A1EGR

Comment sécuriser les données des patients face aux systèmes d'informations des hôpitaux fragilisés par leur digitalisation?

Le but de cet essai est de réfléchir sur quelques-unes des solutions proposées pour sécuriser les données des patients des hôpitaux français. Nous avons pour cela adopter un angle argumentatif.
Nous pensons que les solutions qui vont être détaillées plus tard doivent être renforcées pour que les hôpitaux puissent préserver une gérance éthique des données des patients grâce à des systèmes d'informations sécurisés.

Résumé:

La digitalisation des systèmes d'informations français apporte des avantages dans le parcours de santé français. Elle permet la coordination entre les différentes unités des hôpitaux grâce à des données facilement accessibles mais aussi une meilleure communication avec les patients. Mais les hôpitaux sont souvent victimes d'attaques informatiques. Selon l'agence nationale de sécurité des systèmes d'informations (ANSSI), en 2021, en moyenne, un incident par semaine a eu lieu dans une entité du secteur de la santé. Pour protéger ces systèmes d'informations, la législation supposée prévenir les attaques informatiques en partageant notamment des informations sur les cyberattaques n'est pas encore assez efficiente. Les hôpitaux français manquent aussi de moyens financiers pour protéger leurs systèmes d'informations. Les hôpitaux doivent poursuivre la mise en place des outils de préventions offerts par les différents plans de renforcement de la cybersécurité.

L'éthique professionnelle peut être définie comme l'ensemble des principes moraux qui régissent le comportement des entreprises et des organisations.
Les établissements de santé tels que les centres hospitaliers régionaux universitaires (CHRU) ou encore les centres hospitaliers (CH), doivent tout comme toutes les organisations collecter, stocker, traiter et distribuer des données de santé. C'est le management des systèmes d'informations. Cette gestion doit permettre la confidentialité, l'intégrité et la disponibilité des données pour être éthique. Le progrès technologique pousse les entreprises et organisations à adapter leurs systèmes d'information. La digitalisation qui est l'utilisation de technologies numériques dans le but de changer le modèle économique ou commercial des organisations apporte des nouveaux outils innovants. Dans le cas des hôpitaux, il peut s'agir de dossiers médicaux électroniques ou de nouveaux systèmes d'informations hospitaliers. Mais la digitalisation malgré les bénéfices qu'elle apporte n'est pas sans risques. Comment les hôpitaux peuvent alors adopter un comportement éthique, c'est-à-dire garantir la confidentialité et l'intégrité des données sensibles des patients?

Nous nous demanderons donc comment sécuriser les données des patients présents dans les systèmes d'information numérisés des hôpitaux français. Nous verrons d'abord pourquoi

les établissements de santé adoptent un système d'information digital malgré les risques encourus, nous verrons ensuite pourquoi la législation en matière de cybersécurité ne permet pas encore de limiter les cyberattaques des hôpitaux. Enfin, nous verrons comment le manque de moyens des hôpitaux les empêchent d'avoir des systèmes d'informations sécurisés.

Avant la digitalisation des systèmes d'informations des hôpitaux, les données des patients existaient uniquement sous formes physiques. Tout comme de nos jours, les dossiers papiers étaient triés et stockés. Cela augmentait cependant d'une part les délais de traitement, car la communication entre les différents services hospitaliers et professionnels de santé de était difficile et longue et donc d'autre part aussi l'efficacité et la qualité de la prise en charge. Pour répondre à la problématique, nous avons étudié les différentes solutions possibles et évalué leurs efficacité.

