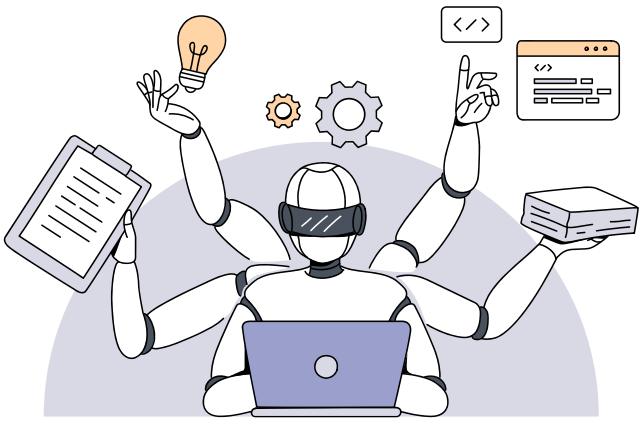
L'intelligence artificielle et la cybersécurité : un duo ambivalent

Illustration dans le secteur de la santé

Cécile Théard-Jallu, Avocate associée, De Gaulle Fleurance
avec l'aide de Leïla Said Cherif

>> Dans un contexte de cyberattaques quasi quotidiennes où les acteurs de santé sont particulièrement visés, la cybersécurité tantôt s'appuie sur l'IA, tantôt la combat. Ce duo ambivalent est appréhendé par un arsenal juridique de plus en plus sophistiqué au niveau français et européen tandis que les autorités proposent des dispositifs concrets pour aider les organisations à se protéger. Voici un aperçu des enjeux et des avancées dans ce domaine.

Chaque année, près d'un milliard de personnes dans le monde sont touchées par une cyberattaque[1]. Le secteur hospitalier français est particulièrement affecté par ce phénomène : comme l'indique le journal La Tribune, les hôpitaux français traversent une véritable « tempête cyber »[2] comme le montrent les attaques emblématiques des hôpitaux de Versailles et Corbeille Essonne en 2022, de Vittel, de Neufchâteau, de l'AP-HP, AP-HM et CHU de Lyon en 2023[3] ou encore d'Armentières en février 2024 [4], avec des conséquences redoutables (urgences fermées, services interrompus ou ralentis, millions de dossiers de patients piratés, etc.). Cela n'a rien de surprenant, quand l'on sait la manne que représentent les données de santé sur le *dark web*[5]. Ce constat oblige à s'interroger sur la sécurité et la circulation des données de santé, et les moyens mis en œuvre par les acteurs de ce secteur pour y faire face.



Si cette problématique n'est pas récente, l'intelligence artificielle (IA) joue ces dernières années un nouveau rôle : selon l'usage qui en est fait, elle peut contribuer soit à l'attaque (cyberattaque), soit à la défense (cybersécurité) dans le cyberespace. Le Professeur Michel Séjean a d'ailleurs souligné une certaine relation d'interdépendance : ainsi, pour que l'IA contribue à la cybersécurité, elle doit d'abord elle-même être un outil sûr, et donc en "situation de cybersécurité"[6]. C'est là tout l'enjeu de la règlementer. L'IA peut ainsi contribuer à la sécurité dans le cyberespace en renforçant les outils et les processus. Elle est aujourd'hui largement utilisée dans des systèmes de pares-feux, ou des logiciels afin d'accélérer et de simplifier la détection des menaces. Par exemple, les solutions traditionnelles de machine learning ou de réseaux neuronaux sont exploitées non seulement pour permettre une analyse rapide d'un volume important de données, mais également pour remédier aux attaques en générant un correctif de défense et de sécurisation des systèmes par la mise en place de logiciels de sécurité[7]. L'IA offre un gain de temps significatif en différenciant les vraies cyberattaques des « faux positifs de cyberattaques » (par exemple, un employé en télétravail entrant plusieurs fois un mot de passe erroné) : ce travail peut nécessiter un traitement de données gigantesque ainsi qu'une rapidité qu'aucun être humain n'est capable d'atteindre[8]. L'IA peut ainsi améliorer la capacité et l'optimisation des ressources des organisations, qu'elles soient publiques ou privées et notamment celles qui ont l'obligation d'un plan de cybersécurité robuste. Il s'agit plus particulièrement d'acteurs dont l'activité est considérée comme d'importance vitale (alors qualifiés d'opérateurs d'importance vitale ou « OIV ») ou comme un service essentiel (qualifiés alors d'opérateurs de service essentiel ou « OSE ») (cf. infra).

