Bulletin Juridique Des Assurances
BJDA
Anciennement Actuassurance
www.bjda.fr
LexisNexis®
www.lexisnexis.fr

Le secret médical à l'épreuve du numérique

Intervention au Webinaire « *Transparence, Secret professionnel et Assurance en santé* »
28 mai 2021, IFROSS et ERLJ, Université Lyon 3

Rodolphe Bigot,
Maître de conférences en droit privé,
UFR de Droit, Le Mans Université
Membre du Thémis-UM et Ceprisca

Assurance – Contrat – Secret médical- Numérique

Introduction[1]. Le magistrat Xavier Leonetti perçoit à travers les technologies numériques le rêve d'une sécurité absolue[2]. Mais la tête ainsi dans les nuages, on ne verrait pas toujours « la dictature invisible du numérique » où « les entreprises du Big Data, les GAFA, nous mettent à nu en nous rendant totalement transparents. Contre des promesses de confort, de vie éternelle et de vie meilleure, nous alimentons la « matrice » en renonçant sans état d'âme à notre intimité et notre liberté. Tout est organisé pour collecter la donnée, cette énergie inépuisable »[3]. Des philosophes nous disent que l'identité hypermoderne est prise au piège entre accoutumances numériques et protection du secret[4]. Juridiquement, la transparence imposée par le numérique aurait-elle aussi tendance à immerger les îlots du secret professionnel ? Le professeur Mestre a souligné que le débat est toujours difficile entre transparence et secret : la jurisprudence récente[5] « laisserait entrevoir des secrets professionnels bien relatifs, pour lesquels, d'une certaine façon, la transparence tendrait à devenir la règle ! »[6].

---

[1] Le style oral de la conférence a été maintenu.

[2] X. Leonetti, *Smartsécurité et cyberjustice*, PUF, coll. Questions judiciaires, 2021, p. 18.

[3] M. Dugain et C. Labbé, « *L'homme nu. La dictature invisible du numérique* », Plon éd. 2016.

[4] P.-A. Chardel, A. Khatchatourov, « Identité, différence et droit au secret à l'ère numérique, Collège international de philosophie », 2020/2 n° 98, p. 103 et s.

[5] Cass. crim., 13 oct. 2020, n° 19-87.341, JCP G 2021, n° 151, note J.-C. Saint-Pau.

[6] J. Mestre, « *Transparence ou secret, un débat toujours difficile…* », RLDC n° 192, mai 2021, Editorial, p. 3 : « Un arrêt qui n'hésite pas à affirmer que « *le secret médical étant un droit propre au patient, son médecin n'est pas recevable à se constituer partie civile du chef de violation du secret professionnel, dans l'intérêt de celui-ci* ». Certes, les derniers termes de cette formule entendent probablement en atténuer la portée, en l'inscrivant délibérément dans le cadre particulier d'un litige prud'homal où l'ancienne salariée d'une SELARL de médecins avait produit le dossier médical d'un patient, et où les praticiens concernés demandaient réparation du préjudice qu'ils estimaient personnellement souffrir, mais l'affirmation n'en reste pas moins assez étonnante, qui laisserait

Les derniers événements conduisent à avoir une approche juridique mais aussi sociologique de la problématique du secret confronté au numérique. Il n'est pas nécessaire de revenir sur les contours classiques du secret professionnel du médecin, mis à part quelques aspects prégnants en liant avec le digital. Peu importe, par ailleurs, le support de l'information révélée. La doctrine s'accorde : le secret médical est un « des piliers de l'exercice de la médecine et plus généralement des missions confiées aux professionnels de santé et plus généralement aux établissements, services et organismes de santé »[7]. Bien que le pilier ait été renforcé de manière extrinsèque, la fissure intrinsèque réapparaît (I), au point qu'on puisse s'interroger de son effondrement (II).