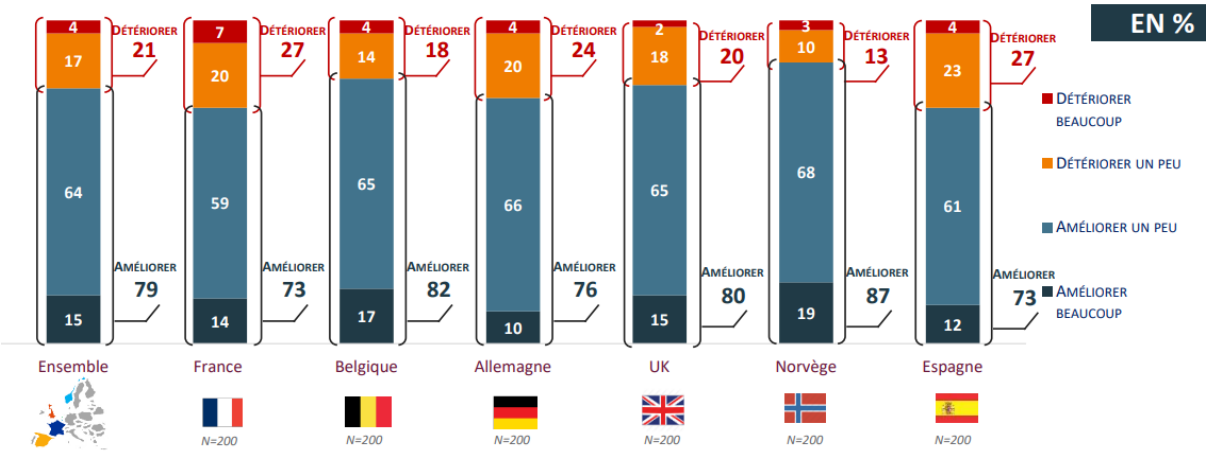
Selon le baromètre Digital Gouv'2018 , en 2018 85% des français se sentaient disposés à réaliser en ligne toutes leurs interactions avec le service public. En outre, depuis le 1er janvier 2022, la création de "mon espace santé" a permis le stockage de l'ensemble des documents de santé des français afin de les partager facilement avec les professionnels de santé. En 2022, plus de 42 millions de documents y ont été ajoutés par les professionnels de santé.
Les hôpitaux en tant que service public font face à la numérisation de leurs services. Cependant, les risques liés à cette digitalisation sont élevés et en 2021 1,4 millions de personnes testées contre le COVID-19 mi-2020 ont été concernés par une fuite de données provenant de l'Assistance Publique-Hôpitaux de Paris (AP-HP).

I. Les bénéfices de la numérisation des systèmes d'informations

Tout d'abord, la digitalisation des établissements de santé est au premier abord bénéfique pour les patients. En effet, elle leur permet d'obtenir des informations dans des délais moins élevés qu'autrefois. D'autre part, la digitalisation des systèmes d'informations des hôpitaux facilite non seulement le partage d'information entre les différents services ce qui favorise une meilleure coordination des soins mais aussi la communication entre médecin et patients.
Dans un article nommé l'*E-santé, digitalisation ou transformation numérique: impact sur les soins de support en oncologie* publié en 2022, l'auteure explique les bénéfices de l'e-santé dans le domaine de l'étude du diagnostic et du traitement du cancer. Le terme e-santé comprend selon l'article, les différents outils de numérisation du domaine de la santé comme les outils d'échange d'informations mais aussi les systèmes d'informations hospitaliers.
Selon l'auteure "en permettant des évaluations et des interventions en temps réel, dynamiques et assistées par la technologie, la e-santé est un outil d'optimisation des soins de support oncologiques en 2021".

De plus, dans le cadre d'une enquête européenne sur la digitalisation du parcours santé publiée en juin 2019 par sopra steria, 1600 citoyens ont été interrogés. Il leur a été demandé s' ils pensent que le développement de solutions digitales dans le domaine de la santé (applications et objets connectés,dossier médical électronique, intelligence

artificielle,robots…) va améliorer ou détériorer la qualité du système de santé de leurs pays. Il a été observé que près de 80% des européens considèrent que la digitalisation va améliorer la qualité du système de santé de leur pays.



Plus particulièrement, 74% des français pensent que le développement de solutions digitales va “un peu” ou “beaucoup” améliorer la qualité du système de santé français. Qui plus est, plus récemment en 2020, plus de 40 millions de patients ont utilisé Doctolib, une application de gestion de rendez-vous, pour prendre des rendez-vous médicaux.
Les hôpitaux, dans le but de s’aligner dans la volonté d’un grand nombre de patients de digitaliser les parcours de santé, doivent digitaliser leurs services. Mais la digitalisation des systèmes d’information des hôpitaux ne provient pas seulement du souhait des patients de digitaliser les services de santé mais aussi des équipes hospitalières. Dans le panel d’observation des pratiques et des conditions d’exercice en médecine générale publié en 2020 par la direction de la recherche, des études, de l’évaluation et de statistiques, en 2020, 80% des médecins de moins de 50 ans utilisaient 3 outils de santé numérique: le dossier patient informatisé, le logiciel d’aide à la prescription et la messagerie sécurisée de santé.

