cette perpective, le projet tend à garantir une collecte et une utilisation de données à caractère personnel de santé respectueuses des droits fondamentaux du patient[28].

---

[26] VITARD (Alice), *Ransomware, Covid-19, espionnage, terrorisme… L'ANSSI fait un état des lieux de la cybersécurité*, 5 novembre 2020, site de l'Usine Digitale.

[27] CARTAU (Cédric), « Chapitre 2. Les fondamentaux, La sécurité du système d'information des établissements de santé », *Presses de l'EHESP*, 2018, page 21.

[28] KERMARREC (Jean-Michel), « La judiciarisation de l'usage numérique en santé…un risque émergent », *Revue Droit et Santé n°88*, mars 2019, page 238.

Par ailleurs, la préoccupation du Gouvernement pour la cybersécurité au sein des établissements de santé a été mise en exergue par le programme HOP'EN pour un *« Hôpital numérique ouvert sur son environnement »* présenté le 25 avril 2019 par l'ancienne Ministre des Solidarités et de la Santé, Agnès Buzyn. Pour la première fois, le Ministère des Solidarités et de la Santé a prononcé un discours sur la cybersécurité. La cybersécurité y est alors présentée comme une priorité nationale pour tous les EPS.

En dépit de ces programmes successifs, le renforcement de la cybersécurité est ralenti par la pression financière croissante pesant sur les EPS, contraignant ces derniers à effectuer des restrictions budgétaires. Ces complications ont été accentuées par la survenance en novembre 2019 du virus de la Covid-19. Le fonctionnement de la société française, et plus particulièrement des EPS a été particulièrement affecté. Profitant de cet affaiblissement et considérant que le Gouvernement paierait pour une continuité du service public, des multiples cyberattaques à l'encontre des EPS ont été perpétrées. En l'espace d'un an seulement, les attaques via des *ransonwares* ont été multipliés par trois voire quatre. Selon Guillaume Poupard, directeur de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), c'est un phénomène particulièrement inquiétant. Il ajoute qu'*« il n'existe aucune raison que cela s'infléchisse à court terme »*[29].

A sa grande surprise, au début de la crise sanitaire, Guillaume Poupard révèle le fait qu'un communiqué de presse de la part des grands groupes criminels annonçait une suspension des cyberattaques à l'encontre des hôpitaux. Par exemple, un des groupes actifs en matière de *ransonwares*, *Maze Team ransonware gang*, a annoncé renoncer à toute attaque[30]. Durant le printemps dernier, en Europe, une seule attaque contre un hôpital tchèque a été recensée[31]. Malheureusement, cette suspension des cyberattaques n'a été que de courte durée. Un virus informatique, *Emotet*, a été actif dans un grand nombre d'entreprises et d'institutions françaises entre le mois d'août et fin septembre 2020.

---

[29] VITARD (Alice), *Ransomware, Covid-19, espionnage, terrorisme… L'ANSSI fait un état des lieux de la cybersécurité*, 5 novembre 2020, site de l'Usine Digitale.

[30] FEVRIER (Rémy), « Vers une nécessaire évolution du paradigme dominant en management stratégique ? », Covid-19 et cyberattaques, *Revue Française de Gestion 2020/8,* n°293, page 90.

[31] BERKAOUI (Héléna), *Cyberattaque : « Il y a une explosion de la grande criminalité », rapporte le directeur de l'Anssi*, Public Sénat, 4 novembre 2020.

Par conséquent, au delà du défi de l'hygiène sanitaire lancé par la pandémie mondiale actuelle de la Covid-19, et face à la multiplication des actes cybermalveillants, les EPS doivent relever le défi d'une *« hygiène numérique »*. L'adoption d'une hygiène numérique est d'autant plus importante et urgente au regard des conséquences pouvant être engendrées par une cyberattaque.

L'analyse de cette problématique majeure se limitera principalement à la sécurité numérique des établissements publics de santé en France. Du fait du caractère international de la menace cybercriminelle, quelques exemples de pays étrangers seront néanmoins donnés pour illustrer les propos.

De cette façon, les cyberattaques sont des électrochocs pour les EPS : anticiper avant la survenance de ces actes cybermalveillants est primordial. La question ici sera de comprendre dans quelle mesure l'instauration d'une sécurité numérique des établissements publics de santé en France doit être une priorité à la fois individuelle et collective, autant pour garantir le fonctionnement des EPS que pour préserver les données personnelles de santé traitées par ces derniers.

La survenance d'une cyberattaque à l'encontre des EPS révèle l'importance de la protection des données personnelles (Première partie). Il convient alors de comprendre les enjeux et les éléments à prendre en considération pour une sécurité numérique protectrice et non destructrice des EPS, et donc des données personnelles traitées. Pour cela, renforcer la sécurité numérique des EPS via une stratégie de défense se révèle indispensable autant pour affronter les défis actuels que futurs (Deuxième partie).

# PREMIÈRE PARTIE - La survenance de cyberattaques à l'encontre des établissements publics de santé, témoignage de l'importance de la protection des données personnelles

*« Vingt-sept attaques majeures concernant des hôpitaux en 2020 ; il y a en a une par semaine en 2021 »*. Ces chiffres exponentiels énoncés devant le Sénat par Cédric O[32], lors d'une session en février 2021[33] mettent en exergue l'intensification de la survenance des cyberattaques à l'encontre des établissements publics de santé. Par ailleurs, avant d'envisager un renforcement de la sécurité numérique de ces établissements, une protection adéquate des données personnelles de santé traitées par les établissements implique nécessairement d'appréhender les origines complexes et globales de cette menace grandissante (Titre I) et d'évaluer l'impact de cette dernière autant envers l'usager que sur l'ensemble du système du santé français (Titre II).

[32] Secrétaire d'Etat chargé de la transition numérique et des communications électroniques depuis 2019.

[33] *Compte rendu intégral, séance du mercredi 17 février 2021* (63ème jour de séance de la session), session ordinaire de 2020-2021, Sénat, Journal Officiel de la République Française, page 1145.

# Titre I : Les cyberattaques, origines complexes et globales d'une menace grandissante

Chaque jour, des attaques numériques de masse parcourent le cyberespace dans le but d'atteindre des objets non sécurisés pour en prendre le contrôle facilement et les utiliser, le cas échéant, dans des attaques. Ces attaques numériques de masse visent, intentionnellement ou pas, les établissements publics de santé. Visés ou pas, ces établissements détiennent et traitent des données personnelles de santé. En dehors des attaques de masse, ces données se révèlent être l'objet de convoitise pour diverses raisons (Chapitre I). Ces convoitises poussent alors des cybercriminels à exploiter les failles des EPS, révélant par la même occasion les défaillances numériques des SIH (Chapitre II).

## Chapitre I : Les données personnelles de santé, objet de convoitise multifactorielle

Les données personnelles de santé détenues par les EPS, de par leur quantité et leur sensibilité, sont convoitées. De manière générale, selon Samuel Hassine, chef d'Etat major du centre opérationnel de l'ANSSI, les cyberattaques sont motivées, principalement, par trois motifs : les cybercrimes, la propagande et l'espionnage[34]. En ce qui concerne les SI des EPS, les cyberattaques à leur encontre peuvent être, à titre exceptionnel, issues de motivations individuelles ou dans un but de propagande. Des personnes désintéressées, communément désignées sous l'appellation de *hackers*, piratent un système informatique par jeu, sans intention de nuire[35]. Ce sens du défi apparaît indépendant de l'âge, d'un diplôme ou de l'expérience professionnelle[36]. Concernant les EPS, les cyberattaques proviennent principalement de cybercrimes en raison de l'enjeu économique représenté par les données personnelles de santé (Section I) et de l'espionnage, exacerbé par le contexte sanitaire actuel (Section II).

---

[34] *Dans la peau d'un expert en cybersécurité* (ft Master Geopolitix), Justin Izu, 30 août 2018, sur youtube.com (4:22).

[35] *Définition d'un hacker*, Dictionnaire Le Robert.

[36] ARPAGIAN (Nicolas), *La cybersécurité*, Que Sais-je ?, Presses Universitaires de France, page 5.

## Section I : La valeur économique autant de la cible que des données personnelles recueillies

Les cyberattaques révèlent un souhait de déstabiliser les EPS (Paragraphe I) et surtout dévoilent l'existence d'un marché lucratif des données personnelles de santé (Paragraphe II).

### Paragraphe I : La déstabilisation des établissements publics de santé

Les EPS sont des cibles, choisies pour leur rôle fondamental dans la permanence des soins (A), qui sont incitées à ne pas céder aux demandes des cybercriminels (B).

#### A) Des cibles choisies pour leur rôle fondamental dans la permanence des soins…

Au 31 décembre 2018, le secteur hospitalier français est constitué de 3 036 structures dont 1 356 établissements de santé du secteur public[37]. Ces établissements représentent plus de 243 000 lits. Ils assurent, en autre, le diagnostic, la surveillance et le traitement des malades, des blessés et des femmes enceintes[38]. Le rôle des EPS apparaît indispensable dans la permanence des soins. Cette permanence des soins a d'ailleurs été reconnue par la loi HPST[39] comme la première mission de service public assurée par les établissements de santé[40]. Le caractère indispensable des EPS a été d'autant plus confirmé depuis le début de la pandémie mondiale de la Covid-19 en novembre 2019. Les EPS s'illustrent comme un des piliers de la gestion sanitaire de cette pandémie en France. Parallèlement à ce rôle clé dans la gestion sanitaire, depuis novembre 2019, plusieurs EPS ont été victimes de cyberattaques via des rançongiciels à l'image du Centre Hospitalier (CH) de Dax (Landes), le mardi 9 février 2020. L'accès aux ordinateurs, téléphones ou tout matériel informatique s'est révélé impossible[41]. En effet, les données personnelles du SIH étaient chiffrées et donc inaccessibles. Le rétablissement de l'accès aux SIH était conditionné par le versement d'une rançon en bitcoins.

---

[37] *Personnels et équipements de santé,* Tableaux de l'économie française, INSEE, 27 février 2020, édition 2020.

[38] Article L.6111-1 du Code de la santé publique.

[39] Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, *JORF* n°0167, 22 juillet 2009.

[40] Article L.6112-1 du Code de la santé publique.

[41] QUÉGUINER (Thomas), « La cyberattaque par rançongiciel à Dax illustre l'explosion de cette menace sur l'hôpital », Bloc note sanitaire, *Hospimedia*, 12 février 2021.

Attaquer informatiquement ces EPS, c'est partir du principe qu'ils sont tellement indispensables au bon fonctionnement du système de santé français et de la gestion sanitaire de la Covid-19 que tout sera fait pour que la cyberattaque prenne fin. Cette idée préconçue est avérée puisque certaines cibles ont tendance à céder aux demandes des cybercriminels. Pour autant, les EPS sont incités à ne pas céder aux demandes des cybercriminels.

### B) … qui sont incités à ne pas céder aux demandes des cybercriminels

La France est aujourd'hui l'un des pays les plus attaqués en matière de *ransonwares*. Cette menace vise, en autre, les établissements de santé. Cette recrudescence est expliquée selon Johanne Brousse, Vice-Procureur chargée de la section cybercriminalité du Parquet de Paris, par un paiement trop facile des rançons de la part des victimes[42]. En France, payer la rançon aux cybercriminels n'est pas illégal. Néanmoins, ces paiements effectués encouragent les cybercriminels à réitérer leurs actes malveillants. Certains établissements de santé, notamment dans le privé, ont déjà cédés et payés les rançons réclamées. Guillaume Poupard, directeur général de l'ANSSI, justifie ces paiements par le fait que les cibles de cyberattaques préfèrent payer quelques millions de rançons plutôt que quelques dizaines de millions au titre de la perte des données garantie par la police d'assurance contractée[43]. Ces paiements s'expliquent donc par une évaluation des coûts. En effet, il semble, bien souvent, que payer la rançon revient moins coûteux par rapport à une gestion de la cyberattaque sans payer la rançon. Ne pas payer la rançon implique de remplacer les outils informatiques infectés par exemple, et surtout de perdre des données nécessaires au bon fonctionnement de l'établissement ainsi qu'à la prise en charge qualitative des patients.

Cependant, la politique menée est tout autre dans le public. Dans le public, le mot d'ordre est de ne pas payer. Cette injonction est un des leitmotivs de l'ANSSI. En cas de cyberattaque, les EPS sont incités à ne jamais payer la rançon demandée pour le déverrouillage des outils informatiques. Le paiement ne garantit pas en rien l'obtention d'un moyen de déchiffrement. De surcroît, l'obtention d'une clé de déchiffrement ne garantit pas toujours de récupérer l'intégralité des fichiers chiffrés. Les fichiers de base de données modifiés et chiffrés par le rançongiciel ont de très fortes probabilités d'être corrompus[44]. Par

---

[42] *Table ronde sur « La cybersécurité des ETI-PME-TPE : la réponse des pouvoirs publics »*, Délégation aux entreprises, Sénat, jeudi 15 avril 2021, 9:38.

[43] *Ibid.*, 9:55.

[44] *Attaques par rançongiciels, tous concernés, Comment les anticiper et réagir en cas d'incident ?*, guide de sensibilisation de l'ANSSI en partenariat avec la DACG du Ministère de la Justice, août 2020.

ailleurs, le paiement risque d'inciter les cybercriminels à poursuivre leurs activités, entretenant alors ce système frauduleux. D'autant plus que le paiement de la rançon risque de financer d'autres activités illégales (secte, terrorisme, mafia)[45].

Certes, les établissements de santé sont déstabilisés et de prime abord, la solution semble de payer pour déverrouiller les outils informatiques et rétablir le fonctionnement des SIH. Les cyberattaques, lorsque les établissements de santé cèdent en payant, peuvent alors se révéler lucratives pour les cybercriminels. Au delà du paiement des rançons, les données personnelles détenues par les EPS constituent des éléments de plus en plus convoités pour leur valeur marchande.

## **Paragraphe II : L'existence d'un marché lucratif des données personnelles de santé**

Les données personnelles de santé ont une valeur marchande (A) et sont vendues pour diverses finalités, autant directes que indirectes (B).

### A) La valeur marchande des données personnelles de santé…

Récupérer les données personnelles de santé des personnes ayant été admises dans un établissement public de santé permet à la fois de capter les richesses d'autrui (numéro de carte bancaire, numéro de Sécurité Sociale, signature) et à la fois de les vendre. Du fait de l'abolition des frontières physiques, les cyberattaques peuvent provenir de n'importe où et les données recueillies peuvent être vendues à n'importe qui sur le globe. De plus, le XXIème siècle est qualifié de *« siècle de la révolution numérique et de l'économie de la donnée »*. Au début du siècle, les cyberattaques visaient principalement les banques, les assurances et les industries. Progressivement, la valeur économique des données dans le monde a dépassé celle des données bancaires et même celle du pétrole. Qualifiées de « *nouveau pétrole »*, les données personnelles ont une valeur économique mondiale estimée à 170 milliards d'euros en 2020. Ce chiffre est probablement sous-estimé[46]. Il appert alors que les cyberattaques se sont déportées progressivement sur la santé du fait de la faible sécurité numérique des EPS et de l'utilité de ces données pour diverses finalités.

---

[45] RAIMONDO (Laurane), *La protection des données personnelles, 100 Questions/Réponses, Pour comprendre et mieux se protéger*, janvier 2021, page 197.

[46] *Ibid.*, page 35.

## B) … convoitées pour diverses finalités directes ou indirectes

Sur Internet, rien n'est gratuit. Les sites en apparence à l'accès gratuit récupèrent les données personnelles fournies lors d'une inscription ou d'un achat (email, nom, prénom, date de naissance, adresse). Même l'historique des recherches est enregistrée via les cookies[47] à des fins publicitaires ou statistiques pour déterminer les préférences vestimentaires ou politiques par exemple. Toutes ces données personnelles constituent un marché lucratif. Concernant les EPS, les cibler permet, par exemple, de récupérer les répertoires d'adresses mails. Ces répertoires sont convoités par les pirates du web puisque la diffusion d'un virus s'effectue généralement via l'envoi de mails[48].

Au sein de l'Union Européenne (UE), le marché des données personnelles représenterait plus de 400 milliards d'euros. Selon les projections de la Commission Européenne, ce marché pourrait atteindre jusqu'à 839 milliards d'euros dans l'UE à 27[49] d'ici 2025. Ce marché est la source principale des GAFAM[50]. Rien qu'en 2018, Facebook a généré plus de 55 milliards de dollars de revenus dont 22 milliards de bénéfices grâce aux données personnelles[51]. En dehors des GAFAM, ces données sont le fond de commerce des entreprises de courtage des données depuis les années 1960. Ces données servent autant pour le marketing, les assurances ou encore vérifier la solvabilité d'une personne physique ou morale.

Dans le monde, plus de 4 000 entreprises ont pour activité principale le commerce des données personnelles[52]. Ces vendeurs de données sont qualifiés de *data brokers*. Les données personnelles deviennent alors l'objet de multiples convoitises basées sur les intérêts financiers pouvant découler de leur commerce. Autant les GAFAM que les entreprises de courtage de données, considèrent les données personnelles comme une matière première dans l'essor de

---

[47] *« Petit fichier stocké par un serveur dans le terminal (ordinateur, téléphone) d'un utilisateur et associé à un domaine web »,* Définition d'un cookie, sur le site cnil.fr.

[48] QUILLIOU-RIOUAL (Mikael), QUILLIOU-RIOUAL (Morgane), *18. Accompagner les professionnels aux bons usages des TIC, Communication professionnelle et travail en équipe pluridisciplinaire en ESSMS en 29 notions*, 2020, page 213, collection Aide Mémoire, éditeur Dunod.

[49] *Stratégie européenne pour les données, Une Europe adaptée à l'ère numérique*, sur le site de la Commission Européenne ec.europa.eu.

[50] Acronyme pour les initiales des cinq entreprises américaines dominant le marché du numérique : Google, Apple, Facebook, Amazon et Microsoft.

[51] *The Great Hack*, documentaire réalisé par Karim Amer et Jeanne Noujaim, 2019.

[52] *La sécurité des données personnelles*, conférence du 17 mai 2021 animée par Laurane Raimondo, chercheuse associée (cyberdéfense, espace exo-atmosphérique et données personnelles) au sein du Centre Lyonnais d'Etudes de Sécurité Internationale et de Défense, et Sana Bakfalouni, co-fondatrice d'AKANT, experte en sécurité de l'information, Lyon - Disrupt Campus / Université de Lyon, 20:04.

leur activité. Les données récupérées par le biais de cyberattaques trouvent, sans aucun doute, des acquéreurs friands d'en savoir toujours plus sur les citoyens, quelque soit le pays.

Cette convoitise est d'autant plus accentuée par la confrontation de modèles de traitement de données entre les pays, notamment entre celui du RGPD et des GAFAM. Cette confrontation engendre alors des traitements de données illégitimes. Cette illégitimité a été mise en évidence par un arrêt majeur rendu par la Cour de Justice de l'Union Européenne (CJUE) le 16 juillet 2020. Dans cet arrêt[53], la Cour estime que le régime de transfert de données entre l'UE et les Etats-Unis, dit « *Privacy Shield* » est invalide. Cette absence de validité est justifiée au regard du RGPD. Le RGPD dispose qu'un transfert de données personnelles vers un pays tiers ne peut se faire que si ce dernier est capable d'assurer un niveau de protection adéquat[54]. Néanmoins, au regard des exigences posées par le RGPD, la Cour estime que la réglementation interne des Etats-Unis n'encadre pas suffisamment la protection des données à caractère personnel. Cette réglementation ne répondrait pas à des exigences substantiellement équivalentes à celles requises par l'UE. En conséquence, la confrontation des modèles de traitement des données entre les pays peut amener à des acquisitions et des utilisations de données illégales.

En dehors de ces enjeux économiques, les cyberattaques constituent un enjeu sanitaire, surtout dans le contexte actuel de crise sanitaire avec la course aux vaccins.

## Section II : La valeur sanitaire des données personnelles de santé

Les données personnelles de santé se révèlent avoir une véritable valeur sanitaire provoquant l'émergence d'espionnages. Ces espionnages restent, encore aujourd'hui, occultés (Paragraphe I). Malgré tout, une prise de conscience s'effectue sur le véritable fléau qu'ils constituent en terme de concurrence sur le marché de la santé (Paragraphe II).

### Paragraphe I : L'espionnage, phénomène occulté en dépit de sa gravité

L'espionnage est une menace qui ne doit pas être oubliée (A) et cette menace est d'autant plus d'actualité depuis la recherche mondiale d'un vaccin contre la Covid-19 (B).

---

[53] *Affaire C-311/18, Data Protection Commissionner contre Maximillian Schrems et Facebook Ireland Ltd*, Cour de Justice de l'Union Européenne, 16 juillet 2020.

[54] *La Cour invalide la décision 2016/1250 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis*, Cour de Justice de l'Union Européenne, communiqué de presse n°91/20, Luxembourg, 16 juillet 2020, page 1.