I) Le pilier du secret extrinsèquement renforcé mais intrinsèquement fissuré

Le pilier du secret, bien que colmaté par quelques dispositions éparses, n'aurait jamais été aussi fragile de par son exposition au numérique. Cette fragilité procède d'un rétrécissement en cours du champ du secret médical (A), auquel s'ajoute un risque imminent de violation globale à raison de l'ensemble des données médicales relatives au secret qui fera incessamment l'objet d'une concentration numérique (B).

A) Un champ du secret médical en voie de rétrécissement

Malgré les évolutions fulgurantes de la société vers la transparence, par la circulation des données de santé notamment, aucune réforme d'ampleur ne s'est intéressée au secret médical. Il est possible de mesurer la protection, notamment pénale, propre au secret médical au travers des hypothèses de révélations non punissables. Or, depuis la loi Touraine du 26 janvier 2016 ces hypothèses de communication n'ont cessé d'augmenter. En effet, « la loi comme la jurisprudence obligent ou permettent au professionnel de santé de trahir la confidentialité lorsqu'un impératif supérieur prévaut : les exigences de la justice, l'ordre public ou la continuité des soins. […] En outre, la liste des maladies infectieuses qui doivent faire l'objet d'un signalement a été allongée ; de même, l'on permet au médecin de témoigner de l'état de santé du patient si un tiers a un intérêt légitime à le demander »[8].

Symétriquement, depuis 2016, la protection du secret s'affaiblit dans son périmètre mais aussi dans l'effectivité des sanctions. De plus en plus de révélations du secret médical ne connaissent plus de sanctions, à l'instar des informations qui peuvent désormais être partagées. Les divulgations publiques, aujourd'hui massives parfois, semblent être confrontées à une politique législative et judiciaire de « contournement de la répression », afin que la libre circulation des données voulue, avec parfois un intérêt éventuellement important en termes de progrès médicaux qu'on ne discute pas, ne soit pas entravée, au point de conduire à une forme de redéfinition implicite du secret.

Déjà, en soutien de la jurisprudence, la loi « Kouchner » du 4 mars 2002 avait autorisé, à l'article L. 1110-4 du Code de la santé publique et sous certaines conditions, « le secret partagé

entrevoir des secrets professionnels bien relatifs, pour lesquels, d'une certaine façon, la transparence tendrait à devenir la règle ! ».

[7] D. Duval-Arnoud, *Droit de la santé. Prise en charge des patients et réparation des dommages liés aux soins*, Dalloz Référence, 2019-2020, n° 135.390.

[8] M. Bénéjat-Guerlin, « Que reste-t-il de la protection pénale du secret médical ? », *AJ pénal* 2017, p. 368.

»[9] au sein d'une équipe de soins. Le partage a été étendu par la loi du 26 janvier 2016, au gré d'une définition plus large de l'équipe de soins (incluant des personnels hors établissement et des non-soignants comme les psychologues ou éducateurs) et de la possibilité d'échange hors équipe de soins mais sous réserve du consentement préalable du patient recueilli par tout moyen, y compris de façon dématérialisée[10]. En contrepoids, une incrimination spécifique a été créée à l'article L. 1110-4, V du Code de la santé publique pour lutter contre le fait d'obtenir ou de tenter d'obtenir la communication d'informations en violation des nouvelles règles de partage, avec une peine d'un an d'emprisonnement et de 15 000 € d'amende, par analogie avec l'article 226-13 du Code pénal. La doctrine convient qu' « en vérité, la révélation entre personnels de santé au sens large ne donne guère plus lieu à répression. Le risque pénal apparaît plutôt dans la numérisation des informations médicales »[11].