En revanche, lorsqu'elle est utilisée avec une intention malveillante, l'IA peut agir au détriment de la cybersécurité, en permettant la mise en place de stratégies plus sophistiquées et donc plus difficiles à contrer. Par exemple, l'utilisation de *deep fakes*[9], de modèles de courriers de phishing adaptés à chaque destinataire, ou encore de techniques d'apprentissage par renforcement sont des applications très répandues. Ce revers de l'avancée technologique qu'est l'IA est d'ailleurs une des principales préoccupations de l'AI Act, en particulier pour les IA à haut risque, qui se voient imposer des obligations particulières notamment en cybersécurité[10].

Les fuites de données constituent par ailleurs une perte importante de ressources (ainsi, leur coût moyen pour les organisations s'élevait à 4,45 millions de dollars en 2023[11]).

Ces différentes attaques mettent en lumière les nombreuses lacunes affectant les acteurs de santé, et tout

particulièrement du soin, en matière de cybersécurité. Ainsi, selon le rapport de l'ENISA (l'Agence européenne de sécurité des systèmes d'informations), ce sont 73% des organisations de la santé qui ne disposent d'aucun programme de protection contre les rançongiciels, 40% qui ne possèdent pas de programme de sensibilisation à la sécurité pour leur personnel et 46% qui n'ont jamais effectué d'analyse des risques informatiques[12].

C'est pourquoi les droits français et européen, s'attachent à mettre en place une règlementation de plus en plus précise et harmonisée pour à la fois renforcer la sécurité dans le cyberespace et encadrer efficacement l'IA (I). Il est d'ailleurs intéressant de constater que les règlementations parallèles concernant la cybersécurité et l'IA se croisent, s'influencent, et se complètent (II). Enfin, préserver la cybersécurité est un véritable défi dans un monde qui ne cesse de se digitaliser : en conséquence, nombreuses sont les autorités compétentes qui proposent des solutions concrètes (III).

I. Le cadre juridique en place et à venir

Ces dernières années, les textes adoptés en matière de cybersécurité et d'IA se sont multipliés. Ils s'inscrivent globalement dans la stratégie de souveraineté numérique de l'Union européenne reposant sur trois principes : 1) améliorer l'accès aux biens et services numériques sur l'ensemble du territoire ; 2) mettre en place des conditions optimales pour le développement de réseaux numériques et de services innovants ; et 3) accroître le potentiel de croissance de l'économie numérique[13]. Dans ce cadre, il est essentiel pour le marché européen, à la fois de renforcer la cybersécurité pour assurer la protection des données et des infrastructures critiques et de soutenir l'innovation, tout en réduisant au maximum les risques de ses dérives.

Arsenal législatif en place

Au sein d'un véritable arsenal de textes adoptés ou en cours d'adoption par l'Union européenne, que ce soit en matière de cybersécurité ou d'IA, les directives NIS I de juillet 2016[14] et NIS II de décembre 2022[16 17] (sur la sécurité des réseaux et des systèmes d'information) s'inscrivent dans une démarche européenne commune sur la cybersécurité (la seconde directive venant compléter et renforcer les avancées de la première).

Ainsi, la directive NIS 1, transposée en droit interne en février 2018, prévoyait déjà des mesures pour lutter contre l'insécurité dans le cyberespace telles que la notification systématique des incidents de sécurité pour les opérateurs de services essentiels (OSE[15]) (dont font partie un certain nombre d'acteurs de santé tels que des centres hospitaliers[18]), et les fournisseurs de services numériques (FSN), ou encore la mise en place d'autorités nationales compétentes et la coopération entre les Etats membres.

La directive NIS 2, devant être transposée au plus tard en octobre 2024, vient largement étendre le champ d'application initial de cette règlementation[19]. Adoptée en décembre 2022, elle introduit de nouvelles obligations, et ce, pour un spectre d'entités plus large (désormais entités essentielles (EE) ou importantes (EI)), incluant notamment les administrations publiques, les télécommunications et les plateformes de réseaux sociaux. Elle prévoit à la fois des mesures minimales de gestion des risques tels que l'établissement d'une politique interne de sécurité et de gestion des incidents ou encore la mise en place d'audits réguliers, et des mesures de gestion des incidents de sécurité, et de sécurité des chaînes d'approvisionnement. NIS 2 renforce également la coopération entre Etats membres pour la gestion des crises de cybersécurité en apportant un cadre formel au réseau CyCLONe (Cyber Crisis Liaison Organisation Network) qui rassemble l'ANSSI (Agence nationale de la sécurité des systèmes d'information) française et ses homologues européens[20].