## A) Une menace à ne pas oublier…

La crise sanitaire actuelle ne doit en aucun cas faire oublier les autres menaces comme l'espionnage. Selon Guillaume Poupard, l'espionnage est la menace dont personne ne veut parler alors c'est probablement la plus grave[55]. Cette gravité est d'autant plus avérée que des opérations d'espionnage sont perpétrées de manière exponentielle. Plus précisément, cet espionnage se fait via des *spywares*. Aussi appelé espiogiciel, un *spyware* est un logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur l'environnement sur lequel il est installé[56]. Ces informations portent par exemple, sur les usages habituels des utilisateurs du système. Cet espionnage est bien présent sur le territoire français puisque la majeure partie des cyberattaques à l'encontre des EPS français s'est déroulée, de prime abord, via un logiciel espion. La cyberattaque subie par le Centre Hospitalier Universitaire (CHU) Charles Nicolle de Rouen (Seine-Maritime) le 15 novembre 2019 illustre ces propos. Un logiciel espion a d'abord été installé et ensuite, les données et fichiers ont été chiffrés[57].

De plus, divers virus d'espionnage sont régulièrement détectés au sein des systèmes d'information d'organisations privées et publiques françaises. En effet, en 2014, un éditeur d'anti-virus a découvert un virus d'espionnage nommé « *REGIN* ». Actif depuis au moins 2008, ce virus serait utilisé comme plateforme de cyberespionnage contre des organisations autant privées que publiques. Ce virus serait actif dans 5% des organisations françaises liées à la santé. Il aurait pour rôle principal de collecter des données et pourrait également prendre le contrôle d'ordinateurs cibles, prendre des captures d'écrans et voler les mots de passe sur des cibles bien identifiées[58]. En dehors de ce virus, d'autres virus dits d'Etat comme « *FLAME* » circulent dans le cyberespace. Ces virus sont des virus de cyberespionnage crées par un Etat. Par exemple, des groupes cyber tels qu'*Advanced Persistent Threat APT41* mènent des opérations d'espionnage pour la Chine[59]. L'espionnage est une menace à ne pas occulter, plus particulièrement, en période de pandémie mondiale, depuis la recherche du vaccin.

---

[55] VITARD (Alice), *Ransomware, Covid-19, espionnage, terrorisme… L'ANSSI fait un état des lieux de la cybersécurité*, 5 novembre 2020, site de l'Usine Digitale.

[56] *Définition d'un spyware*, glossaire en ligne sur le site de l'ANSSI.

[57] QUEMENER (Myriam), « Cybersécurité et protection des données de santé », *Dalloz IP/IT*, 20 mai 2020, page 303.

[58] *Unité 2 - Les fichiers en provenance d'Internet*, Module 3 - Sécurité sur Internet, Défis et enjeux de la cybersécurité, MOOC ANSSI.

[59] ADEYOOLA (Hassan), *Advanced Persistent Threat : Detection and Defence, Bachelor in Science University of Bradford,* 15 July 2021, HAL, page 3.

### B) … d'autant plus d'actualité depuis la recherche du vaccin

Les opérations d'espionnage sont l'occasion pour les cyberattaquants d'obtenir des informations stratégiques sur les politiques extérieures et de défense, mais également un moyen d'accéder à des informations industrielles et aux secrets commerciaux des organisations[60]. En autre, ce vol de données personnelles est particulièrement attrayant dans la course aux vaccins. La recherche pour le vaccin se révèle être alors une cible de renseignement. Cet espionnage est illustré notamment par la cyberattaque dont a été victime l'Institut Pasteur de Lille en juin 2020. Cible de tentatives chaque semaine, aucune donnée n'a pu être piratée. Cependant, ces tentatives soulignent à quel point le souhait de recueillir des données sur les recherches vaccinales devient omniprésent. Un autre exemple illustre cet espionnage, c'est celui de la cyberattaque de l'Agence Européenne du Médicament (EMA) en décembre 2020[61]. Lors de cette cyberattaque, des documents relatifs à la réglementation portant sur le vaccin de BioNTech contre le Covid-19 ont été consultés illégalement. Ces documents concernaient les tests effectués et les personnes concernées. La crise sanitaire a donc accentué la survenance d'espionnages à l'encontre d'établissements détenant des données personnelles de santé. Au delà des vaccins, ces espionnages constituent, pour la France, un véritable désastre en terme de concurrence sur le marché de la santé.

## <u>Paragraphe II</u> : L'espionnage, véritable fléau en terme de concurrence sur le marché de la santé

Les données personnelles sont la matière première des nouvelles technologies numériques (A) et une fois récupérées, ces dernières sont un moyen de défier la concurrence sur le marché de la santé (B).

### A) Les données personnelles de santé, matière première des nouvelles technologies numériques…

Les données de santé sont devenues prépondérantes autant dans la recherche que l'intelligence artificielle (IA). Elles sont des éléments recherchés dans le développement de

---

[60] « Papiers numériques », *Revue annuelle de l'ANSSI*, édition 2020, page 34.

[61] ROBILLARD (Jérôme), « L'Agence européenne du médicament est visée par une cyberattaque », Système d'information, *Hospimedia*, 10 décembre 2020.

nouvelles technologies. En effet, l'IA est tributaire de cette matière première[62]. L'IA, dite *machine learning,* a besoin d'une masse phénoménale de données pour apprendre et s'améliorer. Grâce à ces données, l'IA peut impacter positivement le système de santé via la détection de cancers ou de maladies neuro-dégénératives[63]. Cependant, l'utilisation des données par l'IA doit être encadrée. L'IA peut effectivement impacter, négativement, le système de santé français en brouillant la frontière de l'éthique pour certaines recherches. Cette dimension éthique est évoquée par l'Organisation Mondiale de la Santé (OMS) dans son premier rapport mondial consacré à l'éthique et à la gouvernance de l'IA dans le domaine de la santé[64]. Ce rapport souligne le fait que, certes, l'IA constitue un grand espoir dans l'amélioration de la prestation des soins et de la médecine mais seulement à condition que l'éthique et les droits humains soient placés au coeur de sa conception, de son déploiement et de son utilisation. C'est pourquoi les données personnelles de santé se révèlent être une matière première pour les nouvelles technologies numériques, et par la même occasion, un moyen de défier la concurrence sur le marché de la santé.

### B) … comme moyen de défier la concurrence sur le marché de la santé

Récupérer des données personnelles de santé peut constituer un enjeu majeur en matière de concurrence sur le marché de la santé. Par exemple, ces données se révèlent précieuses dans le cadre de l'oncologie. En effet, elles sont considérées comme une mine d'or pour le business des médicaments. Ces données se retrouvent alors vendues sur le *dark net*[65] à des laboratoires pharmaceutiques. Ces laboratoires peuvent ensuite adapter leur production en fonction des pathologies ciblées à travers les données personnelles de santé des patients.

De surcroît, cette préciosité des données personnelles de santé dans le domaine pharmaceutique a dernièrement été révélée par le scandale d'IQVIA en mai 2021. Le fonctionnement de l'entrepôt de données de la société, a été autorisé par la CNIL le 12 juillet

---

62 MONNERIE (Nils), « Les défis de la commercialisation des données après le RGPD : aspects concurrentiels d'un marché en développement »*, Revue Internationale de Droit Economique 2018/4,* avril 2018, page 432.

63 *La sécurité des données personnelles*, conférence du 17 mai 2021 animée par Laurane Raimondo et Sana Bakfalouni, Lyon - Disrupt Campus / Université de Lyon, 44:10.

64 *L'OMS publie le premier rapport mondial sur l'intelligence artificielle (IA) appliquée à la santé et six principes directeurs relatifs à sa conception et à son utilisation*, communiqué de presse, 28 juin 2021.

65 Web clandestin.

2018[66]. Cependant, il a fait l'objet de polémiques concernant la collecte de données de santé par les pharmacies, via la carte vitale. A l'insu des patients, un logiciel utilisé par une pharmacie sur deux collectait le numéro de Sécurité Sociale, les achats de médicaments et donc un ensemble d'informations relatives à la santé physique et mentale du patient. A cette occasion, la CNIL a rappelé les règles applicables et garanties exigées de la part d'IQVIA[67]. La CNIL est venue préciser que les données de santé destinées au secteur public, à la Sécurité Sociale ou des professionnels de santé peuvent être réutilisées pour des projets d'intérêt public[68]. Par déduction, les projets de recherche d'Iqvia sont rendus possibles selon la CNIL, pour favoriser la recherche médicale. Ces conditions d'accès assouplies créent alors une brèche juridique pour des acteurs privés comme IQVIA. L'obtention légale ou illégale des données personnelles de santé constituent donc un enjeu majeur dans le domaine pharmaceutique pour défier la concurrence sur le marché de la santé. Cette concurrence se reflète aussi par certaines cyberattaques qui visent exclusivement à détruire les SI.

Que ce soit pour des raisons individuelles, financières ou sanitaires, les données personnelles de santé sont l'objet de convoitises. Au delà de ces convoitises générées, les cyberattaques témoignent des failles des EPS.

---

[66] Délibération 2018-289 du 12 septembre 2018 autorisant la société IQVIA Opérations France à mettre en oeuvre un traitement automatisé de données à caractère personnel ayant pour finalité la constitution d'un entrepôt de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, dénommé base de données LRX (n°2120812), CNIL.

[67] *Entrepôt de données santé IQVIA : la CNIL rappelle les conditions et cadre légal ayant permis son autorisation en 2018*, 17 mai 2021, cnil.fr.

[68] Article L.1460-1 du Code de la santé publique.

# Chapitre II: Les cyberattaques, révélatrices des failles des établissements publics de santé

*« La numérisation accroît la qualité des soins de santé mais fait apparaître de nouvelles vulnérabilités »* admet Paul-Emile Cloutier, Président et chef de la direction de SoinsSantéCAN[69]. Le secteur de la santé fait partie des secteurs les plus fragiles en matière de sécurité informatique[70]. Selon Xavier Léonetti[71], cette fragilité a pour origine l'exploitation des failles liées à la crise sanitaire, les vulnérabilités des réseaux informatiques et le télétravail qui accroît les risques de défaillances des SIH. Ces risques de défaillances, au delà des exemples concrets évoqués par le magistrat, sont exacerbés par d'autres failles, qu'elles soient organisationnelles (Section I), ou encore réglementaires et humaines (Section II).

---

## Section I : Les failles organisationnelles des EPS : fragilités exploitées et révélées par les cyberattaques

Les failles organisationnelles exploitées par les cyberattaques révèlent l'existence de SIH morcelés et vétustes (Paragraphe I) dont le morcellement est accru par les pratiques numériques des utilisateurs du SIH (Paragraphe II).

### Paragraphe I : Des systèmes d'information hospitaliers morcelés et vétustes

Les SIH des EPS apparaissent inefficaces (A) et la disparité des logiciels ne fait que fragiliser cette absence de performance (B).

#### A) Des SIH inefficaces…

Seuls 30% des établissements publics de santé disposent d'un SIH réellement efficace. Tel est le constat dressé par un rapport du Sénat de 2005[72] demandé par la Commission des

---

[69] VENNE (Jean-François), « Les établissements des réseaux de la santé dans la mire des pirates », *Gestion 2019/3*, Volume 44, page 71.

[70] LOMBARD-LATUNE (Marie-Amélie), *Les données personnelles, la matière première de la cybercriminalité*, Sécurité et Liberté, 5 avril 2021, lopinion.fr.

[71] Magistrat au sein de la juridiction économique et financière de Marseille et futur dirigeant de la mission de prévention et de lutte contre la cybercriminalité à la Direction des Affaires Criminelles et des grâces du Ministre de la Justice.

[72] JÉGOU (Jean-Jacques), *Rapport d'information sur l'informatisation dans le secteur de la santé, Sénat*, 2005, n°62, page 11.

Finances, du contrôle budgétaire et des comptes économiques de la Nation. Ce manque d'efficience est accentué par l'utilisation d'applications jugées vieillissantes et peu intégrées. Pour pallier à ces lacunes numériques, depuis 2005, plusieurs programmes ont été initiés. Parmi eux, le programme Hôpital numérique a été piloté par la Direction Générale de l'Offre de Soins (DGOS). Lancée en novembre 2011, cette stratégie nationale définit un plan de développement et de modernisation des SIH via des pré-requis et des domaines fonctionnels devant être atteints par les établissements de santé entre 2012 et 2017. Par exemple, un des pré-requis est la confidentialité et un des domaines prioritaires est le Dossier Patient Informatisé et Interopérable (DPII). Les résultats 2018 publiés par la DGOS, en collaboration avec l'ATIH, démontrent une nette amélioration des SIH, en comparaison avec le rapport de 2005 évoqué précédemment. En effet, l'ensemble des prérequis du programme Hôpital Numérique est atteint dans 71% des établissements[73]. En dépit de cette amélioration significative, ce même rapport fait état d'une forte disparité en matière de logiciels.

### B) … affaiblis par la disparité des logiciels dans le secteur de la santé

Depuis les années 1990, les EPS peuvent s'adresser librement au fournisseur de leur choix. Cependant, les acteurs industriels proposant des logiciels dans le secteur de la santé présentent une forte diversité. En 2018, 317 sociétés sont inscrites sur le Répertoire des Editeurs de Logiciels et des Intégrateurs du Monde de la Santé (RELIMS)[74]. Ce qui représente plus de 864 logiciels disponibles sur le marché français[75]. Cette disparité des logiciels est également flagrante au sein de nombreux établissements. Certains SIH français comptent entre 80 et 300 applications informatiques propres à des processus (dématérialisation des factures, gestion des achats, résultats d'examens de biologie, prescriptions pharmaceutiques) ou des fonctions (gestion des ressources humaines, gestion économique et financière, demande de transport interne, gestion administrative des patients)[76]. Ce nombre d'applications atteint 518 aux Hospices Civils de Lyon (HCL) et 1 000 à l'Assistance Publique - Hôpitaux de Paris (AP-HP). Cette diversité des logiciels accentue le morcellement des SIH des EPS.

---

[73] *Etat des lieux des systèmes d'information hospitaliers*, Atlas des SIH, Direction Générale de l'Offre de Soins (DGOS), 15 mai 2018, page 5.

[74] Application web sécurisée, développée, maintenue et hébergée par la Direction Générale de l'Offre de Soins (DGOS) du Ministère de la Santé.

[75] *Etat des lieux des systèmes d'information hospitaliers*, Atlas des SIH, Direction Générale de l'Offre de Soins (DGOS), 15 mai 2018, page 5.

[76] *Rapport sur l'application des lois de financement de la Sécurité Sociale*, Cour des Comptes, septembre 2016, page 330.

De surcroît, la pression financière croissante pesant sur les EPS et les restrictions budgétaires ont conduit les EPS à ne consacrer que 2% de leurs dépenses aux SIH[77]. Le manque de moyens financiers se répercute sur l'efficience du matériel informatique. Les restrictions ont mené à une vétusté du matériel informatique, à l'absence de mises à jour du système d'exploitation (logiciels, versions anciennes de Windows) et à l'utilisation d'outils gratuits peu protégés comme Dropbox. Enfin, contrairement à d'autres secteurs, le secteur de la santé fonctionne via divers réseaux où coexistent différents niveaux de confidentialité. Ce morcellement édifie les EPS en cibles de premier choix. Les SIH, en plus d'être morcelés et vétustes se révèlent fragilisés par les pratiques numériques des utilisateurs du SIH.

## **Paragraphe II : L'accentuation du morcellement par les pratiques numériques des utilisateurs du SIH**

Le morcellement des SIH est exacerbé par les difficultés d'interopérabilité entre les applications (A) et par l'existence de pratiques numériques à risque (B).

### A) De difficultés d'interopérabilité entre les applications…

Le morcellement des SIH est accentué par des difficultés d'interopérabilité. Depuis la loi du 26 janvier 2016[78], et plus particulièrement depuis l'ordonnance du 12 mai 2021[79], les SI, les services ou outils numériques destinés à être utilisés par les professionnels de santé et les personnes exerçant sous leur autorité, et par les établissements et services de santé, doivent être conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public[80], soit par l'ANS[81], pour le traitement des données, leur conservation sur support informatique et leur transmission par voie électronique[82]. Néanmoins, en l'absence de solutions de marché couvrant l'ensemble des fonctions hospitalières, le manque d'interopérabilité entre les applications demeure l'obstacle majeur à la cohérence et à

[77] *Etat des lieux des systèmes d'information hospitaliers,* Atlas des SIH, Direction Générale de l'Offre de Soins (DGOS), mai 2015, page 5.

[78] Loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022, 27 janvier 2016.

[79] Article 1 de l'ordonnance n°2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie, *JORF* n°0111, 13 mai 2021.

[80] Article L.1111-24 du Code de la santé publique.

[81] Anciennement l'ASIP Santé. Nouvelle dénomination consacrée par l'article 1 de l'arrêté du 19 décembre 2019 portant approbation d'un avenant modifiant la convention constitutive du groupement d'intérêt public « Agence nationale des systèmes d'information partagés de santé », *JORF* n°0295, 20 décembre 2019.

[82] Article L.1470-5 du Code de la santé publique.

l'évolution des SIH[83]. En pratique, ce manque d'interopérabilité contraint les professionnels de santé à saisir plusieurs fois les mêmes données. Le risque de survenance d'erreurs est accru par ces multiples opérations. Par manque de temps, les professionnels de santé sont davantage amenés à baisser leur vigilance et commettre des erreurs fragilisant la sécurité des SIH. De plus, ces difficultés d'interopérabilité sont exacerbées par l'hyperspécialisation des logiciels. En effet, du fait de la spécificité des pratiques médicales, les professionnels souhaitent davantage de logiciels en adéquation avec leurs pratiques. Cette multiplication des logiciels ne contribue en rien au renforcement de l'interopérabilité entre les applications. Au delà de ces difficultés, le morcellement est accentué par des pratiques numériques à risque.

### B) … à l'accentuation des fragilités numériques par des pratiques inadéquates

Les SIH sont fragilisés par des pratiques numériques inadéquates. Avec les confinements et l'incitation au recours au télétravail pour éviter la propagation du virus de la Covid-19, selon Guillaume Poupard, le télétravail a pu ouvrir des brèches dans les SI[84]. Ces brèches peuvent s'expliquer par un déploiement dans l'urgence, sans connaissance des minimas des mesures de sécurité. En conséquence, le manque de vigilance, l'utilisation d'outils informatiques non protégés par des antivirus ou la connexion à un réseau non sécurisé ont pu être des facteurs générateurs de failles. Par ailleurs, certains EPS ont fait l'acquisition d'outils informatiques pour les professionnels en télétravail. A contrario, certains professionnels, par manque de moyens financiers de l'EPS, ont été contraints d'utiliser leurs outils informatiques personnels. Ces pratiques ont nettement augmenté les risques de vulnérabilité. Par exemple, les risques de contamination ont pu être exacerbés par l'utilisation de l'ordinateur personnel pour aller sur des sites non sécurisés. De même, le réseau sans fil des domiciles des professionnels est bien souvent peu sécurisé. Ces réseaux sans fil sont plus vulnérables surtout en l'absence de mot de passe, ou d'une technologie de chiffrement WEP. Ces pratiques professionnelles démontrent à quel point chacun a un rôle dans la sécurité numérique. Chaque utilisateur d'un outil informatique professionnel doit être conscient de l'impact de son comportement et des risques associés. Par conséquent, en dehors des failles organisationnelles, les versants humain et réglementaire ne doivent pas être négligés.

---

[83] *La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer*, Cour des Comptes, Rapport sur l'Application des Lois de Financement de la Sécurité Sociale (RALFSS) 2016, page 349.

[84] BERKAOUI (Héléna), *Cyberattaque : « Il y a une explosion de la grande criminalité », rapporte le directeur de l'Anssi*, Public Sénat, 4 novembre 2020.

## Section II : Les failles réglementaires et humaines des EPS, sources de multiples vulnérabilités numériques

Les cyberattaques mettent en exergue des lacunes réglementaires liées aux difficultés d'application des textes en vigueur (Paragraphe I), et cette menace est accentuée par l'ignorance des bons réflexes à adopter par les utilisateurs du SIH (Paragraphe II).

### Paragraphe I : La difficile application des textes en vigueur

Des défaillances réglementaires existent du fait du retard dans l'application des textes et de par le caractère récent de ces textes. Ces défaillances sont, en autre, exacerbées par la mise en place des Groupements Hospitaliers de Territoire (A) et l'application du RGPD (B).

#### A) De la déstabilisation de la gouvernance hospitalière par la création des Groupements Hospitaliers de Territoire…

La création des Groupements Hospitaliers de Territoire (GHT) a déstabilisé les EPS. Leur mise en place obligatoire depuis 2016[85] a bouleversé la gouvernance hospitalière en imposant une logique de groupe à l'échelle des territoires. Cette nouvelle organisation a été instaurée dans une perspective d'approfondissement de la restructuration de l'hospitalisation publique autour d'un projet médical commun et de la mutualisation de certaines fonctions transversales[86]. Le caractère coercitif de la restructuration des EPS en GHT a conduit à une fusion d'ampleur. Cette fusion a impliqué une réflexion sur la sécurité du SI. A terme, les établissements membres du GHT s'interconnectent de manière plus ou moins forte avec le SI de l'établissement support. Cette fusion sur le long terme ne peut être faite instantanément. Sans adjonction de moyens financiers ou humains, fusionner un SI en cinq ans sur des périmètres fonctionnels aussi vastes est absolument impossible[87]. Ces difficultés de réorganisation sont soulignées par Vincent Trely, Président et fondateur de l'Association Pour la Sécurité des Systèmes d'Information en Santé (APSSIS), lors de ses visites de 56 hôpitaux en 2017. Les équipes étaient en plein mouvement de réorganisation et de repositionnement à

[85] Loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022, 27 janvier 2016.