Les informations couvertes par le secret ont fait l'objet d'une nouvelle qualification dans l'ère numérique, celles des données personnelles, dont certaines sensibles[12], avec la classification réalisée par le Règlement pour la Protection des Données Personnelles (RGPD)[13]. La loi Informatique et libertés considérait déjà comme sensibles les données de santé, autrement dit celles qui sont personnelles au patient. La protection initialement instaurée visait à interdire en principe les fichiers et permettre quelques exceptions (aux fins de recherche, de médecine préventive). Puis, en très peu de temps, le principe a cédé. Pour faciliter leur circulation au sein de l'Union européenne, un élargissement de la définition des données de santé, intégrant les aspects sociaux en plus des éléments thérapeutiques, a été mise en œuvre par le règlement européen du 27 avril 2016 applicable au 25 mai 2018. Sous l'effet du RGPD, on passe ainsi d'un système d'autorisation préalable du traitement[14] à un régime d'agrément *a priori* et un contrôle *a posteriori* de l'hébergeur. Avec un allègement des procédures, la responsabilisation des acteurs a été préférée dans le règlement. Elle pourrait n'être qu'artificielle cependant.

---

[9] Sur la question du secret partagé confronté au numérique, *cf.* S. Hennion, « Le partage du secret professionnel à l'ère du numérique », RDSS 2020, p. 129.

[10] CSP, art L. 1110-4 III. V. les deux décrets d'application : Décr. n° 2016-994 du 20 juill. 2016 et n° 2016-996 du 20 juill. 2016. L. Morlet-Haïdara, « Le nouveau cadre légal de l'équipe de soins et du partage des données du patient », RDSS 2016. 1103.

[11] M. Bénéjat-Guerlin, « Que reste-t-il de la protection pénale du secret médical ? », *AJ pénal* 2017, p. 368.

[12] C. Férarl-Schuhl, *Cyberdroit. Le droit à l'épreuve de l'internet, Dalloz*, coll. Praxis, 7e éd., 2018, n° 513.62 : « Les données à caractère personnel relatives à la santé des personnes sont des données sensibles, qu'elles soient recueillies ou produites à l'occasion d'activités de prévention, de diagnostic ou de soins. Les biologistes, les médecins ou encore les pharmaciens par conséquent responsables des données des patients qui relèvent du secret médical et s'exposent, en cas de violation, aux sanctions de l'article 226-13 précité. À ce titre, l'article 110 de la loi du 26 janvier 2016 a inséré un nouvel article L. 1111-8-2 du Code de la santé publique prévoyant un nouveau dispositif de sécurité incombant aux établissements de santé et aux organismes ou services exerçant lesdites activités. Ceux-ci ont l'obligation de signaler sans délai à l'Agence régionale de santé (ARS) les incidents graves de sécurité des systèmes d'information, à charge pour l'ARS de transmettre le signalement des incidents jugés significatifs aux autorités compétentes de l'État (en France, il s'agit de l'Anssi). Par ailleurs, avec l'ordonnance du 12 janvier 2017, le Code de la santé publique s'est enrichi de nouvelles dispositions (CSP, art. L. 1111-25 à L. 1111-31) relative aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et destruction des documents conservés sous une autre forme que numérique ».

[13] D. Cocteau-Senn, A. Charpentier et R. Bigot, « *La protection des données personnelles en assurance : dialogue du juriste avec l'actuaire* », *in* E. Netter (dir.), *Regards sur le nouveau droit des données personnelles*, CEPRISCA, coll. Colloques, nov. 2019.

[14] M. Bénéjat, « Les droits sur les données personnelles », *in Droits de la personnalité*, dir. J.-C. Saint-Pau, Lexis-Nexis 2013, p. 545.

Le périmètre des données stockées, mais aussi celui des prestataires, ont été élargis par la loi « Touraine »[15]. Ce texte accorde des garanties annoncées comme renforcées pour le patient, tel que l'anonymat ou le droit à l'oubli. De même, les sanctions pénales relatives au secret professionnel que pouvait connaître le corps médical sont désormais applicables aux personnes responsables du traitement, en particulier en cas de détournement de fichiers[16]. Le secret médical est soumis à un élargissement des personnes assujetties, en contrepoint du partage accru d'informations. Les hébergeurs ont l'interdiction de céder les données[17]. Il s'agit de l'opération de colmatage de la fissure.