Pour assurer l'application de ces règles, l'ENISA fournit des conseils pratiques et des recommandations aux Etats membres et aux institutions et coordonne leurs actions. Le règlement européen *Cybersecurity Act* du 7 juin 2019[21] vient renforcer son rôle en lui conférant un mandat élargi pour fournir une réponse coordonnée face aux cyberattaques et promouvoir les bonnes pratiques. Il établit également un cadre européen de certification de la cybersécurité.

En droit interne, des règles de cybersécurité relevant du Code de la défense, viennent protéger les secteurs d'activité d'importance vitale (SAIV) et responsabiliser les OIV contre les actes malveillants (terrorisme, sabotage, cyberattaque) et les risques naturels, technologiques, sanitaires… Ces opérateurs identifiés par les différents ministères de tutelle sont désignés par arrêté. Là encore, de nombreux hôpitaux, notamment, en font partie[22]. Le régime existe depuis 2006 mais pour faire face à l'augmentation en quantité et en sophistication des attaques informatiques, l'article 22 de la loi de programmation militaire de 2013 est venu compléter ce dispositif en imposant aux OIV le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent : les systèmes d'information d'importance vitale (SIIV). Une série de dispositions sont prévues sur la sécurité des systèmes d'information, notamment sur la prévention, la détection et la réponse aux cyberattaques.

Dans ce cadre, l'ANSSI a pour double mission d'accompagner les OIV dans la sécurisation de leurs systèmes d'information critiques et de contrôler, en tant qu'autorité nationale, le respect de ce cadre réglementaire précurseur en matière de réponse à la cybermenace.

Afin de contribuer à cette cybersécurité, l'IA peut être intégrée dans une stratégie de défense pour renforcer la détection des menaces, l'analyse des vulnérabilités et la mise en place de mesures adaptées. La récente loi du 1er août 2023 *relative à la programmation militaire pour les années 2024 à 2030* comporte d'ailleurs un volet consacré à la cybersécurité dans lequel sont prévues des nouvelles dispositions permettant à l'ANSSI d'augmenter sa connaissance des modes opératoires des cyberattaquants, de mieux leur faire face, et d'alerter de façon plus efficace les victimes des incidents de sécurité ou des menaces.

Dans la lutte contre l'insécurité dans le cyberespace, le très attendu AI Act voté par le Parlement européen le 13 mars 2024, est la première règlementation à l'échelle internationale sur l'intelligence artificielle. Il établit des obligations spécifiques en fonction des différentes catégories de risques des systèmes d'IA. Ces obligations sont principalement à destination des fournisseurs de systèmes, mais également des utilisateurs et sont plus nombreuses et contraignantes pour les IA à haut risque : par exemple, avant d'introduire un tel système d'IA sur le marché de l'Union européenne, les fournisseurs doivent le soumettre à une évaluation de conformité aux exigences obligatoires pour une IA fiable[23]. S'imposera également à eux une obligation de contrôle humain tout au long du cycle de vie de l'IA[24].

… et à venir

D'autres règlementations sont en cours de discussion, venant consolider les textes déjà en vigueur en cherchant, encore une fois, à soutenir l'innovation tout en la sécurisant. Ainsi, par exemple, un règlement sur l'espace européen des données de santé est en cours de négociation au sein du Parlement européen[25]. Il permettra, dès son adoption, l'accès et le partage des données de santé pour un usage à la fois primaire et secondaire, la mutualisation des bases de données, et un espace commun au sein duquel les personnes physiques pourront aisément contrôler leurs données de santé. Le but de ce nouveau système est d'améliorer le fonctionnement du marché intérieur pour le développement, la communication et l'utilisation des dossiers médicaux électroniques. Une telle circulation des données de santé à l'échelle de l'Union et la recherche d'harmonisation sous-jacente des protocoles d'échanges de données devront à la fois s'inscrire dans le renforcement de la cybersécurité et y contribuer, en permettant une meilleure surveillance et une mise en œuvre plus efficace d'une politique européenne commune de partage des données dans le cyberespace. En revanche, le Comité européen de la protection des données (CEPD) a émis des réserves[26] quant à l'adoption de ce texte en l'état, notamment au regard du règlement général sur la protection des données (RGPD)[27]. En effet, un tel dispositif concernerait environ 500 millions de citoyens européens, ce qui représente une vaste quantité de données à traiter en cohérence avec cet autre texte. C'est pourquoi le législateur européen est invité à y renforcer les garanties quant à la protection des données personnelles.