[86] SAISON (Johanne) avec la collaboration de MONTERO (Antoine), *Droit hospitalier*, Fonction publique Hospitalière, 4ème édition, 2019, page 198.

[87] CARTAU (Cédric), « Chapitre 8. Le cas des GHT, La sécurité du système d'information des établissements de santé », *Presses de l'EHESP*, 2018, page 275.

l'échelle du territoire[88]. La mutualisation de l'informatique des GHT, ajoutée à la succession des impératifs réglementaires depuis les années 2000, engendre une panique sur le terrain. Les équipes comprennent les enjeux de la réglementation mais sont dépassées par les sollicitations réglementaires. De plus, cette mutualisation des SI est mise à mal par la fréquente concurrence entre les établissements au sein du GHT. Signaler des problèmes numériques auprès de l'établissement support est bien souvent perçu comme un aveu de faiblesse. Cette réticence à demander des conseils et cette rivalité inter-établissements exacerbent alors la difficile restructuration. En conséquence de cela, la mise en oeuvre de la restructuration des établissements au sein de GHT est l'une des défaillances réglementaires fragilisant les SIH. Une autre défaillance réglementaire se révèle être l'application contraignante du RGPD.

## B) … à l'application contraignante du RGPD

Le RGPD, depuis le 25 mai 2018, a renforcé la protection des données personnelles de santé en définissant pour la première fois la notion de *« données concernant la santé »*[89]. De plus, le règlement a confié la mise en oeuvre de mesures techniques et organisationnelles à des responsables de traitement[90]. Ces mesures tendent vers un juste équilibre entre les intérêts des professionnels de santé et les droits fondamentaux des patients[91]. Cependant, son application a nécessité un temps d'adaptation et une vulgarisation des termes. Par ailleurs, l'application a été compliquée par le manque de moyens autant qu'humains que financiers, et les contraintes d'objectifs ont empêché d'appliquer le droit correctement. L'application des textes, entre 2016 et 2018, selon les acteurs, n'a pas été suffisamment anticipée. Cette application réglementaire reste encore aujourd'hui un défi du fait de l'ampleur des SIH, de la complexité des textes et de l'appropriation parfois difficile par les professionnels non juristes. Les application complexes des textes en vigueur, autant pour la mise en place des GHT que du RGPD, constituent des failles réglementaires fragilisant les SIH. Cette fragilité numérique est exacerbée par l'ignorance des bonnes pratiques par les utilisateurs du SIH.

---

[88] *GHT, RGPD et cybersécurité: les informaticiens hospitaliers "débordés" par le réglementaire,* TIC santé, 24 janvier 2018.

[89] Article 4 du RGPD - *Définitions* : *« […] les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne […] ».*

[90] LAMI (Arnaud) et VIOUJAS (Vincent), *Droit Hospitalier*, 2ème édition, 2020, page 330.

[91] KERMARREC (Jean-Michel), « La judiciarisation de l'usage numérique en santé…un risque émergent », *Revue Droit et Santé n°88*, mars 2019, page 238.

## <u>Paragraphe II</u> : L'ignorance des bonnes pratiques par les utilisateurs des SIH

Les utilisateurs des SIH adoptent des comportements à risque (A), bien souvent liés à un manque de formations (B).

### A) Des utilisateurs aux comportements à risque…

80% des risques numériques proviennent de l'utilisateur de l'outil informatique et 20% seraient liés à des failles du système[92]. Les utilisateurs du SIH, de par leur comportement, peuvent alors être à l'origine de gestes, semblant anodins, mais qui facilitent une intrusion malveillante. Par exemple, l'infection d'un poste peut se faire via l'introduction d'une clé USB inconnue, le téléchargement d'un fichier, l'ouverture d'un mail ou d'un lien. Un simple clic peut infecter le poste de travail et faire entrer un logiciel dit *trojan*. Ce terme fait référence à l'épisode du Cheval de Troie dans la mythologie grecque. C'est une forme de virus spécifique qui a pour objectif de créer une porte dite *backdoor* permettant un accès au poste de travail[93]. A partir de l'ouverture de cette porte, quelques jours plus tard, un autre logiciel malveillant peut infecter le poste, chiffrer les données et bloquer les accès à l'utilisateur. C'est par cette technique, communément nommée sous l'appellation de rançongiciel, que divers EPS français ont été paralysés. Les utilisateurs du SIH font donc preuve de comportements à risque qui fragilisent la sécurité numérique des EPS. Ces comportements proviennent, en partie, d'un manque de formations.

### B) … en manque de formations

Le secteur de la santé est l'un des secteurs de l'économie les moins digitalisés. Ce manque de digitalisation s'explique en partie par des lacunes en matière de formations[94]. Sur tout le cursus de médecine, seulement une formation très brève en informatique est effectuée. Des formations plus approfondies et adaptées peuvent être prodiguées une fois le professionnel en poste. Cependant, la dispensation de formations au sein des EPS est plutôt récente et dépend des EPS selon leurs moyens. En effet, les formations ont bien souvent un

---

[92] RAIMONDO (Laurane), *La protection des données personnelles, 100 Questions/Réponses, Pour comprendre et mieux se protéger*, janvier 2021, page 102.

[93] « C'est quoi un Trojan et comment s'en protéger ? », *ML/ACTU,* 9 novembre 2020.

[94] *E-santé : augmentons la dose !*, Institut Montaigne, Rapport Juin 2020, page 13.

coût que les EPS ne peuvent se permettre. Le manque de formations est accentué par le *turn over* selon les zones géographiques. Les zones peu attractives où les personnes viennent et repartent rapidement, n'ont pas forcément l'opportunité de former et sensibiliser comme il se doit les utilisateurs du SIH. Les utilisateurs du SIH se retrouvent alors bien souvent formés et sensibilisés sur le terrain lors de la survenance des cyberattaques.

En conséquence, les cyberattaques révèlent des failles organisationnelles, humaines mais également réglementaires. Les failles sont multidimensionnelles tout comme les acteurs impactés par les cyberattaques. Les atteintes à la sécurité numérique des SIH impactent à tous les échelons : de l'usager à l'ensemble du système de santé français.

# Titre II : L'impact des cyberattaques à tous les échelons : de l'usager à l'ensemble du système de santé français

L'évolution de NTIC depuis les années 1980 modifie inexorablement l'environnement stratégique et la sécurité des données personnelles concernant la santé. Ces bouleversements engendrés sont d'autant plus importants avec la montée en puissance des périls dans le cyberespace. Ces périls accentuent, à tous les échelons, le risque d'atteinte à la sécurité informatique des EPS, et à la sécurité au sens strict[95]. Selon un rapport de l'Agence des Systèmes d'Information Partagées de santé (ASIP Santé) et du Haut Fonctionnaire de Défense et de Sécurité (HFDS)[96], 478 incidents ont été référencés en 2018. Parmi ces incidents, 88% proviennent d'établissements de santé, et 46% des incidents ont contraint ces établissements à instaurer un fonctionnement dégradé du système de prise en charge des patients. Ce fonctionnement dégradé, engendré par la survenance d'incidents, est conforté par un autre rapport de huit analystes sur la base de 490 attaques[97]. Ce rapport dresse un bilan alarmant sur l'augmentation des incidents graves en terme de santé publique. Ces impacts sur la santé publique s'expliquent en partie par la paralysie des services d'urgences et les risques vitaux encourus par les patients. De ce fait, lors de la survenance d'une cyberattaque, les conséquences s'étendent de l'usager (Chapitre I) au système de santé français (Chapitre II).

## Chapitre I : L'usager du système de santé, première victime

L'usager du système de santé se révèle être la première victime. En cas de captation des données personnelles, le droit au respect de la vie privée de l'usager est atteint (Section I). Cette captation de données exacerbe la défiance des usagers envers le système de santé entraînant un renoncement aux soins pouvant se révéler fatal (Section II).

### Section I : L'atteinte au droit au respect de la vie privée

Chaque patient a le droit de refuser à ce que ses informations médicales soient diffusées (Paragraphe I). D'autant plus, que la divulgation de ces données peut impacter la vie personnelle et professionnelle de la personne concernée (Paragraphe II).

[95] GAUTIER (Louis), « Cyber : les enjeux pour la défense et la sécurité des Français », *Politique étrangère 2018/2*, page 31.

[96] *Structures de santé : pourquoi déclarer ses incidents SI ? ACSS, 18 mois après, HIT 2019,* ASIP santé et Haut Fonctionnaire de défense et de sécurité (HFDS), 22 mai 2019, page 11.

[97] *Cyberthreat Handbook*, Thales et Verint, octobre 2019.

## <u>Paragraphe I</u> : Le droit de chaque patient de refuser la divulgation de ses données personnelles de santé

Chaque patient a le droit de décider des destinataires des informations médicales le concernant (A). Ce droit est protégé par le RGPD et les juges (B).

### A) Un droit de décision sur les destinataires des informations médicales…

Depuis 2002[98], un patient a le droit de refuser d'être informé de son état de santé[99]. Il peut être tenu dans l'ignorance d'un diagnostic ou d'un pronostic, sauf en cas de risque de transmission. Concernant l'information médicale aux proches, une seule dérogation est prévue : en cas de diagnostic ou de pronostic graves[100]. La famille, les proches ou la personne de confiance peuvent recevoir les informations nécessaires destinées à permettre d'apporter un soutien direct au patient. Cette délivrance d'informations ne se fait qu'en absence d'opposition de la part de la personne concernée. De ce fait, un patient a le droit de refuser à ce que son état de santé soit révélé à sa famille ou ses proches. Le patient est acteur de sa santé. Ce droit de refus est renforcé par le respect du secret professionnel par tout professionnel de santé. Ce secret couvre tout ce qui est venu à la connaissance du professionnel de santé dans l'exercice de sa profession. Le principe du secret professionnel est codifié dans le CSP[101] et a un caractère général et absolu[102]. En cas de divulgation de données personnelles relatives à l'information médicale, sans l'accord du patient, le patient se trouve alors lésé dans ses droits. Ce droit est d'autant plus important qu'il est protégé par le RGPD et affirmé maintes fois par les juges.

### B) … protégé par le RGPD et les juges

Les données personnelles concernant la santé, dites « *sensibles* » sont protégées par le RGPD[103]. Le préambule du RGPD énonce le respect de tous les droits fondamentaux, ainsi

---

98 Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, *JORF*, 5 mars 2002.

99 Article L.1111-2 du Code de la santé publique.

100 Article L.1110-4 V. du Code de la santé publique.

101 Article L.1110-4 I. du Code de la santé publique.

102 Arrêts de la Chambre Criminelle de la Cour de Cassation (Watelet du 19 décembre 1885 et Degraene du 8 mai 1947) et du Conseil d'Etat (Deve du 12 avril 1957).

103 Article 9 du RGPD - *Traitement portant sur des catégories particulières de données à caractère personnel.*

que des libertés et principes reconnus par la Charte[104] dont le respect de la vie privée et familiale. De plus, les données de santé recueillies dans le cadre des soins ne peuvent être utilisées à d'autres fins que si le patient y consent ou si la loi l'autorise[105]. Néanmoins, le traitement des données personnelles suscite des risques pour les droits fondamentaux. Pour endiguer ces risques, le Conseil de l'Europe base toutes ses décisions sur l'article 8 de la CEDH[106]. Cet article relatif au droit au respect de la vie privée et familiale est le fondement de toute législation née à propos de la protection des données personnelles. Sur la base de cet article, des droits comme le droit à l'oubli ont été consacrés. La Cour Européenne des Droits de l'Homme a également considéré que les informations relatives à la santé d'une personne constituent un élément important de sa vie privée[107].

Par conséquent, chaque patient a le droit de refuser la divulgation de ses données personnelles de santé. Ce droit est d'autant plus important que la divulgation de ces données peut avoir un impact sur la vie personnelle et professionnelle de la personne concernée.

## <u>Paragraphe II</u> : L'impact de la divulgation des données personnelles sur la vie personnelle et professionnelle

La divulgation de données personnelles de santé amène à une prise de connaissance non souhaitée (A) et sur la base de ces données, les personnes concernées peuvent faire l'objet de chantages individuels (B).

### A) D'une prise de connaissance non souhaitée…

La divulgation de ces données sensibles porte atteinte au droit au respect de la vie privée des patients. La révélation d'informations médicales peut effectivement impacter la vie personnelle et professionnelle de la personne concernée. Ces données n'étaient pas forcément destinées à être divulguées. Les familles et proches peuvent être mis au courant ainsi que les employeurs voire les assureurs. Une fois que l'Assurance a pris connaissance des données, la personne concernée peut avoir des difficultés à contracter un prêt ou ses primes peuvent être

---

[104] Article 7 de la Charte des droits fondamentaux de l'Union Européenne, 18 décembre 2000, Journal Officiel des Communautés européennes 2000/C 364/01.

[105] Article 458 du Code Pénal.

[106] Convention Européenne des Droits de l'Homme, aussi appelée Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Conseil de l'Europe, 1950.

[107] Yvonne Chave née Jullien c. France, 1991, §75.

majorées. La prise en compte des informations médicales est illégale mais possible. De plus, la prise de connaissances de telles informations médicaux peut explicitement, ou implicitement incitée un employeur à embaucher ou pas. Par exemple, si un employeur prend connaissance de problèmes d'alcoolisme, il pourrait être réticent à employer cette personne dans une démarche de productivité ou pour éviter de potentiels accidents du travail (conduite d'un véhicule, chutes, blessures). De même, les banques refusent actuellement des prêts au motif de critères de santé non compatibles avec un remboursement sur le long terme. Des prises de connaissances sur des informations médicales plus précises pourraient alors compromettre davantage les possibilités d'obtention d'un prêt. Enfin, la prise de connaissance d'informations médicales peut aboutir à un refus de visas pour la personne concernée selon les pays. Selon un rapport de la Cellule Internationale de réflexion sur les restrictions au voyage liées au VIH, 59 pays, territoires et zones refusent l'entrée, le séjour et la résidence aux personnes séropositives[108]. En effet, des pays comme les Etats-Unis, la Russie ou la Thailande conditionnent l'obtention d'un permis de travail à un examen sérologique négatif.

La divulgation d'informations relatives à l'état de santé d'une personne peut donc avoir des conséquences dévastatrices sur la vie privée et familiale de la personne concernée et sur sa situation sociale et professionnelle[109]. La divulgation de telles informations peut aboutir à une discrimination autant dans la vie professionnelle que personnelle, et donc un risque d'exclusion. Au delà de cette prise de connaissance non souhaitée, les données personnelles concernant la santé de l'usager peuvent être une occasion pour les cybercriminels ou les personnes ayant récupéré les données, de faire du chantage individuel.

## B) … à des tentatives de chantage individuel

Suite aux cyberattaques, sur la base des données personnelles de santé récupérées, les usagers peuvent faire l'objet de demandes de rançons individuelles. Ces demandes de rançons ne sont pas forcément rendues publiques. L'un des seuls exemples médiatisés est en Finlande. En octobre 2020, une clinique psychiatrique a été victime d'une cyberattaque[110]. En plus de demander une rançon à la clinique, le pirate informatique a demandé des rançons de deux cent euros en bitcoins sous 24h à des dizaines de patients. En l'absence de paiement de ces

[108] *L'impact des restrictions à l'entrée, au séjour et à la résidence liées au VIH : témoignages personnels*, Programme Commun des Nations Unies sur le VIH/Sida, ONUSIDA, mai 2009, page 3.

[109] Arrêts CEDH : Z c. Finlande, 1997, § 96 ; C.C. c. Espagne, 2009, § 33 ; P. et S. c. Pologne, 2012, § 128 ; Avilkina et autres c. Russie, 2013, § 45 ; Y. c. Turquie (déc.), 2015, § 65.

[110] *Finlande : une cyberattaque contre un hôpital psychiatrique choque le pays*, 21 décembre 2020, 20minutes.fr.

rançons, le cybercriminel menaçait de diffuser les données personnelles de santé. Par conséquent, en plus de voir leur état de santé dévoilé à des tiers, l'usager subit une pression financière. Chaque patient voit donc son droit au respect de sa vie privée atteint en cas de cyberattaques. Cette atteinte a de fortes chances d'accentuer la défiance des usagers envers le système de santé français. Cette défiance est préjudiciable puisqu'elle peut engendrer un accroissement du nombre de renoncements aux soins.

---

## Section II : L'accentuation de la défiance, cause de renoncement aux soins

L'obtention illicite et la divulgation de données personnelles génèrent un contexte anxiogène où la défiance et l'ambiance de complotisme atteignent leur paroxysme. Les patients sont alors inquiets (Paragraphe I) et en viennent à renoncer aux soins par peur des conséquences d'une cyberattaque (Paragraphe II).

### Paragraphe I : L'inquiétude des patients

La défiance est intensifiée par la surmédiatisation des cyberattaques (A) et pour autant, ces risques liés aux cyberattaques sont perçus différemment selon les générations (B).

#### A) L'intensification de la défiance par la surmédiatisation des cyberattaques…

Dax, Villefranche sur Saône, Albertville-Moûtiers… et encore tant d'autres d'EPS qui sont passés en boucle sur les diverses chaînes télévisées ces derniers mois dans le cadre de cyberattaques. Dans un monde hyperconnecté où tout est transmis, les cyberattaques sont médiatisées en un clic. Néanmoins, dans un climat anti vax, de défiance entre le Gouvernement et envers la qualité du système de santé, la médiatisation de ces cyberattaques ne font qu'accroître la défiance des usagers du système de santé. Le patient veut être informé de tout. Il veut être acteur de santé, être informé de ses droits et des risques. Dans la balance bénéfices-risques, en plus de la peur d'apprendre un diagnostic grave, les usagers du système de santé pourraient exprimer des réticences à aller se faire soigner dans un EPS dont la sécurité numérique est questionnable.

La défiance envers les SIH est intensifiée par la surmédiatisation des cyberattaques avec, pour autant, une perception différente selon les générations.

### B) … perçue différemment selon les générations

Les cyberattaques font l'objet d'une perception différente selon les générations. Pour certaines, souvent chez les jeunes, ces cyberattaques provoquent de l'indifférence et pour d'autres, ces atteintes à la sécurité numérique des EPS provoquent de la paranoïa. Cette mentalité différente selon l'âge pourrait s'expliquer par une évolution sociétale qui tend vers une hyperconnexion des utilisateurs des outils numériques. Un utilisateur hyperconnecté pourrait faire preuve d'individualisme sur l'appréciation économique-sanitaire de la santé, et ne pas considérer la divulgation de ses données comme grave. La défiance est illustrée par la mise en place d'applications collectant des données comme StopCovid. Au 5 octobre 2020, avant le lancement de la mise à jour TousAntiCovid, l'application a été installée 2 640 805 fois depuis son lancement en juin 2020, et a été désinstallée 1 138 600 fois et seulement 7 969 personnes se sont déclarées comme étant positives[111]. Ce faible nombre de téléchargements met en exergue la méfiance des usagers envers le recueil de leurs données personnelles. Les patients se révèlent alors inquiets et anxieux les amenant alors à renoncer aux soins par peur des conséquences en cas de cyberattaques de l'EPS.

## <u>Paragraphe II</u> : Le problématique renoncement aux soins

La défiance persistante des usagers du système de santé français (A) amène à un renoncement aux soins (B).

### A) Une défiance persistante…

Les usagers peuvent exprimer une peur du numérique et donc d'une divulgation inopinée de leurs informations personnelles. De manière plus factuelle, l'état de la confiance des Français dans les usages numériques est analysé depuis dix ans par l'Association pour le Commerce et les Services En Ligne (ACSEL). L'édition la plus récente du baromètre publiée début 2021[112] démontre d'un usage numérique croissant, notamment expliqué par le contexte de crise sanitaire. Pendant la crise, l'accélération des usages a renforcé la confiance dans le

---

[111] *Rapport au nom de la commission d'enquête pour l'évaluation des politiques publiques face aux grandes pandémies à la lumière de la crise sanitaire de la Covid-19 et de sa gestion*, remis à M.le Président du Sénat le 8 décembre 2020, Session ordinaire de 2020-2021.

[112] *Baromètre de la confiance des Français dans le numérique*, synthèse des résultats, 8ème édition, ACSEL, février 2021.

numérique de plus de 28% des personnes interrogées. 89% des Français auraient donc confiance dans le numérique. Cette confiance globale envers le numérique a atteint son meilleur niveau depuis 2015. En dépit de ce regain de confiance, des craintes de la part des utilisateurs persistent. En autre, les Français sont toujours méfiants quant à l'usage de leurs données personnelles. Par exemple, 14% des utilisateurs expriment une peur du manque de confidentialité des échanges, 13% témoignent d'une crainte liée à la sécurité des données de santé (peur d'un piratage de leurs données), et 10% craignent que leurs données soient utilisées à des fins commerciales. De plus, dans un monde hyperconnecté où le patient d'un EPS est au coeur de la santé numérique, l'usager démontre d'une peur de mal se faire soigner par un EPS pouvant être paralysé à tout moment. Cette défiance persistante entraîne inexorablement un renoncement aux soins.