Regrettablement, c'est « le contexte sanitaire, social ou médico-social qui entraîne l'application du régime de l'hébergement des données de santé et non la nature des données hébergées » et donc les tiers intéressés (gafam, assureurs) échappent à ces règles[18]. Ont pourtant démontré les dangers de la collecte des données de santé par les tiers intéressés[19]. Les outils numériques permettent de croiser des données qui seules, n'ont pas directement pour objet la santé mais qui réunies sont susceptibles de donner des indications sur l'état de santé, qui relève alors potentiellement du secret. À ce titre, les règles applicables aux données de santé extérieures au régime la protection des données à caractère personnel sont inadaptées, pourtant sont concernés de nombreux hébergeurs de données, de réseaux et systèmes d'informations, de logiciels ou d'objets connectés[20] qui, par exemple, ne sont pas qualifiés de dispositif médical[21].

Puis la loi « Buzyn » du 24 juillet 2019 a créé l'Espace Numérique de Santé (ENS), avec une entrée en vigueur prévue au plus tard le 1er janvier 2022. Selon Madame Morlet-Haïdara, le futur ENS serait un formidable outil de prévention[22]. Ce pourrait être, aussi, une formidable source de violations du secret, compte tenu de la concentration des données sensibles qu'il s'apprête à réaliser. Il est recherché l'interopérabilité pour que le jeu de la circulation des données s'exprime pleinement. À cet effet, la Caisse nationale de l'assurance maladie (Cnam)

---

[15] L. 26 janv. 2016, CSP, art. L. 1111-8.

[16] C. pén., art. 226-21.

[17] CSP, art. L. 1111-8, VII.

[18] T. Douville, « Les dangers de la collecte des données de santé par les tiers intéressés (gafam, assureurs…) », JDSAM n° 20, 2018/3, p. 12 et s.

[19] T. Douville, *op. cit.*, JDSAM n° 20, 2018/3, p. 12 : « Les « tiers intéressés » - gafam, assureurs et autres entreprises innovantes... - collectent des données de santé et investissent de plus en plus le secteur de la santé. Leurs initiatives sont multiples dans ce domaine. Ils développent parfois une activité en coopération avec des professionnels de santé. Souvenons-nous du partenariat entre le National health system britannique et Alphabet dont l'objet était le traitement des données de 1,6 millions de patients par Deepmind dans le but de mieux détecter les lésions rénales. D'autrefois, leurs initiatives sont autonomes. Alphabet développe ainsi une pluralité de projets : traitement de données de santé, allongement de la vie, prévention et traitement des cancers (Calico), cartographie de la santé humaine (Baseline), développements de dispositifs médicaux connectés ou de robots chirurgicaux (Verily). Facebook, Apple ou des assureurs s'orientent quant à eux vers le suivi de l'activité physique au moyen d'objets connectés. Amazon cherche, de son côté, à développer une assurance santé mais s'intéresse aussi à la détection des cancers ».

[20] Sur le marché des objets connectés en santé, *cf.* Lamy Droit de la santé, 2021, n° 620-5.

[21] T. Douville, *op. cit.*, JDSAM n° 20, 2018/3, p. 14.

[22] L. Morlet-Haïdara, « Le futur Espace Numérique de Santé : un formidable outil de prévention », JDSAM n° 28, 2021, p. 30.

a lancé en mai 2020 un appel d'offres pour la réalisation, l'hébergement, l'exploitation et la maintenance du dispositif ENS[23].

Ensuite, la loi « ASAP » du 7 décembre 2020[24] marque encore « un coup d'accélérateur au partage des données de santé, en modifiant les conditions de création et d'alimentation du dossier pharmaceutique, d'une part, et en assurant une meilleure convergence entre l'espace numérique de santé et le dossier médical partagé (DMP), d'autre part »[25]. Le titulaire de l'ENS ne pourra plus empêcher « l'accès au DMP dans son ensemble mais il pourra masquer certaines données de celui-ci ou empêcher l'accès à certaines données seulement (sauf à son médecin traitant) »[26]. Réservé à l'origine aux seuls bénéficiaires de l'assurance maladie, le DMP est attribué, désormais, à toute personne, et tout professionnel de santé a dorénavant l'obligation de l'alimenter[27].