Nous avons vu que les professionnelles de santé ainsi que les patients sont souvent favorables à la digitalisation des systèmes de santé, nous verrons maintenant comment cette numérisation n’est pas assez protégé par les lois de cybersécurité.

II. Une législation en matière de cybersécurité trop fragile

Les hôpitaux font partie des organismes les plus touchés par les attaques au rançongiciel. Selon le dossier d’information publié par le ministère des solidarités et de la santé publié 2021, en 2020 27 hôpitaux français ont été touchés par des cyberattaques.
En France, plusieurs organismes sont responsables de l’identification des hackers. Il s’agit par exemple de l'Agence nationale de la sécurité des systèmes d'information (Anssi). Il est cependant difficile de retracer les pirates informatiques car ils sont qualifiés et connaissent les failles de sécurité des hôpitaux. Mais même lorsqu'ils sont retrouvés, le manque de législation ou de lois trop limitées empêchent leur arrestation ou extradition.

Il existe en effet des accords bilatéraux entre la France et d’autres pays. Ces accords doivent permettre en théorie le partage d’information concernant une attaque informatique. Ils devraient donc limiter le nombre de cyberattaques dans les hôpitaux dans le futur. Pour

évaluer l'efficacité de tous ces accords, il nous faudrait donc des données sur le nombre de demandes d'extradition ou d'information concernant les cyberattaques d'organismes et entreprises françaises et le nombre de réponses positives mais aussi sur l'impact des autres accords bilatéraux. Mais il existe en réalité peu de chiffres sur le nombre d'extraditions vers la France en cas de cyberattaques.

Récemment, le hackeur français Sébastien Raoult a été extradé du Maroc vers les Etats-Unis suite à son arrestation au Maroc. Il est accusé d'appartenir au groupe cybercriminel ShinyHunter. Un accord bilatéral entre les Etats-Unis et le Maroc a donc permis l'extradition de Sébastien Raoult. Mais cette affaire, nous montre les limites de la législation en termes de cybercriminalité. En effet, bien que l'extradition ait déjà eu lieu, le Comité des droits de l'Homme des Nations unies a demandé au Maroc de suspendre l'extradition vers les Etats-Unis.
Outre les accords bilatéraux entre les pays, la convention de Budapest signée par 68 pays, doit permettre entre autres l'extradition de criminels vers la France et les autres pays signataires. Il s'agit d' une convention sur la cybercriminalité.

Dans un rapport sur les avantages et impact de la convention de Budapest publié par le conseil de l'Europe en 2020, "En 2019, la France a envoyé 55 demandes d'entraide judiciaire émanant de services français pour des données électroniques, toutes ces demandes se fondant sur la Convention, et a traité 20 demandes entrantes de cette nature." Mais ces demandes d'entraide judiciaire, bien qu'elles concernent la cybercriminalité, ne traitent pas seulement des cyberattaques et des hackers. Le rapport ne donne d'ailleurs aucun détail sur la nature de ces demandes. Ces demandes sont-elles liées à des cyber-infractions concernant la fraude électronique par exemple ou bien des cyberattaques? De plus, seulement 20 demandes sur 55 ont été traitées. Or dans le cas de cyberattaques d'hôpitaux, il est primordial de raccourcir les données de traitement des demandes d'entraide. Les données des patients étant sensibles, les longs délais augmentent les risques de récidives des cybercriminelles. Il est donc encore une fois difficile de confirmer l'efficacité de cette convention dans l'éradication des cyberattaques en France.

Concernant les autres pays signataires, on peut néanmoins citer le cas de l'Italie qui d'après le rapport "a constaté que le réseau s'est révélé utile pour transférer des informations et des alertes concernant des cyberattaques et des cybermenaces à l'encontre d'infrastructures critiques dans d'autres pays et pour fournir des indicateurs de compromission, s'ils sont disponibles." Le rapport ne précise pas les pays touchés par ce transfert de données, cependant, les cybercriminels s'attaquent souvent à des entités de différents pays. On peut donc affirmer que dans une moindre mesure, la convention permet à la France d'obtenir des données sur les cybercriminels.

Nous avons vu que la législation mise en place pour lutter contre la cybercriminalité n'est pas assez solide, nous traiterons maintenant de la question du manque de moyen des hôpitaux qui empêche l'éradication des cyberattaques dans les hôpitaux.