L'usage de l'IA dans les cyberattaques pose également des questions de responsabilité : l'on peut par exemple s'interroger sur la chaine de responsabilité à la suite du décès d'un patient n'ayant pas pu bénéficier d'une opération vitale en raison d'une cyberattaque[28]. Là encore, le législateur européen a cherché à harmoniser les règles nationales en matière de responsabilité applicables à l'IA pour permettre aux victimes de dommages d'obtenir plus facilement réparation[29]. Ainsi, elles disposeront par exemple d'un droit d'accès aux preuves auprès des fournisseurs ou des entreprises en cas d'utilisation d'un système d'IA à haut risque.

Finalement, une certaine interdépendance se dessine entre les différentes règlementations sur l'IA et la cybersécurité.

II. Des règlementations convergentes et complémentaires

A l'ère d'une numérisation croissante des secteurs d'activités, règlementer la cybersécurité au niveau interne et communautaire ne peut se faire sans une règlementation concomitante de l'IA. Et nécessairement, encadrer les systèmes d'IA exige la prise en compte systématique des potentiels abus qui peuvent en découler, notamment dans des cyberattaques.

La nécessité de combattre une cybermenace de plus en plus accrue

La menace cyber est devenue telle qu'aujourd'hui, elle se professionnalise et atteint un niveau d'organisation internationale, et ce en partie en raison de l'IA : c'est notamment le constat de la CNIL, qui en fait l'un de ses principaux chantiers pour 2024[30]. C'est également le cas de l'ENISA, qui dans un rapport de mars 2023, examine le rôle de la normalisation dans l'intégration et l'application des aspects de cybersécurité dans l'AI Act[31].

Un objectif commun de renforcement de la sécurité

Ces deux corpus de règles s'inscrivent dans une même logique de renforcement de la sécurité technologique et plus largement de la stratégie de souveraineté numérique commune de l'Union, comme évoqué ci-dessus. En revanche, il n'existe pas de disposition juridique spécifique à la cybersécurité de l'IA ou à la cybersécurité par l'IA[32]. A ce stade, ces deux matières évoluent en parallèle tout en se référant l'une à l'autre explicitement ou non. Pourtant, l'on pourrait imaginer une règlementation couvrant les deux et leurs enjeux communs.

En attendant, l'on peut espérer que l'entrée en vigueur récente des dernières règlementations sur la cybersécurité permette d'éviter ou au moins de diminuer les violations de données massives. D'ailleurs, l'ANSSI a récemment constaté une amélioration sur le terrain de la cybersécurité des hôpitaux[33].

III. Des solutions concrètes mises en place par les autorités de protection

Outre les textes juridiques, les autorités de contrôle se mobilisent sur le sujet de la cybersécurité et de l'IA, en s'efforçant d'établir des recommandations de façon régulière.

- **Les fiches pratiques de la CNIL pour s'informer.** Depuis 2022, la CNIL publie fréquemment des fiches pratiques sur la cybersécurité et l'IA. Il est ainsi possible de se documenter sur les fuites de données[34], la sécurité des données personnelles[35], ou encore la cybersécurité dans le respect du RGPD .

- **Les *guidelines* de l'ANSM à suivre pour les dispositifs médicaux.** Les recommandations de l'ANSM (Agence nationale de sécurité du médicament et des produits de santé) de septembre 2022 sur la cybersécurité des dispositifs médicaux[37] sont également un cadre à suivre, principalement par les fabricants de dispositifs médicaux. L'objectif étant de réduire au maximum les risques de cyberattaques à l'encontre du matériel médical et de « *prévenir la compromission des données et l'utilisation détournées des dispositifs médicaux* »[38]. Dans ce cadre,

il est recommandé aux acteurs du secteur de s'informer sur la cybersécurité, pour ensuite identifier les failles de leur système informatique et enfin définir une stratégie de défense efficace.