La réduction du champ du secret tient encore à la possibilité donnée par la loi ASAP aux professionnels du secteur social et médico-social d'accéder, sous réserve du consentement de la personne préalablement informée, au DMP de celle-ci et de l'alimenter[28]. Un auteur s'inquiète de ce que « l'alimentation ultérieure de son DMP par ce même professionnel est soumise à une simple information de la personne prise en charge. Le législateur ouvre ici une brèche importante dans le secret médical, en autorisant des personnes qui ne sont pas des professionnels de santé et n'ont donc pas nécessairement les connaissances nécessaires pour en comprendre et en interpréter le contenu, à accéder au DMP d'une personne. Ces dispositions s'inscrivent toutefois dans la droite ligne de l'article L. 1110-4 du code de la santé publique, permettant le partage des données personnelles de santé entre professionnels de santé et certains autres professionnels participant à la prise en charge d'une même personne, avec le consentement de cette dernière »[29].

Il s'agit donc d'un « nouveau tournant dans la révolution numérique » : « Dossier pharmaceutique, DMP, espace numérique de santé sont autant d'outils tendant vers un même but, poursuivi par le législateur depuis près de 25 ans : mettre le numérique au service de la « maîtrise médicalisée des dépenses de santé », autrement dit utiliser le numérique pour réduire les dépenses de santé et, tout à la fois, améliorer la prise en charge, en évitant les examens redondants, les prescriptions excessives et dangereuses, en assurant une meilleure coordination des soins et en faisant de l'usager un acteur de sa propre santé. Concilier ces intérêts avec le

---

[23] *Ibid.*

[24] L. n° 2020-1525 du 7 décembre 2020 d'accélération et de simplification de l'action publique.

[25] M. Contis, « La loi ASAP ou l'accélération du partage des données personnelles de santé », Ed. législatives, 21 déc. 2020.

[26] *Ibid*.

[27] CSP, art. L. 1111-15 : « chaque professionnel de santé, quels que soient son mode et son lieu d'exercice, doit reporter dans le dossier médical partagé, à l'occasion de chaque acte ou consultation, les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge, dont la liste est fixée par arrêté du ministre chargé de la santé. Chaque professionnel doit également envoyer par messagerie sécurisée ces documents au médecin traitant, au médecin prescripteur s'il y a lieu, à tout professionnel dont l'intervention dans la prise en charge du patient lui paraît pertinente ainsi qu'au patient ».

[28] CSP, art. L. 1111-17.

[29] M. Contis, *op. cit.*, Ed. législatives, 21 déc. 2020.

secret médical est souvent un travail d'équilibriste »[30]. En d'autres termes, « le secret médical a changé de paradigme : le devoir éthique consiste moins à garder le silence qu'à faire un bon usage des informations protégées »[31]. Regrettablement, l'opération en cours de concentration numérique de ces données est sur le point d'amplifier les risques de révélation de masse.