III. Le manque de moyen des hôpitaux

Les hôpitaux au vu de la nature des données qu'ils traitent ont besoin de budgets élevés pour assurer le traitement, le stockage, et la gestion sécurisée des données des patients. Le

budget peut permettre d'une part d'embaucher des employés ou des équipes spécialisées dédiées à la sécurité des systèmes d'information des établissements de santé. D'autre part, le budget peut aussi contribuer à acheter des logiciels et des technologies plus performantes et plus sécurisées avec des coûts élevés mais aussi à former les employés à la cybersécurité.

Pour répondre à ce manque de moyen, le gouvernement français à lancé le ségur de la santé qui s'est déroulé du 25 mai 2020 au 10 juillet 2020. Ce Ségur regroupait le ministre de solidarités de la santé ainsi que tous les représentants du système de santé français comme les syndicats hospitaliers par exemple. L'un des cinq enjeux du Ségur de la santé était le numérique. Plus précisément, la modernisation du numérique dans les espaces de santé. Son objectif était d'accélérer le partage sécurisé des données de santé en France, entre les professionnels de santé et les patients. Dans ce cadre, le ségur à donc reçu une enveloppe de 2 milliards d'euros pour la numérisation du système de français. Parmi ces 2 milliards, 350 millions sont dédiés à la sécurité des systèmes d'informations des établissements de santé.
L'intervention du ségur est avant tout axé sur la prévention, en donnant aux établissements la possibilité de mettre en place des outils pour augmenter leur niveau de protection. Cette précaution se traduit par des audits de sécurité des systèmes d'information et des séances de sensibilisation. Une autre partie de leur travail consiste aussi à répondre aux incidents.
Néanmoins, malgré le budget de 350 millions alloué à la cybersécurité des établissements de santé en 2020 par le Ségur, le nombre de cyberattaques des hôpitaux a augmenté en 2021. C'est pourquoi, dans un dossier d'information sur la Cybersécurité dans le secteur de la santé et du médico-social publié en 2021, le ministère des solidarités de la santé annonce un plan de renforcement de la cybersécurité de la santé.
Malgré tout, en 2021, on a constaté un millier de rançon logiciel en France. Les plans de renforcement de la sécurité des systèmes d'informations des hôpitaux mis en place depuis 2020 par le gouvernement français ne sont donc pas suffisants pour sécuriser les données des patients.

Enfin, indépendamment d'un budget pour la mise en place d'outil de protection des systèmes d'information ou d'audit de sécurité, les hôpitaux doivent former leurs employés à la gestion des cyberattaques mais aussi à les prévenir. Les cyberattaques sont en fait parfois dues à de simples erreurs d'employés peu formés aux questions de cybersécurité. Le piratage d'un système d'information peut avoir lieu suite au clic d'un lien frauduleux par un employé. Il pourrait donc être intéressant d'inclure dans les plans de sécurisation de renforcement des systèmes d'informations des hôpitaux, des formations pour les employés non spécialistes de la cybersécurité.

Conclusion:
Les hôpitaux face à l'essor de la technologie et le progrès technologique continuel devront continuer à adapter leur modèles de gestion. Pour garantir la sécurité des données sensibles de leurs patients et assurer une gestion éthique des données, il faudra améliorer les solutions déjà mises en place. Premièrement, l'efficacité de la législation contre les cyberattaques doit être évaluée. Les conventions comme la convention de Budapest doivent permettre des réponses rapides aux demandes d'information concernant les cyberattaques. Ensuite, il est nécessaire de continuer à prioriser la prévention des cyberattaques dans les hôpitaux tout en apportant de nouvelles solutions. Dans cette continuité, et afin de respecter

la stratégie d'accélération pour la cybersécurité de “France 2030”, le Gouvernement a aussi établi un programme d'investissement d'un milliard d'euros. Ce programme a pour ambition de soutenir le développement d'un écosystème privé de fournisseurs de solutions souveraines et innovantes, ce qui pourra, peut-être, permettre aux hôpitaux de bénéficier de systèmes d'informations sécurisés.