### B) … amenant à un renoncement aux soins

En France, le renoncement aux soins représente 25% selon un baromètre du renoncement aux soins réalisé en 2019[113]. De manière plus précise, aucune étude n'a encore été faite à propos d'un renoncement aux soins engendré par la réticence à se faire soigner par un hôpital public défaillant informatiquement. Cependant, plusieurs études font état d'une réticence des Français envers l'utilisation de technologies numériques en santé. En effet, l'utilisation croissante du numérique dans le monde sanitaire et social, ainsi que la dématérialisation renforcée des démarches administratives sont des sources d'inquiétudes largement partagées. Cette dématérialisation des échanges entre l'administration et le public génère entre autre du renoncement et du non-recours[114]. La défiance a alors des conséquences sociétales, psychologiques et sanitaires sur le système de santé français.

L'usager du système de santé est, certes, la première victime en cas de cyberattaques. Cependant, l'EPS ciblé est un pilier dans le fonctionnement du système de santé français donc toute cyberattaque le visant impacte inexorablement de multiples aspects de son fonctionnement.

---

[113] *Baromètre du renoncement aux soins (BRS),* Observatoire des non-recours aux droits et services (ODENORE), en partenariat avec la CNAM et la CPAM du Gard, 2019.

[114] *Renoncement et accès aux soins. De la recherche à l'action*, Cinq années de collaboration entre l'Assurance Maladie et l'Observatoire des non-recours aux droits et services (Odenore), actes synthétiques du colloque des 6 et 7 juin 2019, Paris, Cité des Sciences et de l'Industrie, 2020, page 30.

## Chapitre II : L'établissement public de santé, pilier dans le fonctionnement du système de santé français

En cas de cyberattaque, le personnel, paralysé informatiquement, ne peut plus accéder aux dossiers patients faisant courir un risque mortel aux patients hospitalisés ou qui risquent de l'être. Les cyberattaques à l'encontre du secteur public hospitalier mettent en péril alors la continuité des soins, essentielle à la protection des vies humaines (Section I) et entraîne, de surcroît, des conséquences financières colossales (Section II).

---

## Section I : La mise en péril de la continuité des soins, essentielle à la protection des vies humaines

Cette continuité des soins est compromise puisque des données essentielles pour une prise en charge de qualité sont indisponibles informatiquement (Paragraphe I) et le fonctionnement de l'EPS s'avère être paralysé (Paragraphe II).

### Paragraphe I : L'indisponibilité de données essentielles à une prise en charge de qualité

Une cyberattaque engendre une perturbation de l'accès aux données personnelles de santé (A) qui impacte inexorablement la qualité de la prise en charge (B).

#### A) Une perturbation à l'accès aux données personnelles de santé…

Pour illustrer la perte de données occasionnée, en juillet 2018, un Ehpad Nantais de 80 lits a été victime d'une attaque d'un cryptolocker[115]. Entre deux et quatre mois de données ont été perdus. Ces données concernaient des fichiers de travails présents sur le serveur, la facturation des résidents, les données comptables et salariales[116]. Les défaillances numériques des hôpitaux exposent donc les données personnelles des patients. Les cyberattaques peuvent aussi conduire à une paralysie de l'EPS. A titre d'exemple, le CH d'Albertville-Moûtiers, a fait l'objet d'une cyberattaque dans la nuit du 21 décembre 2020. Un certain nombre d'équipements, de serveurs, de logiciels et une partie du réseau informatique ont été indisponibles pendant plusieurs semaines. L'atteinte numérique d'un SIH perturbe l'accès aux données personnelles de santé impactant alors la qualité de la prise en charge du patient.

---

[115] Logiciel malveillant de type rançongiciel ciblant les disques durs, les clés USB et les fichiers synchronisés avec le Cloud.

[116] « Cyber-attaque en ESSMS : la menace sous-estimée », *Revue Actualités Sociales Hebdomadaires (ASH),* n° 3093, 18 janvier 2019.

### B) … impactant la qualité de la prise en charge

Lors ou suite à une cyberattaque à l'encontre d'un EPS, la prise en charge d'un patient peut être impactée, au point de favoriser la survenance d'erreurs médicales. En effet, l'atteinte des SIH peut engendrer une indisponibilité numérique des données, ou des falsifications de résultats médicaux. Or, les données personnelles sont essentielles au bon fonctionnement des établissements de santé (antécédents, incompatibilités médicamenteuses), et donc à la continuité des soins[117]. De manière plus grave, une cyberattaque peut impliquer le contrôle à distance des ascenseurs, des défibrillateurs, des pompes à insuline, de robots chirurgicaux ou d'autres dispositifs médicaux connectés. La santé des usagers du système de santé est alors inexorablement mise en danger. En plus de cette inaccessibilité informatique, le fonctionnement de l'EPS se retrouve paralysé, et tente de réagir avec les outils à disposition.

## <u>Paragraphe II</u> : La paralysie du fonctionnement de l'EPS, aggravée par les outils lacunaires à disposition

Lors d'une cyberattaque, l'EPS active des plans de continuité de gestion de crise (A) et pour pallier à la perte de chance, l'EPS active l'assurance contractée en amont (B).

### A) De l'activation de plans de continuité de gestion de crise…

En cas de crise, des plans de continuité sont prévus. Par exemple, lors de la cyberattaque envers le CH d'Albertville-Moûtiers, les conséquences ont été limitées par le contexte de maîtrise de la crise sanitaire, la fermeture des stations de skis, l'aide des établissements membres du GHT et surtout l'existence de plans de continuité d'activité. Au niveau national, une démarche sur la continuité de l'activité a été entreprise notamment suite à des crises sanitaires comme la canicule de 2003. Les plans blancs ont aussi aidé et permis d'intervenir rapidement avec des réunions. Néanmoins, les procédures de continuité d'activité ne sont pas adaptées à ce type de tensions. Elles sont faites pour des interruptions d'activités courtes et non de plusieurs semaines voire mois. La continuité d'activité se doit d'être restructurée et le premier objectif est de se focaliser sur le soin. Cette continuité d'activité est d'autant plus importante que la santé fait partie des douze secteurs retenus dont les activités sont stratégiques. La liste précise est secrète mais dans la santé, sont englobés les EPS. Ce

[117] DOUVILLE (Thibault), *L'émergence d'un droit commun de la cybersécurité*, Recueil Dalloz 2017, page 2255.

caractère stratégique vaut aux EPS d'être considérés comme des opérateurs d'importance vitale (OIV)[118]. Par définition, un OIV est une infrastructure vitale gérée par l'informatique, pouvant générer des dommages corporels importants. Par conséquence, les OIV de la santé doivent faire l'objet de mesures spécifiques de protection contre les actes de malveillance dont les cyberattaques. Les OIV existent depuis la mise en place en 2005 d'un dispositif interministériel de sécurité des activités d'importance vitale[119]. Piloté par le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), ce dispositif a été complété par un décret en 2006[120] et par un guide pour réaliser un plan de continuité ou de reprise d'activité en 2013[121]. Le but est de protéger les OIV dont le fonctionnement et la continuité d'activité sont indispensables à la Nation[122]. Cette protection implique l'analyse des risques en quatre étapes : l'étude du contexte et des spécificités du secteur, l'identification des scénarios de menaces, l'évaluation des risques et enfin, la détermination d'un dispositif de sécurité. De cette analyse, doit être créée une matrice de risques pour déterminer les objectifs de sécurité à atteindre pour obtenir un risque identifié à un niveau acceptable[123]. La création d'un plan de continuité spécifique aux cyberattaques est indispensable pour permettre, selon un mode dégradé, d'assurer la disponibilité des données quelque soient les circonstances[124]. En plus de l'activation de tels plans de continuité de gestion de crise, l'EPS est confronté à une perte de chance, faisant l'objet d'assurances spécifiques émergentes.

### B) … à l'émergence timide d'une anticipation assurancielle de la perte de chance

Les EPS anticipent via les assurances, notamment pour permettre une indemnisation et éviter le contentieux. En fonction des termes du contrat, le risque cyber peut être pris en charge et la victime pourra être dédommagée des dépenses engagées. Ces assurances sont importantes pour anticiper la perte de chance. L'une des plus grosses assurances pour les EPS est la Société Hospitalière d'Assurance Mutuelle dite SHAM. Aujourd'hui, des contrats

[118] Article R.1332-1 du Code de la Défense.

[119] Loi n°2005-1550 du 12 décembre 2005 modifiant diverses dispositions relatives à la défense (1), *JORF* n°289, 13 décembre 2005.

[120] Décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale, *JORF* n°47, 24 février 2006.

[121] *Guide pour réaliser un plan de continuité d'activité*, SGDSN, édition 2013.

[122] QUEMENER (Myriam), « Cybersécurité et protection des données de santé », *Dalloz IP/IT*, 20 mai 2020, page 304.

[123] *Id.*

[124] LAMI (Arnaud) et VIOUJAS (Vincent), *Droit Hospitalier*, 2ème édition, 2020, page 329.

d'assurance cyber permettent d'accompagner les EPS victimes de cyberattaques. En cas de sinistre, une assistance juridique et une couverture financière de préjudice (matériel, immatériel) peuvent alors leur être proposées. Ce marché assuranciel reste encore lacunaire et son développement se poursuit, particulièrement en matière jurisprudentielle concernant l'activation ou non des clauses d'exclusion[125]. La continuité des soins est perturbée lors de la survenance de cyberattaques mais ces dernières ont aussi des conséquences financières.

## Section II : Les actes de cybermalveillance, fléau économique pour les établissements publics de santé

Une cyberattaque engendre des coûts (Paragraphe I) et des sanctions financières peuvent être prononcées à l'encontre de l'EPS (Paragraphe II).

### Paragraphe I : La génération de coûts par l'acte cybermalveillant

Attaquer informatiquement un SIH génère des coûts liés à la perte de données et d'activité (A) et des coûts de réinstallation et de remplacement des outils informatiques (B).

#### A) Des coûts liés à la perte de données et d'activité…

Une cyberattaque a des conséquences financières sur le budget notamment à cause des coûts liés aux blocages des outils informatiques et aux vols de données. Par exemple, le piratage du standard d'un CH a généré une surfacturation de téléphonie de l'ordre de 40 000 euros[126]. De plus, la médiatisation d'une cyberattaque peut entraîner une perte d'attractivité et une perte de confiance des usagers. Or, les EPS fonctionnent sur la base d'une tarification à l'activité. La diminution de la fréquentation peut alors influencer négativement le budget d'un EPS. Pour un établissement de plus de 1 500 lits, une attaque informatique peut amener à des frais pouvant s'élever jusqu'à plusieurs centaines de milliers d'euros[127]. Au delà de ces conséquences financières, ces coûts peuvent être assortis de coûts de réinstallation et de remplacement des outils informatiques infectés.

---

[125] *Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident ?,* guide de bonnes pratiques, ANSSI, août 2020, page 18.

[126] *Mémento à l'usage du directeur d'établissement de santé - Connaître vos risques pour mieux y faire face,* Cybersécurité, édition 2017 - DGOS, page 13.

[127] GOESSAERT (Antoine), « Verso Healthcare mesure et rappelle l'importance de la cybersécurité face aux attaques », Système d'information, 22 avril 2021, *Hospimedia*.

### B) … assortis de coûts de réinstallation et de remplacement des outils informatiques infectés

En quelques secondes, les réseaux informatiques d'un EPS peuvent être anéantis. Leur rétablissement implique bien souvent un remplacement des outils infectés. Le montant exact d'une cyberattaque, au niveau matériel et financier, est difficilement appréciable. Cependant, dans un EPS où la gestion financière est le nerf de la guerre, ces cyberattaques se révèlent être un véritable gouffre financier. D'une autre perspective, selon Mickaël Taine[128], le remplacement du parc informatique peut être perçu comme un investissement bénéfique pour la qualité du service hospitalier, et donc pour la sécurité numérique[129]. En plus de coûts engendrés par les cyberattaques, l'EPS peut faire l'objet de sanctions financières.

## <u>Paragraphe II</u> : Les sanctions financières encourues

Chaque EPS, en tant qu'organisme traitant des données à caractère personnel est tenu d'une obligation générale de sécurité[130]. Suite à une cyberattaque, l'EPS peut donc faire l'objet d'une condamnation de la part de la CNIL (A) et des actions en justice peuvent être initiées par des patients concernés par l'atteinte aux données personnelles de santé (B).

### A) De condamnations par la CNIL…

Lorsqu'un EPS est touché, la peine est double. En plus d'être paralysé informatiquement et de subir des conséquences multidimensionnelles, la CNIL peut faire des audits pour déterminer l'origine des vulnérabilités et vérifier le respect du RGPD. En effet, depuis 2004[131], la CNIL peut contrôler *a posteriori* et a un pouvoir de sanction. Elle constate la présence ou non, de manquements au RGPD et aux réglementations en vigueur en matière de protection des données personnelles. Si la CNIL constate un manquement, alors elle peut mettre en demeure l'EPS ou le sanctionner. Les sanctions applicables prévues par le RGPD[132],

---

[128] Directeur de l'Innovation Numérique et des Systèmes d'Information du GHT des Alpes Maritimes au CHU de Nice.

[129] GOESSAERT (Antoine), « Verso Healthcare mesure et rappelle l'importance de la cybersécurité face aux attaques », Système d'information, 22 avril 2021, *Hospimedia*.

[130] Article 24 du RGPD - *Responsabilité du responsable du traitement.*

[131] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *JORF* n °182, 7 août 2004.

[132] Article 83 du RGPD - *Conditions générales pour imposer des amendes administratives.*

doivent être *« effectives, proportionnées et dissuasives »*. Ces mêmes dispositions prévoit qu'en cas de violations délibérées ou par négligence de plusieurs dispositions du RGPD, l'EPS peut encourir jusqu'à vingt millions d'euros. Jusqu'à lors, aucun établissement public de santé n'a été condamné à une amende aussi importante et les condamnations sont extrêmement rares. Selon la liste des condamnations publiée par la CNIL[133], depuis 2004, deux EPS ont déjà fait l'objet d'avertissements non publics en 2013 et 2014. A titre d'exemple, un avertissement a été donné, le 25 septembre 2014, concernant la gestion des usagers, vis-à-vis de la durée de conservation des données, ainsi que la sécurité et la confidentialité des données. En plus de possibles condamnations de la CNIL, un EPS peut faire l'objet de recours de patients concernés par l'atteinte aux données personnelles.

### B) … à des recours de patients concernés par l'atteinte aux données personnelles

Les patients victimes d'actes de cybermalveillance ont la possibilité de déposer une plainte auprès des services de police et gendarmerie. Ces services se sont adaptés au traitement de tels contentieux[134]. Ces recours démontrent l'importance pour les EPS de souscrire à des assurances spécifiques en matière de cybermalveillance. Cette possibilité de porter plainte est confortée par le RGPD. En effet, un droit à réparation de la part du responsable du traitement ou du sous-traitant est prévu pour toute personne ayant subi un préjudice lié à un manquement aux principes posés par le règlement[135]. Ce même règlement octroie le droit à toute personne victime d'un dommage matériel ou moral issu d'une violation du RGPD, d'introduire un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant[136]. Ce recours ne doit en aucun cas être fait auprès de la CNIL. La CNIL n'est pas compétente pour accorder une indemnisation aux personnes ayant subi un tel dommage[137]. Une plainte doit être déposée auprès des forces de l'ordre et les tribunaux civils peuvent être saisis. Ces tribunaux civils statueront sur l'existence, l'évaluation du préjudice et la potentielle indemnisation de la part de l'EPS.

---

[133] *Les sanctions prononcées par la CNIL*, cnil.fr.

[134] *Confiance numérique, vie privée, données personnelles, cybermalveillance*, Stratégie nationale pour la sécurité du numérique, 16 octobre 2015, page 22.

[135] Article 82 du RGPD - *Droit à réparation et responsabilité*.

[136] Article 79 du RGPD - *Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant.*

[137] *Fuite massive de données de santé : comment savoir si elle vous concerne et que pouvez-vous faire ?*, 1 mars 2021, cnil.fr.

# CONCLUSION TRANSITOIRE

La question à se poser n'est pas la temporalité de la survenance d'une cyberattaque à l'encontre d'un EPS, mais plutôt comment mieux comprendre et anticiper la survenance d'une telle atteinte numérique envers les SIH. Le constat qui peut être établi est que la sécurité numérique des EPS est insuffisante et non maîtrisée. Parallèlement à ce constat, la menace est permanente, avec tous les jours des tentatives à l'encontre des SIH français. Cependant, la santé est un devoir régalien de l'Etat avec une recherche permanente de qualité[138]. En conséquence de cela, une sécurité numérique des EPS parfaite n'est pas possible mais le tout est que cette sécurité numérique tend vers une certaine protection des données personnelles de santé avec le moins de vulnérabilités possibles dans les SIH.

Après avoir exposé les raisons faisant que les EPS sont vulnérables et à quel point les cyberattaques ont de l'impact, il est important de souligner ce qui est fait, ce qui reste à faire, et le fait que ce soit une préoccupation primordiale pour la pérennité des EPS. Une fois la compréhension des vulnérabilités effectuée, il devient alors essentiel d'agir et de mettre en place une cyberrésilience. Une Nation qui veut conserver sa souveraineté doit faire de la sécurité numérique une priorité nationale confirmée.

En conséquence, les cyberattaques témoignent de l'importance de la protection des données personnelles et démontrent de l'urgence d'une stratégie de défense pour renforcer la sécurité numérique des EPS.

---

138 SFEIR (Antoine), « La santé est un devoir régalien de l'Etat, pas un pouvoir », *Tribunes de la Santé,* 2011/4 (n°33), Presses de Science Po, page 99.

# DEUXIÈME PARTIE - Le renforcement de la sécurité numérique des établissements publics de santé : l'urgence d'une stratégie de défense

*« Ce n'est pas à la personne humaine d'être l'esclave de la technique, c'est à elle de servir l'homme »*, affirme René Savatier, professeur de droit civil dans son ouvrage *Les Métamorphoses économiques et sociales du droit civil d'aujourd'hui* (1948)[139]. La technique, sous-entendu les outils du SI, se doit d'être au service de l'homme. Elle se doit d'être une arme au service du système de santé français pour qu'il tend vers la perfection. La technique ne doit en aucun cas devenir un poison altérant le bon fonctionnement des EPS. Cette préoccupation est d'autant plus importante que, selon Guillaume Poupard, les conflits de demain seront numériques. Les attaques informatiques graves à visée terroriste n'existent pas encore[140]. Cependant, dans un monde de plus en plus connecté où les infrastructures d'énergie, de transport, et surtout de santé dépendent du numérique, cette menace terroriste pourrait exister un jour. La recrudescence des cyberattaques, ces derniers mois, à l'encontre des EPS le démontrent. Certes, le système de santé français est plutôt robuste, mais la santé est l'un des piliers fondamentaux de l'Etat. Protéger numériquement le système de santé français apparaît plus que nécessaire. Le numérique peut et doit contribuer à la sauvegarde et à l'amélioration du système de santé français[141]. Pour cela, il semble inéluctable que la France renforce sa capacité de défense dans le cyberspace. La défense, est considérée comme étant la meilleure stratégie en matière de cyberattaques, par Jean-Baptiste Demaison, chargé de mission numérique à l'ANSSI[142]. *« La meilleure défense…c'est la défense ! »*[143]. Tel est l'un des leitmotivs de l'ANSSI. Cette défense implique, à la fois une prévention via une analyse de la menace, des vulnérabilités et de la sécurité des outils numériques, et à la fois une réaction où des acteurs sont présents pour assister l'EPS. Par conséquent, le renforcement de la sécurité numérique des EPS implique nécessairement la mise en place de moyens (Titre I) et un questionnement sur les pratiques (Titre II).

---

[139] CHOPIN (Frédérique), « Cybercriminalité », *Répertoire de droit pénal et de procédure pénale*, janvier 2020, page 1.

[140] BERKAOUI (Héléna), *Cyberattaque : « Il y a une explosion de la grande criminalité », rapporte le directeur de l'Anssi*, Public Sénat, 4 novembre 2020.

[141] ROBIN (Jean-Yves), *L'urgence numérique, Faire de la France un leader de l'e-santé*, 2014, page 26.

[142] *Dans la peau d'un expert en cybersécurité,* Master Geopolitix, 30 août 2018, sur youtube.com (9:12).

[143] « Papiers numériques », *Revue annuelle de l'ANSSI*, édition 2020, page 33.

# <u>Titre I</u> : La mise en place de moyens : une participation à l'efficience de la sécurité numérique des établissements

Les moyens dédiés au numérique ne cessent d'augmenter au fil des programmes gouvernementaux. En dépit de ces programmes, il existe toujours un problème de moyens d'après Vincent Trely, président de l'APSSIS[144]. Ce problème de moyens est un des premiers générateurs de risques. En effet, un dénuement de moyens financiers suffisants conduit à des choix bien souvent restrictifs qui fragilisent la sécurité numérique des EPS. Cette fragilité est mise en exergue par les cyberattaques successives perpétrées sur le territoire national depuis quelques années, qui démontrent l'importance de ne pas faire de concessions en matière de sécurisation numérique des SIH. Pour pallier à ces déficiences, une stratégie cyber a été présentée le 18 février 2021 par l'actuel Président de la République, Emmanuel Macron. Le Gouvernement souhaite renforcer l'accélération de la numérisation des EPS prévue dans le Ségur de la Santé. Parmi l'enveloppe de 2 milliards d'euros d'investissements envisagés, 350 millions sont spécifiquement dédiés au renforcement de la cybersécurité des établissements de santé et médico-sociaux[145]. En dehors de ce financement, le Gouvernement incite les EPS à opter pour une meilleure prise en compte de la cybersécurité. Cette incitation est illustrée par l'absence de soutien étatique si le projet de SI des EPS ne consacre pas une part de 5% à 10% de son budget informatique à la cybersécurité. Ce souhait gouvernemental d'attribuer des moyens financiers plus conséquents dans la cybersécurité des EPS est un atout non négligeable dans l'amélioration de la protection des données personnelles de santé détenues par les EPS. Toujours est-il qu'il convient d'adopter une utilisation convenable des moyens financiers au regard des besoins logistiques via l'actualisation des SIH des EPS (Chapitre I) et au regard des moyens humains (Chapitre II).