B) Les données médicales relatives au secret en voie de concentration numérique

Par suite des travaux du député Cédric Villani dans son rapport parlementaire en date du 28 mars 2018 et de la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et la transformation du système de santé, a été créé le 2 décembre 2019 le *Health Data Hub* (HDH), l'outil de collecte et de centralisation des données de santé, aux fins de recherche et d'analyse. C'est une plateforme numérique - un *cloud* - de « massification » des données de santé. Elle vise à croiser les bases de données de santé disponibles (système national des données de santé, données des hôpitaux, de la médecine de ville, etc.) et faciliter leur consultation par toutes les différentes équipes scientifiques de recherche médicale. Elle est portée par un groupement d'intérêt public nommée « Plateforme des données de santé » et créé sous l'autorité de l'Institut national des données de santé (INDS)[32]. Mais « de nombreuses voix s'élèvent pour en dénoncer les risques […]. En effet, le HDH regroupe les données issues de centres hospitaliers, des pharmacies ou encore du dossier médical partagé, lesquelles sont stockées sur le *cloud* de Microsoft. Ce choix du *cloud* Azure ne fait pas l'unanimité d'autant plus que Microsoft a été nommé via une dispense de marché public par un contrat en date du 15 avril 2020 »[33]. Saisi pour faire annuler ce contrat d'hébergement, le Conseil d'État a été bien embarrassé dans sa décision du 13 octobre 2020, rendu quelques mois après l'affaire *Schrems II*[34], mais beaucoup moins la CNIL ayant donné son avis en amont. Pourtant, les serveurs Microsoft ont fait l'objet de vulnérabilité critique dernièrement[35].

---

[30] *Ibid.*

[31] M. Bénéjat-Guerlin, « Que reste-t-il de la protection pénale du secret médical ? », *AJ pénal* 2017, p. 368. – Comp. V. Olech, *Le secret médical et les technologies de l'information et de la communication*, dir. B. Py, th. Université de Lorraine, 2019, n° 400 : « Le secret professionnel, soit le secret comme « moyen » juridique, semble de moins en moins privilégié pour assurer la préservation des données. Les critères, considérés par la doctrine, comme traditionnellement attachés à la désignation des personnes qui y sont astreintes, ne permettent plus d'expliquer certaines évolutions législatives. Il n'est pas certain, par ailleurs, que la nature des informations soit réellement importante dès lors qu'il est impossible d'évaluer avec certitude la portée de la désignation prévue à l'article L. 1110-4 du Code de la santé publique. L'on constate toutefois que les acteurs techniques et les personnes réutilisant les données sont explicitement soumis au secret professionnel. Ils ne semblent néanmoins pas bénéficier de l'option de conscience offerte aux professionnels de santé ou à ceux de l'action sociale et médico-sociale. Nous avons considéré qu'il s'agissait de secrets de « second rang » puisque leur portée est moindre. La norme est ainsi réduite à un instrument, il n'est plus tenu compte de ses fondements axiologiques. La doctrine de la CNIL n'est pas étrangère à cette évolution. La confiance, critère de la confidentialité, doit être créée à l'égard de tous les acteurs. Tandis que le secret professionnel était institué en raison de la confiance nécessaire que le professionnel devait inspirer en raison de rôle social, le secret professionnel est désormais un outil de confiance dans le traitement des données et dans les technologies numériques ».

[32] CSP, art. L. 1461-1 ; arrêté du 29 nov. 2019.

[33] O. de Maison Rouge, « L'affaire *Health Data Hub* : entre nécessité de recherche médicale et souveraineté numérique », sous CE, 13 oct. 2020, n° 444937, Dalloz IP/IT 2021 p. 103. – *Adde* M. Untersinger et A. Piquard, « Données de santé : la plate-forme de la discorde », Le Monde, 2 déc. 2019.

[34] CJUE, 16 juill. 2020, aff. C-311-8.

[35] *Cf.* cellule d'Accompagnement Cyber sécurité des Structures de Santé (ACSS) rebaptisée le CERT Santé en avril 2021.