Les normes de cybersécurité. Par ailleurs, le règlement *Cybersecurity Act* met en place un cadre de certification de la cybersécurité au niveau communautaire, dont l'objectif est de garantir le respect des normes de sécurité des produits, services et processus. Il permet la délivrance de certificats de conformité aux normes de cybersécurité de l'Union européenne, avec trois niveaux de certifications : élémentaire, substantiel, ou élevé. Chaque niveau d'assurance correspond à un processus de certification et une méthodologie d'évaluation différente. L'objectif est d'assurer une sécurité minimale de la structure pour renforcer la sécurité globale de son système informatique. Notez que ce texte exclut les dispositifs médicaux de son champ d'application.

Le *SecNumCloud*. Dans une même intention, l'ANSSI a élaboré depuis 2016 le référentiel *SecNumCloud*[39] pour renforcer la sécurité des prestataires proposant une offre d'informatique en nuage (cloud) et par ricochet de leurs clients, par l'établissement d'un ensemble de règles de sécurité garantissant un haut niveau d'exigence technique, opérationnel et juridique. Pour être qualifié *SecNumCloud* et obtenir le *Visa de sécurité ANSSI* correspondant, le fournisseur doit remplir une série d'exigences quant à sa fiabilité. L'objectif est de protéger efficacement les données sensibles contre les cybermenaces.

Les bonnes pratiques de l'ENISA. Enfin, à son niveau, l'ENISA préconise entre autres de mettre en œuvre des sauvegardes chiffrées hors ligne des données à caractère confidentiel, de mettre en place des programmes de sensibilisation et des formations pour améliorer les pratiques de sécurité parmi les professionnels de santé, d'analyser régulièrement les vulnérabilités, ou encore d'instaurer des processus permettant l'établissement de correctifs et de mises à jour régulières des logiciels[40].

Si la règlementation européenne tend aujourd'hui à assurer une meilleure sécurité dans le cyberespace dans un contexte d'utilisation croissante de l'IA, qu'elle soit bienveillante ou malveillante, les infrastructures de santé devront également suivre des bonnes pratiques pour garantir la sécurité de leurs systèmes informatiques, et des données de santé des patients.