Bibliographie:

1) *Sauvignet, Théo. « Pourquoi les hôpitaux sont les cibles des hackers ». Le Point, 8 décembre 2022. https://www.lepoint.fr/high-tech-internet/pourquoi-les-hopitaux-sont-les-cibles-des-hackers-08-12-2022-2500948_47.php.*
2) *Le Monde.fr. « Cyberattaque : 20 millions d'euros débloqués pour renforcer la sécurité des hôpitaux », 26 août 2022. https://www.lemonde.fr/societe/article/2022/08/26/cyberattaque-20-millions-d-euros-debloques-pour-renforcer-la-securite-des-hopitaux_6139142_3224.html.*
3) *« pgssi-s_sensibilisation_ssi_sante_v1.0.pdf ».. https://esante.gouv.fr/sites/default/files/media_entity/documents/pgssi-s_sensibilisation_ssi_sante_v1.0.pdf.*
4) *esante.gouv.fr. « Le Ségur du numérique en santé ». Consulté le 26 février 2023. http://esante.gouv.fr/segur.*
5) *Ipsos. « Baromètre Digital Gouv' 2018 : Le développement numérique des services publics prioritaire pour les Français », 12 novembre 2018. https://www.ipsos.com/fr-fr/barometre-digital-gouv-2018-le-developpement-numerique-des-services-publics-prioritaire-pour-les.*
6) *« Système d'information ». In Wikipédia, 31 janvier 2023. https://fr.wikipedia.org/w/index.php?title=Syst%C3%A8me_d%27information&oldid=200956057.*
7) *Gartner. « Definition of Digitalization - Gartner Information Technology Glossary ». . https://www.gartner.com/en/information-technology/glossary/digitalization.*
8) *NXO France. « Transformation digitale en santé, Hôpital numérique - NXO ».*
9) *. https://www.nxo.eu/secteurs/sante/.*
10) *ANSSI. « Cyberdéfense: la France et l'Estonie signent un accord de coopération ». . https://www.ssi.gouv.fr/publication/cyberdefense-la-france-et-lestonie-signent-un-accord-de-cooperation/.*
11) *Cybercriminalité. « Budapest Convention - Cybercriminalité - publi.coe.int ». . https://www.coe.int/fr/web/cybercrime/the-budapest-convention.*
12) *L'Obs. « Imbroglio diplomatico-judiciaire autour de l'extradition de Sébastien Raoult », . https://www.nouvelobs.com/justice/20230201.OBS68998/imbroglio-autour-de-l-extradition-de-sebastien-raoult.html.*
13) *esante.gouv.fr. « Mon espace santé ». Consulté le 1 mars 2023. http://esante.gouv.fr/strategie-nationale/mon-espace-sante.*
14) *« Fuite de données de santé de l'AP-HP : que pouvez-vous faire si vous êtes concerné ? | CNIL ». . https://www.cnil.fr/fr/fuite-de-donnees-de-sante-ap-hp-que-pouvez-vous-faire-si-vous-etes-concerne.*
15) *« ipsos_sopra_steria_digitalisation_des_parcours_de_soin.pdf ».. https://www.ipsos.com/sites/default/files/ct/news/documents/2019-06/ipsos_sopra_steria_digitalisation_des_parcours_de_soin.pdf.*
16) *« dp_-_premier_anniversaire_du_segur_de_la_sante.pdf ».. https://sante.gouv.fr/IMG/pdf/dp_-_premier_anniversaire_du_segur_de_la_sante.pdf.*
17) *« De nouveaux engagements pour renforcer la cybersécurité des établissements de santé | Ministère de l'Intérieur et des Outre-mer ». . https://www.interieur.gouv.fr/actualites/communiques/de-nouveaux-engagements-pour-renforcer-cybersecurite-des-etablissements-de.*
18) *Djabri, Riad. « Prise de rendez-vous en ligne, le bilan 2020 ». Doctolib Blog - France, 22 décembre 2020. https://info.doctolib.fr/blog/42-millions-de-patients-rendez-vous-en-ligne/.*
19) *« E-santé : les principaux outils numériques sont utilisés par 80 % des médecins généralistes de moins de 50 ans. | Direction de la recherche, des études, de l'évaluation et des statistiques ». . https://drees.solidarites-sante.gouv.fr/publications/etudes-et-resultats/e-sante-les-principaux-outils-numeriques-sont-utilises-par-80-des.*
20) *Seguin, Lorène, et Louis Tassy. « E-santé, digitalisation ou transformation numérique : impact sur les soins de support en oncologie ». Bulletin du Cancer, Soins de support, 109, nº 5 (1 mai 2022): 598-611. https://doi.org/10.1016/j.bulcan.2021.08.015.*