Pour parer aux critiques, le politique a réagi par une opération marketing. Le 17 mai 2021, le ministre de l'Economie, des Finances et de la Relance a présenté les nouveaux axes de sa stratégie nationale, en particulier un label *cloud* et une nouvelle doctrine. L'objectif du label *cloud de confiance* est d'offrir aux entreprises françaises les services du *cloud*, *« tout en assurant la meilleure protection pour leurs données »*, notamment les données les plus sensibles et stratégiques comme les données de santé. La stratégie s'appuierait également sur la mise en place d'une nouvelle doctrine : le cloud devrait devenir la méthode d'hébergement par défaut pour tous les services numériques de l'État et pour tout nouveau produit numérique en général. Concrètement, ceux-ci devront être hébergés sur l'un des deux cloud interministériels internes de l'État ou bien chez des entreprises labélisées, qui demeurent des acteurs privés du commerce numérique, soulignons. Le but serait *« d'annuler tout risque de transfert de données hors de l'Union européenne »,* notamment pour le *Health Data Hub* qui est une structure publique qui a pour objectif de rendre accessibles les données de santé des Français aux porteurs de projets publics et privés.
La boucle est donc bouclée, toutes les données de santé sont sur le point d'être concentrées chez un seul hébergeur quasiment. S'il subit une attaque, que restera-t-il du secret médical ? Les États peuvent en outre recourir à la surveillance de masse des communications électroniques – qu'il s'agisse du contenu de celles-ci ou des métadonnées rattachées – , pourtant source de bien d'interrogations, ce que la Cour européenne des droits de l'homme a admis dans deux décisions du 25 mai 2021[36]. Le pilier du secret médical, attaquée par une « réglementation « surréaliste » constituant le cadre juridique numérique de santé »[37], ne serait-il pas en voie d'effondrement ?

II) Un pilier du secret médical en voie d'effondrement ?

Trois signes avant-coureurs alertent d'un risque d'effondrement du pilier soutenant le secret médical. Le domaine du secret médical vient d'être submergé par un tsunami de cyberattaques de masse (A). Une nouvelle vague de technologies numériques est susceptibles de s'attaquer à sa base (B). La faible portée des sanctions à la fois inadaptées et peu appliquées met en lumière l'insuffisance du rempart normatif ainsi constitué (C).

A) Le tsunami des cyberattaques de masse

Aucune institution, aucun établissement, aucune entreprise ne peut garantir de manière absolue le secret dès lors que les éléments y relatifs sont insérés dans un système informatique et numérique, car quel qu'il soit, il n'est pas infaillible. La sécurité prônée par les acteurs y ayant un intérêt n'est qu'une douce illusion.

[36] CEDH 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, req. nos 58170/13, 62322/14 et 24960/15 ; CEDH 25 mai 2021, *Centrum för Rättvisa c. Suède*, req. n° 35252/08 ; M.-C. de Montecler, La CEDH admet le principe de la surveillance électronique de masse, Dalloz Actualité, 28 mai 2021.

[37] C. Zorn-Macrez, « Chroniques martiennes des données de santé numérisées, Brèves observations sur une réglementation surréaliste », RDS, n° 36, 2010. 331 ; E. Debiès, « L'ouverture et la réutilisation des données de santé : panorama et enjeux », RDSS 2016. 697 ; L. Tilman, « Le chantier numérique de la loi relative à l'organisation et à la transformation du système de santé : des innovations à la hauteur des ambitions », RGDM, n° 72, 2019. 99.

En effet, aucun acteur n'échappe aux failles[38] ou cyberattaques et au pillage des informations ou données, qu'il s'agisse de sociétés privées, de collectivités ou établissements publics[39], petits ou grands, mais aussi les géants ou GAFAM, par exemple avec le piratage de la messagerie Microsoft dernièrement[40]. De même, Colonial Pipeline aurait versé une rançon de 5 millions de dollars aux pirates informatiques début mai[41]. Un grand assureur français aurait jeté pendant l'été 2020 plusieurs milliers d'ordinateurs portables après une attaque[42]. On ne saura jamais si des données de santé liées à l'assurance emprunteur, à l'assurance complémentaire santé ou à des dommages corporels en cours de gestion sinistres ont été pillées, en particulier quand ces mêmes acteurs injectent parfois des dizaines de millions d'euros en marketing et publicités. Dans la dernière cartographie des risques émise par la Fédération française de l'assurance (FFA)[43], le cyber-risque est toujours en pôle position au point que les acteurs de l'assurance et de la réassurance se désengagent fortement depuis le début d'année : AXA ne couvrirait plus les dommages liés à un rançon logiciel ; la sinistralité dégraderait trop fortement les résultats techniques, il n'y aurait plus que quatre ou cinq assureurs à intervenir avec des conditions très restrictives, des franchises considérables, une forte sélection des risques (par des certifications et audits exigeants), et des primes augmentant jusqu'à 70 % et des plafonds de garanties très bas (10 millions d'euros)[44]. En outre, l'un des garanties premières proposées dans les contrats d'assurance cyber sont des assistances en communication… Surtout, des clauses de confidentialité y sont stipulées ! Pourtant, le 29 avril 2021, le Club des juristes a publié un rapport intitulé « Le droit pénal à l'épreuve des cyberattaques », comportant 10 préconisations pour faire face à une forme de criminalité en pleine expansion. Si le document est principalement axé sur le renforcement de la réponse pénale, la préconisation 9, à l'attention des entreprises, évoque les investissements assurantiels nécessaires à la prévention contre les cyberattaques. Les assureurs ne sont pas près de suivre semble-t-il.