## <u>Chapitre I</u> : L'actualisation des systèmes d'information hospitaliers : une étape indispensable vers la cyberprotection

La sécurisation des systèmes d'information hospitaliers (SIH) des EPS implique une consolidation de ces derniers pour relever les défis d'aujourd'hui et de demain (Section I) ainsi qu'une réflexion sur l'hébergement des données personnelles (Section II).

---

144 TRIBAULT (Géraldine), « La santé est presque arrivée au niveau de sécurité auquel elle devrait être », *Hospimedia*, 4 novembre 2020.

145 *Sécurité des réseaux informatiques des établissements de santé : le Gouvernement renforce sa stratégie*, communiqué de presse, 22 février 2021 sur le site du Ministère des Solidarités et de la Santé.

## Section I : Des SIH vulnérables à consolider pour relever les défis d'aujourd'hui et de demain

Le renforcement des SIH des EPS implique l'instauration d'une interopérabilité des applications (Paragraphe I) et un renforcement du virage numérique (Paragraphe II).

### Paragraphe I : L'instauration d'une interopérabilité des applications au sein des SIH

Cette interopérabilité est un objectif gouvernemental (A) et des projets innovants tendent à améliorer cette interopérabilité (B).

#### A) L'interopérabilité, un objectif gouvernemental…

Instaurer une interopérabilité des applications au sein des SIH est un des objectifs présentés par Agnès Buzyn, l'ancienne Ministre chargée des Solidarités et de la Santé, le 25 avril 2019. En effet, parmi les cinq orientations énoncées par une feuille de route intitulée *« Accélérer le virage numérique en santé »,* la deuxième consiste à *« Intensifier la sécurité et l'interopérabilité du numérique en santé »*. Pour mener à bien cette orientation, la Ministre annonçait une généralisation de l'identification numérique issue d'un même référentiel national, le lancement d'une étude sur l'opposabilité des référentiels d'interopérabilité communs et la mise en oeuvre d'un service national de cybersurveillance[146]. Depuis, deux bilans en décembre 2019 et décembre 2020 ont été rendus. Il en ressort que, malgré la crise sanitaire actuelle, des opérations de sensibilisation ont été menées et des groupes ont été animés pour les interfaces SI-DEP[147] et VAC-SI[148], en partenariat avec l'ANS et Interop'Santé. Concernant les référentiels, une uniformisation a bien été effectuée. Désormais, il y a des référentiels internationaux (ISO27017, ISO27018), et d'autres spécifiques à la France (SECNUMCLOUD de l'ANSSI, PGSSI-S de l'ANS). Ce souhait gouvernemental

---

[146] *Feuille de route « Accélérer le virage numérique en santé », Virage numérique*, Agence du Numérique en Santé, sur le site du Ministère des Solidarités et de la Santé.

[147] Système d'Information de Dépistage Populationnel : système de surveillance qui vise au suivi exhaustif de l'ensemble des tests effectués en France dans les laboratoires de ville et dans les laboratoires hospitaliers pour la recherche du SARS-CoV-2 (*Foire aux questions : système d'information de dépistage,* Santé Publique France, 8 décembre 2020, page 1).

[148] Système d'Information Vaccin Covid : application informatique développée par la DSI de l'AP-HP pour la prise de RDV, le suivi, les statistiques de la campagne de vaccination contre la Covid-19 à l'AP-HP (*#1andeCovid à l'AP-HP : SI-DEP et SI-VAC*, sur le site aphp.fr, 19 mars 2021).

d'une interopérabilité des SIH est conforté par la loi du 26 avril 2021[149]. En effet, cette loi modifie l'article L.6132-3 du CSP en rajoutant la notion d'interopérabilité. Au sein d'un GHT, un établissement support désigné par la convention constitutive assure alors, pour le compte des établissements parties, *« la stratégie, l'optimisation et la gestion commune d'un système d'information hospitalier convergent et interopérable ».* De plus, dernièrement, une ordonnance du 12 mai 2021[150] a abrogé les dispositions relatives à l'interopérabilité dans le Code de la santé publique[151] et a crée un Titre VII relatif aux services numériques en santé[152].

Parmi les dispositions créées, un Chapitre est consacré à l'interopérabilité et à la sécurité des services numériques en santé[153]. Il appert alors que les services numériques en santé doivent être conformes aux référentiels d'interopérabilité et de sécurité élaborés par l'Agence du Numérique en Santé (ANS)[154]. Cette conformité est vérifiée dans le cadre d'une procédure d'évaluation et de certification, et conditionne l'attribution de fonds publics[155]. Ainsi, les diverses dispositions évoquées démontrent bien l'objectif gouvernemental d'inscrire l'interopérabilité comme condition *sine qua non* pour les SIH. Cette interopérabilité tente également d'être renforcée via des projets innovants.

### B) … renforcé par des projets innovants d'acteurs privés

L'interopérabilité des SIH, en plus d'être recherchée par le Gouvernement, est aussi un souhait d'acteurs publics et privés. Par exemple, la plateforme Lifen, fondée par Franck Le Ouay, Alexandre Huckert et Etienne Depaulis[156], a reçu le Prix Interopérabilité de l'ANS et de la Délégation Ministérielle au Numérique en Santé (DNS) lors de la première cérémonie des Talents de l'e-santé le 10 décembre 2020. Décerné par Annie Prévot, directrice de l'ANS, cette plateforme a été récompensée pour son action en faveur de l'accélération du numérique en santé. Plus précisément, la plateforme Lifen propose des solutions digitales destinées à

---

[149] Loi n°2021-502 du 26 avril 2021 visant à améliorer le système de santé par la confiance et la simplification, *JORF* n°0099, 27 avril 2021.

[150] Article 1 de l'ordonnance n°2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie, *JORF* n°0111, 13 mai 2021.

[151] Articles L.1110-4-1 et L.1110-4-2 du Code de la santé publique.

[152] Articles L.1470-1 à L.1470-6 du Code de la santé publique.

[153] Chapitre II : Interopérabilité et sécurité des services numériques en santé (articles L.1470-5 à L.1470-6 du Code de la santé publique).

[154] Article L.1470-5 du Code de la santé publique.

[155] Article L.1470-6 du Code de la santé publique.

[156] *Qui sommes-nous ?*, lifen.fr.

l'envoi et l'intégration de documents médicaux. Ces solutions permettent, en autre, une connexion avec le dossier médical partagé (DMP) et les messageries sécurisées de santé (MSSanté)[157]. La recherche d'une interopérabilité des applications au sein des SIH est alors primordiale, tout comme le renforcement du virage numérique des EPS.

## Paragraphe II : Le renforcement du virage numérique des EPS

Ce renforcement du virage numérique implique l'utilisation de logiciels informatiques adéquats (A) et la résolution des vulnérabilités à l'approche du déploiement de la 5G (B).

### A) L'utilisation de technologies pérennes…

Une sécurité numérique implique le renforcement des logiciels informatiques. Par exemple, dans les EPS, les logiciels comme Windows ne sont pas forcément mis à jour et de vieux packs office sont utilisés. En France, le virage numérique a été raté. Cette vulnérabilité en matière de logiciels est, sans surprise, exploitée par les cyberattaquants. Selon l'éditeur de solutions anti-virus Symantec, un des groupes hackers les plus actifs dans la e-santé, prénommé *OrangeWorm* exploite les failles de sécurité du système d'exploitation Windows XP. Pour cela, il installe un logiciel malveillant nommé *Kwanpirs* sur les ordinateurs des EPS. Ensuite, ce logiciel permet d'espionner l'activité des supports médicaux numériques en toute impunité[158]. De plus, pour limiter les vulnérabilités des SIH, l'utilisation de technologies pérennes dont la maintenance est assurée est indispensable. Renforcer les logiciels informatiques est d'autant plus important avec l'arrivée de la 5G.

### B) … à l'approche du déploiement du réseau 5G

L'utilisation d'un réseau sécurisé est un des socles de sécurité techniques. En effet, une connexion Wi-fi sécurisée doit être privilégiée par les utilisateurs du SIH avec notamment la technologie WPA2-PSK et un mot de passe fort. Ces vulnérabilités techniques sont exacerbées par des difficultés d'accompagnement des DSSI dans les projets nationaux. La CNIL a même retoqué certaines nouveaux projets pour leur fragilisation. Par exemple, un

---

[157] ZIRAR (Wassinia), *Talents de l'e-santé : 11 lauréats, dont plusieurs établissements, pour cette première édition,* E-santé, 11 décembre 2020, ticsante.com.

[158] QUEMENER (Myriam), « Cybersécurité et protection des données de santé », *Dalloz IP/IT*, 20 mai 2020, page 303.

système national des données de santé (SNDS) a été mis en place suite à la loi de 2016[159], et d'un décret[160]. Ce SNDS a fait l'objet de deux délibérations de la CNIL en 2016[161] et en 2017[162]. La CNIL y relève un algorithme ancien, et une absence de renouvellement des secrets cryptographiques. La Commission enjoint au responsable de traitement de faire évoluer le procédé cryptographique, et recommande d'ajouter un cloisonnement, avec un réseau séparé dédié à l'administration des systèmes SNDS. Cette sécurisation numérique est d'autant plus importante avec l'arrivée de la 5G. Le 14 septembre 2020, face aux acteurs de la *French Tech*, Emmanuel Macron s'est présenté comme le Président de la *« start-up nation »*[163]. Il affirmait que le tournant de la 5G est celui de l'innovation et va bouleverser la société, l'emploi, l'éducation, les transports jusqu'à notre intimité. A l'échelle des EPS, le développement du réseau 5G implique un renforcement et une actualisation des logiciels informatiques.

Pour relever les défis d'aujourd'hui et de demain, le renforcement de la sécurité des SIH apparaît indispensable. Ce renforcement s'accompagne nécessairement d'un encadrement de l'hébergement des données personnelles de santé par une réglementation stricte et précise.

---

## Section II : L'encadrement de l'hébergement des données personnelles de santé par une réglementation stricte et précise

L'hébergement de données personnelles de santé est encadré par une procédure de certification imposée à tout hébergeur de données de santé (Paragraphe I) et une externalisation de cet hébergement peut être envisagée (Paragraphe II).

### Paragraphe I : Une procédure de certification imposée à tout nouveau hébergeur de données de santé

Plusieurs catégories de services d'hébergements existent (A) et une certification est imposée depuis 2018, pour tout hébergeur de données de santé à caractère personnel (B).

---

[159] Article 913 de la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022, 27 janvier 2016.

[160] Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé », *JORF* n°0301, 28 décembre 2016.

[161] Délibération n° 2016-316 du 13 octobre 2016 portant avis sur un projet de décret en Conseil d'Etat relatif au Système national des données de santé (demande d'avis n° 16018114), *JORF* n°0301, 28 décembre 2016.

[162] Délibération n° 2017-022 du 26 janvier 2017 portant avis sur un projet d'arrêté relatif au référentiel de sécurité applicable au Système national des données de santé (demande d'avis n° 16025310), *JORF* n°0071, 24 mars 2017.

[163] « 5G, la course à quoi ? », *Le Monde diplomatique,* François Ruffin et Cyril Poireaux, octobre 2020.

## A) De l'existence de catégories de services d'hébergement…

L'hébergement des données de santé à caractère personnel est encadré par le Code de la santé publique et notamment l'article L.1111-8. Cet article distingue explicitement trois catégories de services d'hébergement de données de santé : sur support papier, sur support numérique dans le cadre d'un service d'archivage électronique, et sur support numérique (hors cas de service d'archivage électronique). Dans le cas des EPS, l'hébergement des données fait partie de la troisième catégorie, soit celle sur support numérique (hors cas d'un service d'archivage électronique). A l'avenir, un référentiel Maturin-H[164] souhaite être mis en place par la DGOS début 2022. Ce référentiel se baserait sur des référentiels déjà connus (Hop'en, HDS, Ségur numérique, EMRAM[165]). La conformité à ce nouveau référentiel permettrait d'obtenir la certification SIH sans passer par la certification HDS expliquée précédemment. Les services d'hébergement sont divers mais quelque soit les modalités d'hébergement, les données ne sont hébergées que par un prestataire technique certifié.

## B) … à l'obligation d'obtenir un certificat de conformité

Depuis 2018[166], l'hébergement des données de santé à caractère personnel n'est plus conditionné par un agrément HADS mais par une procédure de certification. En effet, tout nouveau hébergeur de données de santé à caractère personnel doit être titulaire d'un certificat de conformité. Ce certificat est délivré par les organismes de certification accrédités par l'instance française d'accréditation[167], soit par le Comité Français d'Accréditation (COFRAC). Un décret en Conseil d'Etat, pris après avis de la CNIL et des conseils nationaux de l'ordre des professions de santé, fixe les conditions de délivrance[168]. De manière plus précise, ce dispositif de certification est déterminé par la Délégation à la Stratégie des SI de

---

164 Maturité Numérique des établissements hospitaliers.

165 Electronic Medical Record Adoption Model de l'organisation américaine HIMSS (Healthcare Information and Management Systems Society).

166 Article 1 de l'ordonnance n°2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel.

167 Article L.1111-8 II du Code de la santé publique.

168 Décret n°°2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel, *JORF* n°0049, 28 février 2018.

Santé (DSSIS)[169] et l'ANS, et validé par un comité de pilotage réunissant les représentants institutionnels (Ministre des Solidarités et de la Santé, ANSSI, CNIL, Fédérations hospitalières, Conseils de l'Ordre concerné…) et des représentants d'industriels[170]. Cette procédure de certification donne un cadre à l'hébergement des données dites sensibles traitées par les EPS. Des contrôles sont effectués tous les ans via des audits. Pour une sécurité numérique, le respect de la procédure de certification pour tout nouveau hébergeur de données de santé est indispensable. En plus de cette procédure, pour limiter l'impact des cyberattaques, une externalisation de l'hébergement des données peut être envisagée.

## <u>Paragraphe II</u>: L'externalisation de l'hébergement des données de santé à caractère personnel

L'externalisation répond à des exigences (A) et participe au management des risques dans l'EPS, en amont et lors d'une cyberattaque (B).

### A) Du concept de l'externalisation…

Pour un stockage sécurisé des données, une des options possibles est l'externalisation de l'hébergement des données. Cette externalisation est plutôt perçue positivement par les EPS. En effet, une étude nationale réalisée fin 2017[171] a interrogé plusieurs EPS sur la stratégie qu'ils souhaitaient adopter dans le cadre de la préparation du schéma directeur du système d'information convergent (SDSI) du GHT. Près de 57% de ces établissements déclaraient envisager une externalisation de l'hébergement des données générées. Depuis 2018, pour pouvoir externaliser, l'hébergeur doit obtenir un certificat dit *« hébergeur infogéreur* ». Ce certificat permet, en autre, aux EPS de sauvegarder leurs données de manière externalisée[172]. Au delà du concept d'externalisation, en pratique, cette externalisation de l'hébergement des données personnelles concernant la santé participe au management des risques dans l'EPS.

---

[169] Délégation à la Stratégie des Systèmes d'Information de Santé - remplacée par la Délégation ministérielle au Numérique en Santé (DNS) suite au décret n°2019-1412 du 20 décembre 2019 portant diverses dispositions relatives à l'administration centrale des ministères chargés des affaires sociales, *JORF* n°0296, 21 décembre 2019, texte n°17.

[170] *Mémento à l'usage du directeur d'établissement de santé - Connaître vos risques pour mieux y faire face, Cybersécurité,* édition 2017 - DGOS, page 19.

[171] *Convergence SI et GHT : 2018, le temps des schémas directeurs,* APMnews et TICsanté, 2017, page 7.

[172] *Mémento à l'usage du directeur d'établissement de santé - Connaître vos risques pour mieux y faire face, Cybersécurité,* édition 2017 - DGOS, page 19.

## B) … à la participation au management des risques dans l'EPS

L'externalisation a fait ses preuves et permet de participer au management des risques au sein d'un EPS. Cette externalisation contribue à la gouvernance, à la gestion des risques et au maintien de la conformité des SIH avec le patient qui est au centre de l'environnement numérique[173]. Il apparaît alors primordial de bien choisir le prestataire d'hébergement. A titre d'illustration, le CH d'Albertville-Moûtiers a mis en place une architecte de sauvegarde dite *« sauvegarde 3-2-1 ».* Cette architecte implique 3 copies de sauvegarde différentes, sur 2 supports distincts avec 1 support externalisé. Ce mode de fonctionnement a fait ses preuves lors de la cyberattaque de décembre 2020 puisque grâce à ce mode de fonctionnement, les données ont pu être protégées et rapidement récupérées, réduisent inexorablement le temps de relance du SIH.

Par conséquent, l'actualisation des SIH des EPS est certes nécessaire pour renforcer l'efficience de la sécurité numérique des données personnelles mais le facteur humain contribue grandement à la vulnérabilité des SIH. Des moyens humains sont donc indispensables.

[173] *Les établissements publics de santé : sécurité et défense*, 20 mai 2021, tenu sous l'égide de LEJEP et AFDSD, avec le soutien de l'AFDS, coordonné par le professeur Pierre BOURDON, membre du LEJEP du CY Cergy Paris Université et membre de l'AFDSD, 14:16.

# Chapitre II : La sécurité numérique, une responsabilité humaine à la fois individuelle et collective

La sensibilisation des utilisateurs d'outils informatiques au sein des EPS est un point essentiel. Le facteur humain est en majorité responsable des vulnérabilités des SIH (80%). La mise en place d'une protection des données passe nécessairement par la désignation de postes spécifiques pour la protection des données (Section I) ainsi que par l'alliance des acteurs qualifiés et conscients du risque (Section II).

---

## Section I : L'établissement impératif d'une protection effective des données personnelles au niveau du GHT

La sécurité numérique ne se pense pas qu'au niveau de l'EPS. Avec l'instauration obligatoire des GHT, la sécurité numérique est nécessairement envisagée au niveau du groupement. Protéger les données personnelles implique alors une création de postes présents au niveau de l'établissement support (Paragraphe I) ainsi qu'une solidarité entre les établissements membres et l'établissement support du GHT (Paragraphe II).

### Paragraphe I : La création de postes spécifiques à la sécurité numérique des EPS au sein des GHT

Parmi les postes spécifiques crées dans le cadre de la sécurité numérique des EPS, le délégué à la protection des données (A) et le responsable sécurité des systèmes d'information (B) sont les principaux.

#### A) Un délégué à la protection des données…

Depuis le 25 mai 2018, date d'entrée en application du RGPD, les données concernant la santé sont des données dites sensibles[174]. Ces données relèvent d'une catégorie particulière de données nécessitant un traitement adéquat. Ce traitement, à l'échelle d'un EPS, est considéré comme *« à grande échelle »* et implique une protection renforcée. Cette protection passe notamment par l'obligation pour les EPS de désigner un délégué à la protection des donnés (DPO)[175] présent au niveau de l'établissement support. Ce DPO exerce une mission

[174] Article 9 du RGPD - *Traitement portant sur des catégories particulières de données à caractère personnel.*

[175] Article 37 du RGPD - *Désignation du délégué à la protection des données.*

d'information, de conseil et de contrôle en interne. Dans le cadre de ces missions, le délégué contrôle, en autre, le respect du RGPD, réalise le registre de traitements des données, gère les procédures, sensibilise et forme, réalise des audits, et gère les demandes des personnes souhaitant accéder à leurs données. Le DPO est le point d'entrée avec la CNIL et l'interface privilégiée en matière de protection des données personnelles pour les établissements membres. Les données personnelles sensibles traitées par les EPS sont certes protégées par le DPO mais aussi par d'autres postes spécialisés comme le responsable sécurité des SI.

### B) … accompagné d'un responsable sécurité des systèmes d'information

Au sein d'un EPS, l'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI) est le directeur[176]. Ce dernier est érigé comme étant l'autorité juridiquement responsable de la sécurité des SIH[177]. Pour assurer la sécurité de SIH, l'AQSSI nomme et mandate un Responsable Sécurité des Systèmes d'Information (RSSI)[178]. Ses missions consistent, en autre, à piloter à l'échelle du GHT la sécurité des SI, à mettre en place des plans de sécurité adaptés en concordance avec la politique nationale de sécurité des SI, ou encore à améliorer la sécurité des SI via une veille technologique active et une participation à des groupes de réflexion *ad hoc*[179]. De surcroît, le RGPD[180] impose de sécuriser les traitements de données personnelles. Ces mesures de cybersécurité font partie des attributions du RSSI, avec l'étroite collaboration du DPO. En plus de la création de postes spécifiques à la protection des données personnelles de santé des EPS, une solidarité entre les établissements membres et l'établissement support du GHT apparaît nécessaire.