NOTES

1. Site internet www.cyberocc.com, rubrique « Quelques chiffres ».
2. https://www.latribune.fr/opinions/tribunes/hopitaux-la-france-traverse-une-veritable-tempete-cyber-947101.html.
3. Article France TV Info « Les hôpitaux de Vittel et Neufchâteau dans les Vosges sont la cible d'une cyberattaque : les interventions chirurgicales sont suspendues » - Jean-Christophe Panek, le 7 octobre 2023 - https://www.bfmtv.com/tech/cybersecurite/plusieurs-hopitaux-francais-vises-par-une-cyberattaque_AV-202306300489.html.
4. https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/nord-l-hopital-d-armentieres-victime-d-une-cyberattaque-les-urgences-fermees-pour-la-journee_6359368.html.
5. ENISA Threat landscape 2023 : le secteur de l'administration publique (19%), les individus personnes physiques (11%), la santé (8%).
6. Pr. Michel Séjean, Intelligence artificielle et cybersécurité, in Droit de l'intelligence artificielle, A. Bensamoun et G. Loiseau (dir.), LGDJ, 2022, p.525.
7. Village de la Justice, « Cybersécurité et intelligence artificielle : le paradoxe juridique » par Sabine Marcellin – 5 octobre 2023.
8. Pr. Michel Séjean, Intelligence artificielle et cybersécurité, in Droit de l'intelligence artificielle, A. Bensamoun et G. Loiseau (dir.), LGDJ, 2022, pp.536-537.
9. Exemple d'une «fraude au président» en version «deepfake » par visioconférence, qui a amené, en février 2024, un employé d'une multinationale basé à Hong Kong à virer 25 millions de dollars à des escrocs (https://www.capital.fr/economie-politique/deepfake-piege-en-visioconference-il-transfert-25-millions-de-dollars-a-des-escrocs-1491622).
10. Projet de Règlement européen sur l'intelligence artificielle (AI Act) de février 2024, §43 « Des exigences devraient s'appliquer aux systèmes d'IA à haut risque en ce qui concerne la qualité des jeux de données utilisés, la documentation technique et la tenue de registres, la transparence et la fourniture d'informations aux utilisateurs, le contrôle humain, ainsi que la robustesse, l'exactitude et la cybersécurité. Ces exigences sont nécessaires pour atténuer efficacement les risques pour la santé, la sécurité et les droits fondamentaux, selon la destination du système, et, aucune autre mesure moins contraignante pour le commerce n'étant raisonnablement disponible, elles n'imposent pas de restriction injustifiée aux échanges. » ; v. également : Article 15 AI Act « Exactitude, robustesse et cybersécurité ».
11. IBM, Cost of a data breach, rapport de 2023.
12. Site internet cyberveille-sante.gouv.fr, « Rapport ENISA des cybermenaces concernant le secteur de la santé ».
13. Fiches thématiques sur l'Union européenne, « Une stratégie numérique pour l'Europe ».
14. Directive sur la sécurité des réseaux et des systèmes d'information (Directive NIS 1) 2016/1148.
15. Le régime des OSE vise les opérateurs tributaires des réseaux ou systèmes d'information, fournissant un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société - https://cyber.gouv.fr/faq-operateurs-de-services-essentiels-ose.
16. Directive sur la sécurité des réseaux et des systèmes d'information (Directive NIS 2) 2022/2555.
17. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC.
18. https://www.ticsante.com/story?ID=5747.
19. A l'échelle française, NIS 2 s'appliquera à des milliers d'entités appartenant à plus de dix-huit secteurs qui seront désormais régulés. Environ 600 types d'entités différentes seront concernés, parmi eux des administrations de toutes tailles et des entreprises allant des PME aux groupes du CAC40. Les principaux critères d'intégration ont été définis au niveau européen. Il s'agit principalement du nombre d'employés, du chiffre d'affaires et de la nature de l'activité réalisée par l'entité (https://cyber.gouv.fr/la-directive-nis-2#entite).
20. https://cyber.gouv.fr/la-directive-nis-2#:~:text=Avec%20la%20directive%20NIS%202%2C%20l'objectif%20reste%20inchang%C3%A9%20%3A,prot%C3%A9ger%20face%20%C3%A0%20la%20menace.
21. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32019R0881.
22. https://www.techopital.com/story?ID=6640.
23. Qualité des données, documentation et traçabilité, transparence, supervision humaine, précision, cybersécurité et robustesse.
24. Article 14 de l'IA Act.
25. Proposition de règlement de l'UE sur l'espace européen des données de santé (EHDS) du 3 mai 2022.
26. https://www.cnil.fr/fr/les-cnil-europeennes-adoptent-un-avis-sur-lespace-europeen-des-donnees-de-sante-et-renforcent-leur-0.
27. Règlement général sur la protection des données 2016/679 du 27 avril 2016.
28. Cas d'une patiente décédée en Allemagne n'ayant pas pu subir une opération en urgence à la suite d'une cyberattaque dans une clinique neutralisant son fonctionnement : Le Monde, 17 septembre 2020 ; ICT Journal, 17 novembre 2020.
29. Proposition de directive relative à l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle du 28 septembre 2022.
30. Fiche CNIL « Cybersécurité : la CNIL agit pour le développement de solutions respectueuses du RGPD ».
31. ENISA, Threat landscape 2023.
32. En ce sens : M. Séjean, Intelligence artificielle et cybersécurité, in Droit de l'intelligence artificielle, A. Bensamoun et G. Loiseau (dir.), LGDJ, 2022, p.527.
33. https://www.bfmtv.com/tech/cybersecurite/l-anssi-note-une-amelioration-de-la-securite-informatique-des-hopitaux-et-des-collectivites_AD-202301240709.html.
34. Fiche CNIL « Fuite massive de données de santé : comment savoir si elle vous concerne et que pouvez-vous faire ? » ; Fiche CNIL « Fuite de données de santé : le tribunal judiciaire de Paris demande le blocage d'un site web ».
35. Fiche CNIL « La CNIL publie une nouvelle version de son guide de la sécurité des données personnelles ».
36. Fiche CNIL « Cybersécurité : la CNIL agit pour le développement de solution respectueuses du RGPD ».
37. Guidelines ANSM « Cybersécurité des Dispositifs Médicaux Intégrant du Logiciel au cours de leur cycle de vie ».
38. Guidelines ANSM « Cybersécurité des Dispositifs Médicaux Intégrant du Logiciel au cours de leur cycle de vie ».
39. https://cyber.gouv.fr/secnumcloud-pour-les-fournisseurs-de-services-cloud.
40. Rapport ENISA 2023 : https://www.cyberveille-sante.gouv.fr/actualites/union-europeenne-rapport-enisa-des-cybermenaces-concernant-le-secteur-de-la-sante-2023.