## <u>Paragraphe II</u> : L'indispensable solidarité entre les établissements membres et l'établissement support du GHT

La solidarité entre les établissements membres et l'établissement support doit exister au niveau du GHT (A) mais certaines difficultés sont encore à surmonter (B).

---

176 Arrêté du 13 décembre 2016 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle des ministères chargés des affaires sociales, *JORF* n°0294, 18 décembre 2016, Article 1.

177 *Ibid.*, Article 2.

178 *Ibid.*, Article 4.

179 *Cybersécurité - Menaces et vulnérabilités des systèmes d'information*, 15 mars 2017, site du Ministère des Solidarités et de la Santé.

180 Article 32 du RGPD - *Sécurité du traitement.*

## A) Le rôle clé de l'établissement support…

Depuis 2016[181], le Code de la santé publique[182] précise que l'établissement support désigné par la convention constitutive, assure pour le compte des établissements parties au groupement la stratégie, l'optimisation et la gestion commune d'un système d'information hospitalier convergent. Cette convergence porte notamment sur le dossier patient et implique une prise en charge coordonnée des patients au sein des établissements membres du GHT[183]. Concrètement, le SI du GHT doit comporter des applications identiques pour chacun des domaines fonctionnels et les établissements parties doivent utiliser un identifiant unique pour les patients[184]. Ce SI est, depuis 2021[185], convergent et interopérable. L'établissement support est donc responsable de la mise en place d'un tel SI au niveau du GHT. Le schéma directeur de ce SI est élaboré par le directeur de l'établissement support et doit être conforme aux objectifs du projet médical partagé (PMP), après concertation avec le comité stratégique[186]. Depuis 2018[187], les établissements de soins de santé, y compris les hôpitaux font partis des Opérateurs de Services Essentiels (OSE). Plus précisément, un opérateur est désigné OSE lorsque des réseaux et systèmes d'information sont nécessaires à la fourniture du service concerné[188] et qu'un incident affectant ces réseaux et systèmes aurait, sur la fourniture de ce service, des conséquences graves, appréciées au regard de divers critères[189] (nombre d'utilisateurs, part du marché, portée géographique…).

---

[181] Article 107 de la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022, 27 janvier 2016.

[182] Article L.6132-3 1° du Code de la santé publique.

[183] BERGOIGNAN-ESPER (Claudine), « L'hôpital public au sein du plan « Ma santé 2022 » », *RDSS 2019,* page 15.

[184] Article R.6132-15 I. du Code de la santé publique.

[185] Loi n°2021-502 du 26 avril 2021 visant à améliorer le système de santé par la confiance et la simplification, *JORF* n°0099, 27 avril 2021.

[186] Article R.6132-15 II. du Code de la santé publique.

[187] Décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, *JORF* n°0118, 25 mai 2018.

[188] *Ibid.*, Article 2.

[189] *Id.* : […] *«1° Le nombre d'utilisateurs dépendant du service ;*
*2° La dépendance des autres secteurs d'activités figurant à l'annexe au présent décret à l'égard du service ;*
*3° Les conséquences qu'un incident pourrait avoir, en termes de gravité et de durée, sur le fonctionnement de l'économie ou de la société ou sur la sécurité publique ;*
*4° La part de marché de l'opérateur ;*
*5° La portée géographique eu égard à la zone susceptible d'être touchée par un incident ;*
*6° L'importance que revêt l'opérateur pour assurer un niveau de service suffisant, compte tenu de la disponibilité de moyens alternatifs pour la fourniture du service ;*
*7° Le cas échéant, des facteurs sectoriels. ».*

Face à la recrudescence des cyberattaques, une stratégie nationale en matière de cybersécurité a été annoncée le 18 février 2021. Cette stratégie envisageait d'intégrer, d'ici l'été 2021, 135 GHT à la liste des OSE. Finalement, tous les établissements supports de GHT seraient désignés OSE selon Charlotte Drapeau, chef du bureau Santé et Société à l'ANSSI[190]. Cette incorporation au sein de la liste des services essentiels au fonctionnement de la société ou de l'économie implique des règles de sécurité informatique plus strictes. Le respect de ses règles sera assuré par l'ANSSI. Chaque GHT a un rôle dans le renforcement de la politique nationale en matière de cybersécurité. Personne ne peut prévoir quand un EPS peut être attaqué informatiquement mais les diverses cyberattaques des EPS français ont démontré l'importance de l'entraide des EPS au sein d'un GHT et au niveau national.

Au sein d'un GHT, l'établissement support a donc un rôle clé. Cependant, ce rôle est souvent paralysé par la persistance de difficultés organisationnelles.

### B) … paralysé par la persistance de difficultés organisationnelles au sein du GHT

Successivement, avec l'essor de la protection des données personnelles et l'instauration obligatoire du GHT, de nouveaux postes, comme ceux de DPO et RSSI ont été crées. Cependant, ces créations de poste restent récentes et de nombreux GHT manquent encore de RSSI ou de DPO. De plus, dans un contexte de recrudescence des cyberattaques, un RSSI et un DPO pour tous les établissements du GHT au niveau de l'établissement support sont bien souvent insuffisants pour répondre à toutes les problématiques surgissant au quotidien. En dehors du RSSI et du DPO, aucun moyen supplémentaire n'est instauré et un manque de soutien peut se faire ressentir de la part de ces acteurs clés.

Certes, des moyens humains sont mis en place mais pour limiter les vulnérabilités humaines, il est nécessaire d'instaurer une véritable alliance entre des acteurs qualifiés et conscients du risque.

---

190 TRELY (Vincent), *Interview exclusive de Charlotte DRAPEAU, chef du Bureau Santé et Société de l'ANSSI,* 16 juin 2021, apssis.com.

## Section II : L'alliance des acteurs qualifiés et conscients du risque

*« Penser la sécurisation des établissements est une approche globale garantissant le niveau de soins, l'accueil des patients et la qualité de vie au travail des personnels »*[191]. Tel est le constat posé par Agnès Buzyn, ancienne Ministère des Solidarités et de la Santé en novembre 2017. En effet, la sécurité numérique d'un EPS implique irrémédiablement une approche globale. Cette approche se doit de garantir à la fois une prise en charge de qualité pour le patient et à la fois un cadre professionnel serein pour les personnels. Pour cela, la formation permet aux utilisateurs du SIH d'adopter les bons réflexes (Paragraphe I) et la solidarité entre les acteurs du système de santé français doit être encouragée (Paragraphe II).

### Paragraphe I : La formation des utilisateurs du SIH pour adopter les bons réflexes

Il appert que la formation des professionnels de santé (A) et des directeurs d'EPS (B) est essentielle pour instaurer une véritable démarche de gestion du risque numérique. Cette gestion du risque se fait autant dans la perspective de l'anticipation que de la réaction face à un acte de cybermalveillance.

#### A) L'indispensable prise de conscience du risque par les utilisateurs du SIH…

Le manque de connaissances des utilisateurs du SIH vient souvent d'un défaut de connaissance ou d'un défaut d'intérêt pour la sécurité numérique. La sécurité du traitement n'est pas suffisamment prise en compte par ces derniers. Les lacunes se reflètent au travers d'accès illégitimes enfreignant le secret professionnel par exemple. Former les utilisateurs du SIH aux principes d'hygiène numérique et les enjeux de la cybersécurité apparaît indispensable. Les formations peuvent porter autant sur un rappel de bons réflexes, que sur la procédure d'alerte et de réaction en cas d'incident. Par exemple, au sein du CHU de Lille, depuis peu, des formations sont proposées pour les infirmières et les nouveaux arrivants lors de journées spécifiques. Des newsletters pour les professionnels de santé sont également instaurées pour les informer régulièrement de failles numériques sur les logiciels. Une sensibilisation sur les bons réflexes à adopter est aussi effectuée via des fiches pratiques sur l'Intranet du CHU. Des méthodes de protection simple existent, pouvant être expliquées et

[191] Agnès Buzyn, Ministère des Solidarités et de la Santé, *Colloque sur la sécurisation des établissements de santé*, 7 novembre 2017.

adoptées par les utilisateurs du SIH. Par exemple, éviter la lecture de programmes dont l'origine est inconnue (clés USB, pièces jointes inconnues, mails), mettre à jour régulièrement les logiciels, utiliser un antivirus fiable et performant, éviter les sites non fiables, choisir des mots de passe complexes et uniques, instaurer des pares-feu, ou encore ne pas utiliser des appareils non sécurisés ou personnels. Les menaces de contamination sont de plus en plus fulgurantes et peuvent se produire en l'espace de quelques secondes via un mail ou une clé USB. A l'inverse, pour éviter tout effet pervers à l'écoute des risques d'une cyberattaque, une information se doit d'être effectuée pour qu'ils proscrivent de leur habitude toute copie des données. En effet, par anticipation, certains professionnels pourraient être tentés de copier les données. Cette perte de confidentialité majeure est proscrite par l'ANSSI.

En conséquence de cela, former, informer, et sensibiliser les utilisateurs permettent une prise de conscience sur les risques de l'interface homme-machine et l'ampleur de l'impact de la machine sur un EPS. Cette prise en conscience doit également provenir des directeurs d'EPS qui ont une part de responsabilité à assumer en matière de sécurité numérique.

### B) … où les directeurs d'EPS ont une part de responsabilité à assumer

Pour s'armer contre les attaques, des formations pour les directeurs d'établissements de santé sont mises en place. Elles leur permettent de réfléchir sur des scénarios catastrophes. Jean-Baptiste Rouffet, directeur de l'EHPAD *Les 3 sources* à Loperhet (Finistère), estime que les directeurs d'établissement ne doivent pas seulement se reposer sur les Responsables Sécurité SI. La sécurité des SIH est l'affaire de tous. Les directeurs ne doivent pas attendre que leur EPS soit attaqué pour se protéger[192]. Les formations des directeurs d'établissement est d'autant plus importante qu'ils sont les AQSSI au niveau de l'EPS. Cependant, le coût peut parfois freiner la formation des directeurs et de l'ensemble des acteurs. Même si en soit, par rapport aux coûts financiers engendrés par un *ransonware*, le coût de la formation peut paraître dérisoire. De plus, les failles sont parfois très techniques. Cette technicité nécessite d'avoir l'acquisition de compétences pour, en amont, limiter les comportements générateurs de failles et en aval d'une cyberattaque, émettre des hypothèses sur leurs origines et adopter les bons réflexes. Au delà de ces formations des utilisations du SIH, il apparaît indispensable que l'entraide prime entre les acteurs du système de santé français.

[192] RABEUX (Cécile), « Le secteur médico-social est encore vulnérable face aux cyberattaques », Systèmes d'information, *Hospimedia*, 23 août 2020.

## <u>Paragraphe II :</u> L'entraide entre les acteurs du système de santé français

La création d'un espace de confiance entre les professionnels et les patients est un levier essentiel à l'amélioration de la qualité des soins[193]. Pour cela, il appartient aux acteurs de se coordonner (A) et partager leurs connaissances (B).

### A) D'une coordination des acteurs…

Pour endiguer la survenance des cyberattaques, les acteurs du système de santé se doivent de favoriser la concertation et la coordination entre eux. La solidarité doit primer. La réussite de la gestion d'une cyberattaque par la coordination a d'ailleurs été démontrée depuis l'accentuation de la survenance de cyberattaques et le début de prise de conscience de la part des acteurs. La sécurisation des EPS ne peut réussir que si elle fait l'objet d'un travail collaboratif au niveau local entre les EPS, le Parquet, les forces de l'ordre, les collectivités locales et tous les autres acteurs impliqués. En plus de cette coordination, le partage de connaissances via des instances coordonnatrices au sein des EPS ou des comités apparaît comme un élément indispensable dans la gestion appropriée des cyberattaques.

### B) … au partage de connaissances via des instances coordonnatrices

La sécurité numérique des EPS n'est pas seulement une problématique technique. C'est une notion devant être prise en compte au niveau de la gouvernance des organisations intermédiaires. Par exemple, au sein de l'ARS Provence-Alpes Côtes d'Azur, depuis le 22 juin 2017, un comité régional stratégique des SI de santé (CORSSIS) se réunit deux fois par an[194]. Mis en place dans le cadre du schéma directeur régional des SI 2018-2022, ce comité permet de réunir, en autre, l'ensemble des acteurs régionaux du champ de la santé numérique[195]. De plus, au niveau national, le partage d'expériences est également possible depuis 2017[196] via le Comité de maîtrise des risques numériques. Ce comité est crée au sein

---

[193] *Mémento à l'usage du directeur d'établissement de santé - Connaître vos risques pour mieux y faire face, Cybersécurité,* édition 2017 - DGOS, page 10.

[194] *SI en Santé et Télémédecine*, 13 avril 2021, auvergne-rhone-alpes.ars.sante.fr.

[195] *Perpectives du numérique en santé et télémédecine, réunion annuelle des HAD,* 3 octobre 2018, Agence Régionale de Santé Provence-Alpes Côte d'Azur, page 3.

[196] Arrêté du 4 septembre 2017 portant création d'un comité de maîtrise des risques numériques au sein du comité stratégique de maîtrise des risques des ministères chargés des affaires sociales, *JORF* n°0216, 15 septembre 2017.

du comité stratégique de maîtrise des risques des Ministères chargées des affaires sociales, et permet de piloter la politique de sécurité des SI tout en assurant la gestion des risques dans les domaines numériques. Enfin, depuis la stratégie numérique du Gouvernement présentée le 18 juin 2015, le GIP Action contre la Cybermalveillance (ACYMA) permet un partenariat entre des acteurs publics et privés en matière de sécurité numérique via une mutualisation des ressources, compétences et expertises[197]. Ces différentes lignes de défense autant régionales que nationales permettent ainsi une coopération et donc un renforcement de la sécurité numérique des SIH.

Par conséquent, la mise en place de moyens participe à l'efficience de la sécurité numérique des données personnelles. Cependant, le questionnement sur les pratiques est indispensable pour une meilleure hygiène numérique.

[197] *Qu'est-ce que le GIP ACYMA ?, Qui sommes-nous ?,* 27 novembre 2019, cybermalveillance.gouv.fr.

# Titre II : L'indispensable questionnement des pratiques, condition d'une meilleure hygiène numérique

Du fait du caractère récent des outils informatiques et des textes encadrant leur utilisation, les solutions pour une sécurité numérique effective des EPS n'ont émergé que dernièrement et sont donc encore en construction. Cette élaboration implique des questionnements sur les pratiques autant techniques, professionnelles que juridiques. Pour cela, la sécurité numérique des EPS est une contrepartie indispensable à la numérisation et à la pérennisation du système de santé français (Chapitre I) et suppose, nécessairement, que les moyens procéduraux existants soient mis en oeuvre (Chapitre II).

## Chapitre I : La sécurité numérique des établissements publics de santé, contrepartie indispensable à la numérisation et à la pérennisation du système de santé français

La sécurité numérique des EPS implique de déceler les vulnérabilités et négligences via des audits (Section I) mais également de prendre conscience du rôle majeur des technologies numériques dans la modernisation de notre système de santé (Section II).

---

## Section I : Le décèlement des vulnérabilités des SIH, étape d'analyse primordiale pour une réponse adaptée

Les audits se révèlent importants dans le cadre de la préservation des données de santé (Paragraphe I) et la détection des vulnérabilités permet d'adopter les bons réflexes (Paragraphe II).

### Paragraphe I : L'importance des audits dans la préservation des données de santé

Le Gouvernement souhaite réaliser des audits de cybersécurisation des EPS (A) et il appert que les audits permettent de détecter les besoins (B).

#### A) De la réalisation d'audits de cybersécurisation des EPS…

Lors de la présentation de la stratégie Cyber le 18 février 2021, le Président de la République Française a annoncé l'attribution de vingt-cinq millions d'euros à la réalisation

d'audits de cybersécurisation des EPS et au déploiement du service national de cybersurveillance en santé en partenariat avec l'ANS[198]. Ces audits sont indispensables pour le décèlement des vulnérabilités des SIH. Pour détecter ces vulnérabilités, pour chaque processus ou type d'informations, il est identifié un besoin de sécurité au regard de trois critères : la disponibilité, l'intégrité et la confidentialité. De manière plus détaillée, un SIH est disponible lorsqu'il est accessible et que la continuité du service informatique peut être assurée, intègre lorsqu'aucune modification ne peut être faite sans autorisation et confidentiel lorsque l'accès n'est possible qu'en cas d'autorisation[199].

Les audits de cybersécurisation des EPS se révèlent être donc un souhait gouvernemental. Ces audits sont un véritable atout pour détecter les vulnérabilités, évaluer les besoins et sécuriser de manière la plus adéquate possible les SIH.

### B) … à l'évaluation des besoins au regard des vulnérabilités détectées

Les audits réalisés, qu'ils soient de sécurité, de gouvernance ou techniques, permettent de repérer les vulnérabilités et les besoins en terme de moyens. Au niveau national, le service de cybersurveillance de l'ANS a audité depuis fin 2018 plus de soixante établissements. Ces audits ont révélé d'importantes failles dans les SIH. Par audit, en moyenne, vingt-sept vulnérabilités ont été détectées dont huit fortes et sept faibles[200]. Les vulnérabilités les plus détectées sont la divulgation d'information (31%), la gestion des correctifs (18%) et des mises à jour des logiciels (11%). Ces audits ne sont utiles que si, au niveau des GHT et au niveau national, les établissements se coordonnent pour faire des bilans et échangent sur l'évolution de l'état ainsi que sur la gestion de la menace.

Les audits sont d'autant plus importants qu'ils permettent aux utilisateurs des SIH d'adopter les bonnes pratiques en fonction des vulnérabilités détectées.

---

198 *Sécurité des réseaux informatiques des établissements de santé : le Gouvernement renforce sa stratégie*, communiqué de presse, 22 février 2021 sur le site du Ministère des Solidarités et de la Santé.

199 *Mémento à l'usage du directeur d'établissement de santé - Connaître vos risques pour mieux y faire face*, Cybersécurité, édition 2017 - DGOS, page 20.

200 DEBACKER (Perrine), « Les structures de santé pourront commander des audits de cybersécurité via une interface », Système d'information, 6 octobre 2020, *Hospimedia*.

## <u>Paragraphe II</u> : L'établissement de bonnes pratiques à partir de la détection des vulnérabilités des SIH

Plusieurs bonnes pratiques sont prédominantes (A) et pour que ces dernières soient le plus adéquates possible, la réalisation d'études d'impacts régulières est primordiale (B).

### A) Des bonnes pratiques multiples en matière de sécurité numérique des SIH…

Une fois les vulnérabilités sont détectées, pour éviter d'exacerber ces fragilités numériques, des cyber-conseils sont proposés par l'ANSSI. Plus spécifiquement, un guide de bonnes pratiques face aux *ransonwares*[201] préconise en autre, pour réduire le risque d'attaques, de réaliser des sauvegardes régulières, de maintenir à jour les logiciels, les systèmes et les logiciels antivirus, de cloisonner le SIH, de limiter les droits des utilisateurs et les autorisations des applications, de sensibiliser les utilisateurs des SIH, de souscrire à une assurance cyber ou encore de penser à une stratégie de communication de crise cyber. De surcroît, en cas d'attaques, pour limiter les pertes, l'ANSSI incite les entités victimes d'un rançongiciel à adopter les bons réflexes (déconnection des supports), à piloter la gestion de la crise cyber, à trouver de l'assistance technique via la plateforme <u>cybermalveillance.gouv.fr</u>, à communiquer au juste niveau, à ne pas payer la rançon, à déposer plainte ou encore à restaurer les systèmes depuis des sources saines. En plus de ce guide, d'autres guides sont proposés par l'ANSSI sur l'hygiène informatique, ou sur la maîtrise des risques numériques. La CNIL propose aussi des guides sur la sécurité des données personnelles et des fiches sur la notification d'une violation de données personnelles ainsi que sur la sauvegarde et l'anticipation de la continuité d'activité.

Ces bonnes pratiques ne sont efficaces que si des études d'impact sont réalisées régulièrement pour mesurer leur impact et les adapter aux lacunes à combler.

### B) … actualisées par la réalisation régulière d'études d'impact

Pour chacun des traitements de données personnelles sensibles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, une étude

[201] *Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident ?,* guide, ANSSI, août 2020.

d'impact sur la protection des données doit être réalisée[202]. Cette étude d'impact dite étude d'impact sur la vie privée (EIVP)[203], permet d'instaurer un traitement de données personnelles respectueux de la vie privée des patients, d'apprécier les impacts sur la vie privée et de démontrer le respect des principes fondamentaux du RGPD. L'étude contient une description du traitement et ses finalités, une appréciation de la nécessité et de la proportionnalité du traitement, une évolution des risques sur les droits et libertés ainsi que la proposition de mesures pour se conformer au RGPD. Des guides pour la réalisation de ces études d'impact sont disponibles sur la CNIL.

La détection des vulnérabilités est indispensable. En plus de cette détection, les technologies numériques se révèlent être un levier majeur pour la modernisation du système de santé français.

---

## Section II : Les technologies numériques, levier majeur pour la modernisation du système de santé français

La santé numérique est plus que présente au sein des EPS (Paragraphe I), d'autant plus avec l'arrivée d'outils connectés et de l'IA (Paragraphe II).

### Paragraphe I : La présence indéniable de la santé numérique au sein des EPS

Le Gouvernement français souhaite être un leadership en santé numérique (A) avec, concomitamment, la protection d'un patient au centre d'un environnement numérique (B).

#### A) De l'aspiration gouvernementale d'un leadership en santé numérique…

Dans un discours prononcé le 4 décembre 2020, Emmanuel Macron a exprimé son aspiration de faire de la France, un des leaders de la santé numérique. Pour cela, il a annoncé le lancement d'un projet Val-de-Grâce. Ce projet consiste à créer un lieu à Paris, dédié à l'innovation et au numérique en santé. Ce projet est instauré avec la collaboration de l'ANS, le *Health data hub*, l'Institut National de Recherche en Sciences et Technologies du Numérique (INRIA), l'Institut National sur la Santé et la Recherche Médicale (INSERM), le

---

[202] *Règlement européen sur la protection des données personnelles se préparer en 6 étapes*, Etape 4, Règlement Européen, CNIL, 2018, page 5.

[203] *Privacy Impact Assessment* (PIA).

Centre National de la Recherche Scientifique (CNRS), l'Université Paris sciences et lettres, l'AP-HP et des partenaires du privé (Sanofi, Dassaut). L'objectif est de créer un projet interdisciplinaire. Toutes les disciplines de santé, l'apport du numérique de l'IA vont être mis à profit pour, en autre, mieux prévenir les pathologies, accélérer la recherche et améliorer le parcours de soins. Dans le cadre de cette santé numérique actuelle et future, le patient est au coeur d'un environnement numérique. Sa protection doit nécessairement être prise en compte.

### B) … à la protection du patient au coeur d'un environnement numérique

Le patient est au coeur d'un environnement numérique, autant pour sa prise en charge médicale que dans son environnement matériel immédiat. Cette place du patient est accentuée par la mise en place du Dossier Patient Informatisé (DPI). En effet, l'informatisation du dossier patient est progressivement devenue la norme suite à des plans nationaux comme le programme *« Hôpital numérique »* en 2013 ou encore le programme HOP'EN en 2019. D'autant plus qu'en terme de qualité de prise en charge, selon une enquête de juin 2015[204], 60% des malades chroniques utilisant des applications mobiles de santé affirment que ces applications les aident à mieux gérer leurs pathologies. La sécurité numérique au sein des EPS implique de prendre en considération les nouvelles technologies numériques.

## Paragraphe II : L'incorporation des nouvelles technologies numériques au sein des SIH

Les services numériques en santé (A) ainsi que l'arrivée de l'IA (B) impliquent une protection solide pour éviter une accentuation des cyberattaques : tirer tous les bénéfices sans s'exposer à de nouveaux risques.

### A) De la sécurisation des services numériques en santé…

Les services numériques en santé sont définis comme un ensemble de services de santé en ligne permettant aux usagers d'effectuer des démarches de façon dématérialisée, et d'outils numériques de coordination et d'échange ou de partage principalement destinés aux professionnels de santé[205]. Sécuriser ces services numériques en santé est plus

[204] *Santé mobile et connectée : usages, attitudes et attentes des malades chroniques*, Enquête Le Lac e-santé, juin 2015.

[205] *Les services publics numériques en santé : des avancées à amplifier, une cohérence à organiser*, Rapport public annuel 2018, Cour des Comptes, février 2018, page 215.

qu'indispensable, d'autant plus avec le fulgurant développement de l'e-santé[206] dans un contexte de crise sanitaire exceptionnelle. Cette sécurisation est primordiale puisque les nouvelles applications médicales liées à l'utilisation des services numériques en santé risquent de complexifier le périmètre à protéger. En effet, la multiplication et l'hétérogénéité des équipements rendre plus complexe l'instauration d'une sécurité numérique protectrice des EPS. En plus de la nécessité de sécuriser l'utilisation des services numériques en santé, l'arrivée de l'IA soulève d'autres problématiques.

### B) … à l'arrivée de l'intelligence artificielle

L'IA n'a pas vraiment de définition selon Cédric Villani, mathématicien et auteur d'un rapport sur l'IA remis au Gouvernement en mars 2018[207]. L'IA contribuerait à l'amélioration de l'accès aux soins des citoyens, et à l'établissement d'une prise en charge plus personnalisée. Cependant, cette IA ne doit être qu'une aide au diagnostic pour les médecins. En effet, certes, ces nouvelles technologies apportent l'espoir d'une meilleure prise en charge des maladies et la perpective de guérisons plus nombreuses. Néanmoins, le rôle du médecin reste central et la décision finale lui appartient. En conséquence, l'IA ne doit en aucun cas remplacer la relation de soins avec un professionnel de santé. Chaque patient est unique et cette unicité ne peut être effacée[208]. L'IA peut être considérée comme un outil utile en terme de défense dans certaines problématiques de la sécurité numérique. Par exemple, l'IA pourrait détecter les malwares. En effet, elle pourrait être utilisée pour détecter des spam, repérer des intrusions dans un système ou analyser des fichiers[209]. Ainsi, l'automatisation d'un certain nombre de tâches pourrait contribuer à la cybersécurisation des SIH. A contrario, comme toute invention, l'IA peut être utilisée pour une automatisation des tentatives et une détection des vulnérabilités. Ainsi, tout l'enjeu est que les nouvelles technologies numériques doivent faire l'objet d'une utilisation raisonnée et ne doivent pas créer de nouvelles failles au sein des SIH.

Pour numériser et pérenniser le système de santé français, en plus de la mise en place d'une sécurité numérique, la mise en oeuvre de moyens procéduraux est nécessaire.

---

[206] Utilisation de technologies de la communication et de l'information dans le domaine de la santé.

[207] *Donner un sens à l'intelligence artificielle pour une stratégie nationale et européenne*, mission parlementaire confiée par le Premier Ministre Edouard Philippe du 8 septembre 2017 au 8 mars 2018, mars 2018, page 9.

[208] COLLOC (Joel), *Numérique et santé,* conférence de la Cour de Cassation du jeudi 16 mai 2019, sous la direction scientifique de Mmes Bénédicte BOYER-BÉVIÈRE, Astrid MARAIS et Dorothée DIBIE, 20:46.

[209] *Lien entre l'intelligence artificielle et la cybersécurité,* MOOC Défis et enjeux de la cybersécurité, fun-mooc.fr.

## Chapitre II : La nécessaire mise en oeuvre des moyens procéduraux existants

Les incidents de sécurité des SIH sont à signaler (Section I) et ne doivent en aucun cas être laissé impunis (Section II).

---

## Section I : L'indispensable signalement des incidents de sécurité des systèmes d'information de santé

En cas d'incidents de sécurité, un dispositif de gestion de crises est prévu à divers échelons sur le territoire français (Paragraphe I) et des autorités nationales sont compétentes pour assister les EPS en cas de cyberattaques (Paragraphe II).

### Paragraphe I : La gestion des incidents à divers échelons sur le territoire français

Au niveau régional, l'ARS (A) et au niveau national, l'ANSSI (B) assurent la gestion de la crise en cas de cyberattaques auprès des EPS.

#### A) De l'Agence Régionale de Santé, interlocuteur régional en cas de signalement…

Suite à la loi du 26 janvier 2016[210], l'ARS a été placée comme l'interlocuteur principal en cas d'incidents significatifs ou graves de sécurité des SI. Si de tels incidents se produisent, les établissements de santé ont alors l'obligation de les signaler, sans délai, à l'ARS[211]. Lorsque le degré de gravité de ces incidents est jugé élevé, l'ARS les transmet sans délai aux autorités compétentes[212]. Les catégories d'incidents concernés et les conditions de mise en oeuvre de ce signalement ont été précisées en septembre 2016[213]. Concrètement, est considéré comme un incident grave de sécurité des SI, les évènements générateurs d'une situation exceptionnelle au sein d'un établissement. Par exemple, un incident grave est celui qui a des

---

[210] Article 110 de la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022, 27 janvier 2016.

[211] Article L.1111-8-2 du Code de la santé publique, version en vigueur jusqu'au 20 novembre 2020.

[212] *Id.*

[213] Décret n°2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information, *JORF* n°0214, 14 septembre 2016.

conséquences potentielles ou avérées sur la sécurité des soins, celui qui a des conséquences sur la confidentialité ou l'intégrité des données de santé et celui qui porte atteinte au fonctionnement normal de l'établissement.

Dénoncer les incidents auprès de l'ARS permet à l'EPS de ne pas rester seul face à cette menace et permet surtout la mise en oeuvre de solutions. L'EPS ne doit pas partir du principe que ce signalement est inutile, peut nuire à sa réputation ou que les cybercriminels ne seront jamais arrêtés. Au contraire, le signalement permet de solliciter divers acteurs qui vont faire en sorte d'aider numériquement l'EPS, d'éviter tout dysfonctionnement dans la prise en charge des patients et de rechercher les responsables. La cybercriminalité est punie par la loi et les cyberattaques laissent des traces numériques qui peuvent être remontées.

En plus de l'ARS, depuis 2020[214], le Code de la santé publique[215] a été modifié. Désormais, en cas d'incidents significatifs ou graves de sécurité des SI, les EPS sont contraints de signaler sans délai ces derniers aux autorités compétentes de l'Etat et au groupement d'intérêt public[216]. Pour améliorer la gestion de la crise et face à la recrudescence de la menace, l'ARS n'est plus l'interlocuteur unique des EPS. Ce signalement doit être effectué sans délai via le portail de signalement des événements sanitaires indésirables[217]. L'un des acteurs majeurs recevant le signalement est l'ANSSI.

### B) … à l'ANSSI, autorité nationale de défense des SIH

Créée en juillet 2009[218], cette autorité nationale assure la fonction d'autorité nationale de défense des systèmes d'information. Dépendante du Premier Ministre dans le dispositif de cyberdéfense nationale, l'ANSSI recueille les informations techniques relatives aux incidents et apporte son concours pour répondre à ces incidents[219]. Depuis le 1er octobre 2017, à l'initiative du Ministère des Solidarités et de la Santé, un dispositif de traitement des signalements des incidents de sécurité des systèmes d'information (SSI) a été mis en place. Ce dispositif est destiné aux établissements de santé, aux structures médico-sociales et aux

---

214 Article 1 de l'ordonnance n°2020-1407 du 18 novembre 2020 relative aux missions des agences régionales de santé, *JORF* n°0280, 19 novembre 2020.

215 Article L.1111-8-2 du Code de la santé publique, version en vigueur depuis le 20 novembre 2020.

216 Article L.1111-24 du Code de la santé publique.

217 https://signalement.social-sante.gouv.fr.

218 Décret n°2009-934 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence Nationale de la Sécurité des Systèmes d'Information », *JORF* n°0156, 8 juillet 2009, Article 1.

219 *Ibid*., Article 3.

organismes et services exerçant des activités de prévention, de diagnostic ou de soins[220]. Depuis cette date, le signalement des incidents de sécurité des SI dans les EPS est obligatoire. Le lien entre les EPS et les échelons est essentiel. Ces liens sont autant régionaux avec l'ARS, que nationaux avec l'ANSSI. En plus de ces acteurs, des autorités nationales sont compétentes pour assister les EPS en cas de cyberattaques.

## <u>Paragraphe II</u> : La soutien d'autorités nationales aux compétences spécifiques

L'Agence du Numérique en Santé (A) et la Commission Nationale de l'Informatique et des Libertés (B) sont des autorités nationales compétentes pour assister les EPS dans le traitement des incidents de cybersécurité.

### A) Du soutien de l'ANS en matière de sécurité numérique…

L'ANS permet d'instaurer un lien national entre l'EPS ciblé et des acteurs compétents dans l'accompagnement et le suivi des incidents en matière de sécurité numérique. De manière plus spécifique, une cellule dite Cellule d'Accompagnement Cybersécurité des Structures de Santé (ACSS) a été mise en place depuis le 1er octobre 2017[221]. Cette cellule est sous la responsabilité du Fonctionnaire chargé de la Sécurité des SI (FSSI) du Ministère et de l'ANS. Depuis le 27 avril 2021, ce cellule a intégré le groupe interCERT-FR et devient le CERT Santé[222]. Les CERT sont des centres nationaux de réponses en urgence pour répondre aux cyberattaques. Ces centres permettent d'aider à prévenir et analyser les incidents de sécurité. En France, grâce à une étroite coopération avec l'ANSSI, cette cellule accompagne l'ensemble des établissements de santé et structures médico-sociales. En autre, elle répond aux incidents de sécurité et appuie les acteurs jusqu'à la clôture de l'incident. Elle effectue également une veille active via la diffusion d'alertes. Par exemple, depuis plusieurs mois, des alertes sont publiées concernant des vulnérabilités sur Windows Exchange ou encore sur Windows Print Spooler[223].

---

[220] *Cybersécurité*, site de l'Agence du Numérique en Santé.

[221] Décret n°2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information, *JORF* n°0214, 14 septembre 2016.

[222] *ANS - La Cellule ACSS devient le CERT Santé*, <u>cyberveille-sante.gouv.fr</u>.

[223] *Alertes*, <u>cyberveille-sante.gouv.fr</u>.

En cas d'incidents graves, et si l'EPS victime n'a pas les compétences nécessaires, la CERT Santé va au delà de simples investigations et de propositions de mesures. Par exemple pour les cyberattaques visant les CH de Dax-Côté d'Argent et Villefranche sur Saône, la CERT Santé a identifié la menace, a dressé des scénarios de la compromission pour retrouver le chemin, a constitué des preuves, a éradiqué le virus au sein des SIH, et a proposé un plan de retour à la normale ainsi que des mesures d'amélioration.

De manière globale, sur la période 2019-2020, sur les 369 incidents déclarés, la CERT Santé a reçu 90 demandes d'accompagnements[224] et elle est intervenue 32 fois pour un appui technique (investigation numérique, remédiation[225], etc). En plus de cette cellule CERT Santé, la CNIL a un rôle majeur en cas de cyberattaques à l'encontre d'un EPS.

### B) … à la protection des données personnelles de santé par la CNIL

Lors de la survenance d'un incident de sécurité, les données personnelles concernant la santé d'une personne peuvent faire l'objet d'une violation. Les violations peuvent entraîner la destruction, la perte, l'altération, la divulgation non autorisée de données transmises, conservées ou traitées d'une autre manière, ou un accès non autorisé. L'EPS victime d'un tel incident de sécurité doit dans les meilleurs délais le notifier à la CNIL, dans les 72h[226]. En cas de risque élevé pour les droits et libertés d'une personne physique, cette notification doit également être effectuée auprès des personnes concernées dans les meilleurs délais[227]. En règle générale, c'est le DPO qui fait le lien entre la CNIL, l'EPS et les personnes physiques concernées. Si le nombre de personnes physiques est trop important pour une information individuelle, il est possible de procéder à une communication. En cas de cyberattaques, les incidents doivent être signalés aux autorités régionales et nationales compétentes. En dehors des acteurs précédemment cités, d'autres acteurs interviennent comme le Centre d'Analyse en Lutte Informatique Défensive (CALID) et la Direction Générale de l'Armement Maîtrise de l'Information (DGA-MI) dans le cadre de la cyberdéfense des SIH. Les incidents ne doivent en aucun cas rester impunis. Le signalement aux autorités compétentes permet ensuite le déclenchement de poursuites à l'encontre des cybercriminels.

---

[224] *Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé,* Rapport public 2020, ANS, Ministère des Solidarités et de la Santé, avril 2021, page 11.

[225] Correction des failles de sécurité exploitées et amélioration des pratiques.

[226] Article 33 du RGPD - *Notification à l'autorité de contrôle d'une violation de données à caractère personnel*.

[227] Article 34 du RGPD - *Communication à la personne concernée d'une violation de données à caractère personnel*.

## Section II : La poursuite des cybercriminels, une lutte contre l'impunité

Dans le cadre de la cybercriminalité, des acteurs comme la Direction Générale de la Sécurité Intérieure (DGSI), ou encore l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) participent à cette lutte contre l'impunité. Cette impunité n'existe pas puisque des sanctions sont prévues en matière de cybercriminalité (Paragraphe I) et condamner apparaît plus que nécessaire pour dissuader les cybercriminels (Paragraphe II).

### Paragraphe I : L'existence de sanctions en matière de cybercriminalité

Des sanctions pénales sont prévues (A) et suscitent un sentiment de justice rendue de la part des victimes de cyberattaques (B).

#### A) Des sanctions pénales prévues…

En France, si une personne est à l'initiative d'une cyberattaque altérant un SIH et récupère des données personnelles de santé, alors elle peut être déclarée coupable d'extorsion de fonds[228] et d'atteinte aux systèmes de traitement automatisé de données[229]. De surcroît, des réflexions sont actuellement en cours pour simplifier la compréhension et la mise en pratique des règles relatives à la cybersécurité. La création d'un Code de la cybersécurité a été proposée pour permettre, dans un seul Code, de regrouper toutes les règles éparpillées dans le Code pénal, dans le Code de procédure pénale, le Code monétaire et financier, le Code de la santé publique voire même le Code des postes et des communications. Il existe donc un mouvement en faveur de la création d'une compilation raisonnée de l'ensemble des lois et règlements s'appliquant au droit de la cybersécurité[230]. Ces sanctions prévues provoquent bien souvent un sentiment de justice de la part des victimes des cyberattaques.

[228] Article 312-1 du Code Pénal.

[229] Articles 323-1 et suivants du Code Pénal.

[230] *Règles Juridiques de la cybersécurité*, MOOC Défis et enjeux de la cybersécurité, fun-mooc.fr.

### B) … suscitant un sentiment de justice de la part des victimes des cyberattaques

Dans un contexte de développement rapide du secteur de l'e-santé pour relever les défis sanitaires et humains, sécuriser les données personnelles de santé apparaît indispensable. Cette sécurisation des informations confidentielles est une étape incontournable pour éviter toute défiance des citoyens dans les outils et services innovants[231]. De plus, la confiance envers le numérique en santé est établie seulement si plusieurs principes sont respectés. Ces principes éthiques sont ceux de bienfaisance, d'autonomie, de non malfaisance et de justice[232]. Ces derniers sont d'autant plus importants pour maintenir un lien de confiance entre les usagers du système de santé français et les EPS. La conservation de ce lien a fait l'objet d'une campagne nationale présentée dans un communiqué ministériel de presse en octobre 2020[233]. Cette campagne avait pour ambition de mettre en exergue les bénéfices de l'usage du numérique en santé, respectueux des droits des usagers et des bonnes pratiques des professionnels. En plus de ces sanctions en matière de cybercriminalité, il est indispensable qu'un combat soit mené contre les atteintes à la sécurité numérique des SIH.

## <u>Paragraphe II</u> : L'indispensable combat contre les atteintes à la sécurité numérique des SIH

Les condamnations peuvent être des moyens de dissuasion (A) dans une perspective de lutte contre un phénomène exponentiel (B).

### A) Les condamnations, moyens de dissuasion…

Le maintien de la confiance des usagers du système de santé français envers la protection de leurs données personnelles de santé engage nécessairement l'implication de la justice. Une section cybercriminalité du Parquet de Paris a été spécialement créée à cet effet. 148 procédures pour attaques via des rançongiciels ont été ouvertes en 2019 et 436 en 2020. En plus de cette section, la Commission supérieure du Numérique et des Postes (CSNP)

---

231 GAVANON (Isabelle) et LE MAREC (Valentin), « Fuite massive de données personnelles de santé », *Dalloz actualité*, 17 mars 2021.

232 KERMARREC (Jean-Michel), « La judiciarisation de l'usage numérique en santé…un risque émergent », *Revue Droit et Santé,* n°88, mars 2019, page 238.

233 *Pour ma santé, je dis oui au numérique*, communiqué de presse du Ministère des Solidarités et de la Santé, par sa délégation ministérielle au Numérique en Santé, octobre 2020.

recommande la création d'un Parquet national du numérique pour les infractions de cybercriminalité complexes[234].

Par ailleurs, grâce à la coopération internationale, des affaires comme *Emotet* ou *Egregor* ont pu aboutir. Cette coopération policière et judiciaire internationale est primordiale en matière de cybersécurité. Grâce à cette coopération, des réseaux peuvent être démantelés et l'interpellation des cybercriminels en est facilitée. Par exemple, dans l'affaire *Egregor*, le rançongiciel propagé est à l'origine des cyberattaques survenues au CHU de Dax (Landes) et Villefranche-sur-Saône (Rhône). Le réseau de cybermalveillance a pu être démantelé début 2021 grâce à l'action conjointe des autorités ukrainiennes, françaises et américaines. Cette affaire démontre l'importance des pays à mutualiser leurs informations ainsi que leurs moyens pour recouper les informations et donc, retrouver les cybercriminels.

En conséquence, les condamnations sont des moyens de dissuasion qui se doivent d'être prononcées, surtout dans un contexte de constante progression de la menace cyber.

### B) … dans une perspective de lutte contre un phénomène exponentiel

En France, une véritable lutte est progressivement menée pour atteindre une sécurité numérique appropriée. Cette lutte s'intensifie contre la cybercriminalité et les potentielles failles numériques. Une véritable prise de conscience sur le nécessaire encadrement du traitement des données personnelles s'opère. Par exemple, dans le contexte actuel de pandémie, le Conseil d'Etat a rendu une ordonnance statuant sur le stockage des données de santé par la plateforme de Microsoft, *Health Data Hub*[235]. Depuis 2018, cette plateforme recueille les données de santé des personnes soignées en France (hôpitaux, laboratoires, médecine de ville). Le Conseil d'Etat, du fait de l'utilité de la plateforme en temps de crise sanitaire, refuse de suspendre son fonctionnement mais demande des mesures complémentaires de protection des données personnelles de santé pour une solution plus pérenne.

---

[234] Avis n°2021-03 du 29 avril 2021 portant recommandations dans le domaine de la sécurité numérique, Commission supérieure du numérique et des postes.

[235] Ordonnance du 13 octobre 2020, n°44937, *Association Le Conseil National du logiciel Libre et Autre,* Conseil d'Etat statuant au contentieux.

# CONCLUSION GÉNÉRALE

La recrudescence des actes de cybermalveillance à l'encontre des établissements publics de santé démontre l'importance de la protection des données de santé à caractère personnel. Phénomène mondial, le caractère entre autre lucratif de cette « *piraterie moderne* » à distance et l'aspect incontournable de l'informatisation laissent envisager que la menace cybercriminelle perdure et que les auteurs utiliseront tous les stratagèmes pour réussir. Les EPS semblent donc condamnés à devoir renforcer, sans attendre, leur sécurité numérique. L'urgence d'une stratégie de défense est plus que réelle face à cette menace persistante.

Cette stratégie de défense implique nécessairement une approche globale avec, certes, des moyens financiers, mais surtout l'action commune de tous les acteurs concernés, autant nationaux qu'internationaux. La sécurité numérique n'est pas seulement du ressort des techniciens informatiques, mais de chacun des acteurs impliqués dans l'environnement numérique d'un EPS. Chacun doit prendre conscience de la récurrence et de l'impact de telles attaques sur les EPS. Cette prise de conscience collective passe inexorablement par une coopération à tous les échelons, l'assimilation de bonnes pratiques ainsi que la création d'une culture permanente de gestion du risque et de la sûreté afin que chacun s'implique pleinement.

La prévention est plus jamais une étape importante dans l'instauration d'une sécurité numérique efficiente. Sensibiliser, accompagner et former aux usages numériques devraient être effectués dès les premiers contacts avec les outils numériques. Ce principe de précaution doit être appliqué envers tous les utilisateurs des SIH, pour que chacun fasse preuve de bon sens et d'une paranoïa « *polie* ». Toutes ces actions de prévention permettront de préserver, à terme, le fonctionnement des EPS français. Une fois, la prévention effectuée, en cas de cyberattaque, une action de répression doit obligatoirement être mise en oeuvre pour tenter d'enrayer ces actes de cybermalveillance.

Réagir pour sécuriser numériquement les EPS et les données de santé à caractère personnel qui y sont traitées est plus que jamais un enjeu actuel à ne pas négliger où chacun a un rôle à jouer.

# TABLE DES MATIÈRES

# BIBLIOGRAPHIE


Ouvrages

- Ouvrages généraux

- LAMI (Arnaud) et VIOUJAS (Vincent), *Droit Hospitalier,* 2ème édition, 2020, 579 pages
- SAISON (Johanne) avec la collaboration de MONTERO (Antoine), *Droit hospitalier*, Fonction publique Hospitalière, 4ème édition, 2019, 345 pages

- Ouvrages spéciaux

- ARPAGIAN (Nicolas), *La cybersécurité*, Que sais-je ?, n°3891, Presses Universitaires de France/Humensis, mai 2018, 128 pages
- FEVRIER (Rémy), V*ers une nécessaire évolution du paradigme dominant en management stratégique ?*, Covid-19 et cyberattaques, Revue Française de Gestion 2020/8 (n°293), 238 pages
- CARTAU (Cédric)*, La sécurité du système d'information des établissements de santé*, Presses de l'EHESP, 2018, 336 pages
- CHOPIN (Frédérique), *Cybercriminalité*, Répertoire de droit pénal et de procédure pénale Dalloz, janvier 2020, 497 pages
- QUILLIOU-RIOUAL (Mikael), QUILLIOU-RIOUAL (Morgane), *Communication professionnelle et travail en équipe pluridisciplinaire en ESSMS*, collection Aide Mémoire, éditeur Dunod, 2020, 462 pages
- MONNERIE (Nils), *Les défis de la commercialisation des données après le RGPD : aspects concurrentiels d'un marché en développement,* Revue Internationale de Droit Economique 2018/4, avril 2018, 515 pages
- RAIMONDO (Laurane), *La protection des données personnelles, 100 Questions/Réponses, Pour comprendre et mieux se protéger*, janvier 2021, 329 pages
- ROBIN (Jean-Yves), *L'urgence numérique, Faire de la France un leader de l'e-santé*, 2014, 216 pages
- SAVATIER (René), *Les Métamorphoses économiques et sociales du droit privé d'aujourd'hui*, Dalloz, 1959, 340 pages
- SFEIR (Antoine), *La santé est un devoir régalien de l'Etat, pas un pouvoir*, dans les Tribunes de la Santé 2011/4 (n°33), Presses de Science Po, 120 pages
- VENNE (Jean-François), *Les établissements des réseaux de la santé dans la mire des pirates*, dans Gestion 2019/3 (Volume 44), 116 pages

Rapports

- JÉGOU (Jean-Jacques), *Rapport d'information sur l'informatisation dans le secteur de la santé,* Sénat, 2005, n°62, 65 pages
- *L'impact des restrictions à l'entrée, au séjour et à la résidence liées au VIH : témoignages personnels*, Programme Commun des Nations Unies sur le VIH/sida, ONUSIDA, mai 2009, 22 pages
- *Etat des lieux des systèmes d'information hospitaliers*, Atlas des SIH, Direction Générale de l'Offre de Soins (DGOS), mai 2015, 125 pages
- *Stratégie nationale pour la sécurité du numérique*, 16 octobre 2015, 44 pages
- *La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer*, Cour des Comptes, Rapport sur l'Application des Lois de Financement de la Sécurité Sociale (RALFSS) 2016, 349 pages
- *Rapport sur l'application des lois de financement de la Sécurité Sociale*, Cour des Comptes, septembre 2016, 712 pages
- *Les services publics numériques en santé : des avancées à amplifier, une cohérence à organiser*, Rapport public annuel 2018, Cour des Comptes, février 2018, 521 pages
- *Donner un sens à l'intelligence artificielle pour une stratégie nationale et européenne,* mission parlementaire confiée par le Premier Ministre Edouard Philippe du 8 septembre 2017 au 8 mars 2018, mars 2018, 234 pages
- *Etat des lieux des systèmes d'information hospitaliers*, Atlas des SIH, Direction Générale de l'Offre de Soins (DGOS), 15 mai 2018, 131 pages
- *E-santé : augmentons la dose !*, Institut Montaigne, Rapport Juin 2020, 218 pages
- *Attaques par rançongiciels, tous concernées, Comment les anticiper et réagir en cas d'incident ?*, guide de sensibilisation de l'ANSSI en partenariat avec la DACG du Ministère de la Justice, août 2020
- *Rapport au nom de la commission d'enquête pour l'évaluation des politiques publiques face aux grandes pandémies à la lumière de la crise sanitaire de la Covid-19 et de sa gestion*, remis à M. le Président du Sénat le 8 décembre 2020, Session ordinaire de 2020-2021
- *Compte rendu intégral, séance du mercredi 17 février 2021 (63ème jour de séance de la session),* Session ordinaire de 2020-2021, Sénat, Journal Officiel de la République Française, 1241 pages

Textes

*Droit de l'UE*

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (dit Règlement Général sur la Protection des Données), entré en vigueur le 25 mai 2018.
- Convention Européenne des Droits de l'Homme, aussi appelée Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Conseil de l'Europe, 1950

*Droit interne*

Lois

- Loi n° 78-17 du 6 janvier 1978 modifiée par la loi n° 2018-493 du 20 juin 2018
- Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique, *JORF*, 6 janvier 1988
- Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, *JORF*, 5 mars 2002
- Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* n °182, 7 août 2004
- Loi n°2005-493 du 19 mai 2005 autorisant l'approbation de la Convention sur la cybercriminalité et du protocole additionnel à cette Convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, *JORF*, n°116, 20 mai 2005, texte n°2
- Loi n°2005-1550 du 12 décembre 2005 modifiant diverses dispositions relatives à la défense (1), *JORF* n°289, 13 décembre 2005
- Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, *JORF* n°0167, 22 juillet 2009
- Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, *JORF* n°0062, 15 mai 2011
- Loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022, 27 janvier 2016
- Loi n°2021-502 du 26 avril 2021 visant à améliorer le système de santé par la confiance et la simplification, *JORF* n°0099, 27 avril 2021

Ordonnances

- Ordonnance n°2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel (article 1)
- Ordonnance du 13 octobre 2020, n°44937, Association Le Conseil National du logiciel Libre et Autre, Conseil d'Etat statuant au contentieux
- Ordonnance n°2020-1407 du 18 novembre 2020 relative aux missions des agences régionales de santé (article 1), *JORF* n°0280, 19 novembre 2020
- Ordonnance n°2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie, *JORF* n°0111, 13 mai 2021

Décrets

- Décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale, *JORF* n°47, 24 février 2006
- Décret n°2009-934 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence Nationale de la Sécurité des Systèmes d'Information », *JORF* n°0156, 8 juillet 2009
- Décret n°2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information, *JORF* n°0214, 14 septembre 2016
- Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé », *JORF* n°0301, 28 décembre 2016
- Décret n'°2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel, *JORF* n°0049, 28 février 2018
- Décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, *JORF* n°0118, 25 mai 2018
- Décret n°2019-1412 du 20 décembre 2019 portant diverses dispositions relatives à l'administration centrale des ministères chargés des affaires sociales, *JORF* n°0296, 21 décembre 2019, texte n°17

Arrêtés

- Arrêté du 13 décembre 2016 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle des ministères chargés des affaires sociales, *JORF* n°0294, 18 décembre 2016
- Arrêté du 4 septembre 2017 portant création d'un comité de maîtrise des risques numériques au sein du comité stratégique de maîtrise des risques des ministères chargés des affaires sociales, *JORF* n°0216, 15 septembre 2017
- Arrêté du 19 décembre 2019 portant approbation d'un avenant modifiant la convention constitutive du groupement d'intérêt public « Agence nationale des systèmes d'information partagés de santé », *JORF* n°0295, 20 décembre 2019

Délibérations

- Délibération n° 2016-316 du 13 octobre 2016 portant avis sur un projet de décret en Conseil d'Etat relatif au Système national des données de santé (demande d'avis n° 16018114), *JORF* n°0301, 28 décembre 2016
- Délibération n° 2017-022 du 26 janvier 2017 portant avis sur un projet d'arrêté relatif au référentiel de sécurité applicable au Système national des données de santé (demande d'avis n° 16025310), *JORF* n°0071, 24 mars 2017
- Délibération 2018-289 du 12 septembre 2018 autorisant la société IQVIA Opérations France à mettre en oeuvre un traitement automatisé de données à caractère personnel ayant pour finalité la constitution d'un entrepôt de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, dénommé base de données LRX (n°2120812), Commission Nationale de l'Informatique et des Libertés

Jurisprudence

- Chambre Criminelle de la Cour de Cassation : Watelet du 19 décembre 1885 et Degraene du 8 mai 1947
- Conseil d'Etat : Deve du 12 avril 1957
- CEDH : Z c. Finlande, 1997, § 96 ; C.C. c. Espagne, 2009, § 33 ; P. et S. c. Pologne, 2012, § 128 ; Avilkina et autres c. Russie, 2013, § 45 ; Y. c. Turquie (déc.), 2015, § 65
- CJUE : *Affaire C-311/18, Data Protection Commissionner contre Maximillian Schrems et Facebook Ireland Ltd*, 16 juillet 2020

Revues

• ANSSI

- « Papiers numériques », *Revue annuelle de l'ANSSI*, édition 2020, 58 pages

• Dalloz

- BERGOIGNAN-ESPER (Claudine), *L'hôpital public au sein du plan « Ma santé 2022 »*, *RDSS 2019*, page 15
- BERTHELET (Pierre), *Revue de Science criminelle et de droit pénal comparé 2018/1 n°1*, Dalloz, janvier 2018, 328 pages
- DOUVILLE (Thibault), « L'émergence d'un droit commun de la cybersécurité », *Recueil Dalloz 2017*, page 2296
- GAVANON (Isabelle) et LE MAREC (Valentin), « Fuite massive des données personnelles de santé », *Dalloz actualité,* 17 mars 2021
- KERMARREC (Jean-Michel), *Revue Droit et Santé n°88*, mars 2019, pages 238 à 239
- QUEMENER (Myriam), *«* Cybersécurité et protection des données de santé », Avocat général près de la Cour d'Appel de Paris, *Dalloz IP/IT*, 20 mai 2020, pages 303 à 306

• Politique étrangère

- GAUTIER (Louis), « Cyber : les enjeux pour la défense et la sécurité des Français », *Politique étrangère 2018/2 (Été)*, pages 29 à 42

• HAL

- ADEYOOLA Hassan, *Advanced Persistent Threat : Detection and Defence*, Bachelor in Science University of Bradford, 15 July 2021, 5 pages

Articles de presse

- *GHT, RGPD et cybersécurité : les informaticiens hospitaliers "débordés" par le réglementaire - TIC santé*, 24 janvier 2018
- *5G, la course à quoi ?,* Le monde diplomatique, François Ruffin et Cyril Poireaux, octobre 2020
- BERKAOUI (Héléna), *Cyberattaque : « Il y a une explosion de la grande criminalité », rapporte le directeur de l'Anssi*, Public Sénat, 4 novembre 2020
- *C'est quoi un Trojan et comment s'en protéger ?,* ML/ACTU, 9 novembre 2020

- ZIRAR (Wassinia) , Talents de l'e-santé : 11 lauréats, dont plusieurs établissements, pour cette première édition, E-santé, 11 décembre 2020, ticsante.com
- *Finlande : une cyberattaque contre un hôpital psychiatrique choque le pays*, 21 décembre 2020, 20minutes.fr
- TRELY (Vincent), Interview exclusive de Charlotte DRAPEAU, chef du Bureau Santé et Société de l'ANSSI, 16 juin 2021, apssis.com

*Hospimedia*

- DEBACKER (Perrine), « Les structures de santé pourront commander des audits de cybersécurité via une interface », Système d'information, 6 octobre 2020
- GOESSAERT (Antoine), « Verso Healthcare mesure et rappelle l'importance de la cybersécurité face aux attaques », Système d'information, 22 avril 2021
- RABEUX (Cécile), « Le secteur médico-social est encore vulnérable face aux cyberattaques », Systèmes d'information, 23 août 2020
- ROBILLARD (Jérôme), « L'Agence européenne du médicament est visée par une cyberattaque », Système d'information, 10 décembre 2020
- TRIBAULT (Géraldine), « La santé est presque arrivée au niveau de sécurité auquel elle devrait être », 4 novembre 2020
- QUÉGUINER (Thomas), « La cyberattaque par rançongiciel à Dax illustre l'explosion de cette menace sur l'hôpital », Bloc note sanitaire, 12 février 2021

Etudes

- *Santé mobile et connectée : usages, attitudes et attentes des malades chroniques*, Enquête Le Lac e-santé, juin 2015
- *Convergence SI et GHT : 2018, le temps des schémas directeurs,* APMnews et TICsanté, 2017, 8 pages
- S*tructures de santé : pourquoi déclarer ses incidents SI ? ACSS, 18 mois après, HIT 2019*, ASIP santé et Haut Fonctionnaire de défense et de sécurité (HFDS), 22 mai 2019, 34 pages
- *L'excellence cybersécurité dans Rennes Métropole*, Territoire de Confiance, novembre 2019, Observatoire Economie
- *Cyberthreat Handbook*, Thales et Verint, octobre 2019
- *Baromètre de la confiance des Français dans le numérique*, synthèse des résultats, 8ème édition, ACSEL, février 2021, 31 pages

- *Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé*, rapport public 2020, ANS, Ministère des Solidarités et de la Santé, avril 2021, 43 pages

Statistiques

- *Personnels et équipements de santé*, Tableaux de l'économie française, INSEE, 27 février 2020, édition 2020

Communiqués de presse

- *La Cour invalide la décision 2016/1250 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis*, Cour de Justice de l'Union Européenne, n°91/20, Luxembourg, 16 juillet 2020, 4 pages
- *Pour ma santé, je dis oui au numérique*, communiqué de presse du Ministère des Solidarités et de la Santé, par sa délégation ministérielle au Numérique en Santé, octobre 2020
- *Sécurité des réseaux informatiques des établissements de santé : le Gouvernement renforce sa stratégie*, 22 février 2021 sur le site du Ministère des Solidarités et de la Santé
- *L'OMS publie le premier rapport mondial sur l'intelligence artificielle (IA) appliquée à la santé et six principes directeurs relatifs à sa conception et à son utilisation,* communiqué de presse, 28 juin 2021

Mémentos

- *Guide pour réaliser un plan de continuité d'activité*, SGDSN, édition 2013, 76 pages
- *Mémento à l'usage du directeur d'établissement de santé - Connaître vos risques pour mieux y faire face,* Cybersécurité, édition 2017 - DGOS, 39 pages
- *Règlement européen sur la protection des données personnelles se préparer en 6 étapes,* Règlement Européen, CNIL, 2018, 8 pages
- *Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident ?*, guide, ANSSI, août 2020, 38 pages
- *Foire aux questions : système d'information de dépistage, Santé Publique France*, 8 décembre 2020, 9 pages

Sites Internet

- Site de l' Agence du Numérique en Santé : https://esante.gouv.fr/securite/cybersecurite ; https://esante.gouv.fr/virage-numerique/feuille-de-route consulté le 17 janvier 2021
- Site de l'ANSSI, glossaire en ligne, consulté le 12 décembre 2020 et FAQ - Opérateurs de services essentiels consulté le 8 juin 2021
- Site de l'APHP, aphp.fr, consulté le 11 mars 2021
- Site de auvergne-rhone-alpes.ars.sante.fr, consulté le 5 mai 2021
- Site de la cnil.fr, glossaire de la CNIL : https://www.cnil.fr/fr/glossaire consulté le 11 septembre 2020 et *Enquête sur l'entrepôt de données santé IQVIA : la CNIL rappelle les conditions et cadre légal ayant permis son autorisation en 2018* (17 mai 2021) consulté le 20 mai 2021
- Site de la Commission Européenne (ec.europa.eu*), Stratégie européenne pour les données, Une Europe adaptée à l'ère numérique*, consulté le 9 mai 2021
- Site du Conseil de l'Europe, Convention sur la cybercriminalité, 23 novembre 2011 : https://rm.coe.int/168008156d consulté le 24 décembre 2020
- Site du gouvernement.fr, *Fiche d'information relative au RGPD et son application*, juin 2018 consulté le 14 février 2021
- Site du Ministère des Solidarités et de la Santé : https://solidarites-sante.gouv.fr/ consulté le 3 mars 2021
- Site de l'Usine Digitale, VITARD (Alice), *Ransomware, Covid-19, espionnage, terrorisme… L'ANSSI fait un état des lieux de la cybersécurité*, 5 novembre 2020 consulté le 5 mars 2021

Vidéos

- *Dans la peau d'un expert en cybersécurité (ft Master Geopolitix)*, Justin Izu, 30 août 2018, sur youtube.com
- *Dans la peau d'un expert en cybersécurité,* Master Geopolitix, 30 août 2018, sur youtube.com
- *Table ronde sur « La cybersécurité des ETI-PME-TPE : la réponse des pouvoirs publics »*, Délégation aux entreprises, Sénat, jeudi 15 avril 2021

Conférences

- *Numérique et santé (intelligence artificielle, données de santé, Big Data),* Cour de Cassation, jeudi 16 mai 2019, sous la direction scientifique de Mmes Bénédicte BOYER-BÉVIÈRE, Astrid MARAIS et Dorothée DIBIE
- *Renoncement et accès aux soins. De la recherche à l'action*, Cinq années de collaboration entre l'Assurance Maladie et l'Observatoire des non-recours aux droits et services (Odenore), actes synthétiques du colloque des 6 et 7 juin 2019, Paris, Cité des Sciences et de l'Industrie, 2020, 54 pages
- *La sécurité des données personnelles*, 17 mai 2021, animée par Laurane Raimondo, chercheuse associée (cyberdéfense, espace exo-atmosphérique et données personnelles) au sein du Centre Lyonnais d'Etudes de Sécurité Internationale et de Défense, et Sana Bakfalouni, co-fondatrice d'AKANT, experte en sécurité de l'information, Lyon - Disrupt Campus / Université de Lyon
- *Les établissements publics de santé : sécurité et défense,* 20 mai 2021, tenue sous l'égide de LEJEP et AFDSD, avec le soutien de l'AFDS, coordonnée par le professeur Pierre BOURDON, membre du LEJEP du CY Cergy Paris Université et membre de l'AFDSD

Films

- *The Great Hack*, documentaire réalisée par Karim Amer et Jeanne Noujaim, 2019

MOOCs

- *Défis et enjeux de la cybersécurité*, ANSSI effectué en mai 2021
- *Défis et enjeux de la cybersécurité*, fun-mooc.fr effectué en juin-juillet 2021