Dans son rapport public de 2020, l'Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé relève que « l'année 2020 a été marquée à la fois par la crise sanitaire Covid-19, qui a mis à dure épreuve notre système de soins, et par une recrudescence de cyberattaques par rançongiciels, visant notamment les établissements de santé. De nombreux établissements ont subi des attaques, avec parfois des conséquences importantes sur la prise en charge des patients. Ainsi, près de quatre cents incidents ont été signalés au ministère des solidarités et de la santé et une centaine de demandes d'accompagnements ont été formulées auprès de la cellule cybersécurité en santé, dédiée à

---

[38] « Panne chez Orange : le réseau des numéros d'urgence, dont le SAMU, les pompiers et la police, est rétabli », *Le Monde.fr* avec AFP, 2 juin 2021.

[39] « La ville et l'agglomération de Chalon-sur-Saône victimes d'une cyberattaque », *Le Figaro.fr*, 21 févr. 2021.

[40] « Faille chez Microsoft : 30.000 organisations américaines victimes de hackers chinois », *Le Figaro.fr*, 7 mars 2021)

[41] V. Samson, « États-Unis : Colonial Pipeline aurait versé une rançon de 5 millions de dollars à des pirates informatiques », *Le Figaro.fr*, 14 mai 2021.

[42] B. Chabrier, « Petit à petit, MMA se reconstruit après sa cyberattaque », *L'Argus de l'assurance.com*, 10 sept. 2020.

[43] FFA, *Cartographie prospective 2021 des directeurs des risques de l'assurance et de la réassurance*, p. 5 et 15 : https://www.ffa-assurance.fr/la-federation/publications/barometre-des-risques-emergents/cartographie-prospective-2021-des-risques

[44] *Cf.* L. Massel et S. Beccavin (cabinet Marsh), « La couverture assurantielle du cyberrisque des établissements de santé », *in* L. Morlet-Haïdara (dir.), *Les cyberattaques dans les établissements de santé : enjeux et protections*, Université de Paris, colloque du 17 mai 2021.

l'appui des structures de santé au sein de l'Agence du numérique en santé (ANS) »[45]. La menace est croissante avec plus de 17 % d'incidents en 2020 par rapport à 2019[46].

L'année 2021 surenchérit : de nombreux hôpitaux ont été cyberpiratés. À ce jour, pour les cas dévoilés, on recense, le CHU de Rouen (nov. 2019), l'hôpital de Paris et de Narbonne[47], les centres hospitaliers d'Albertville et Moûtiers et deux EHPAD adossés au CHAM (21 déc. 2020) [48], le centre hospitalier des Landes (9 févr. 2021)[49], l'hôpital de Villefranche (15 févr. 2021)[50] et le centre hospitalier d'Oloron-Sainte-Marie (8 mars 2021)[51]. S'ajoutent couramment aux cryptovirus des vols de données de santé dans les centres hospitaliers français[52]. En outre, la négligence de certains responsables de traitement génèrent des failles de cybersécurité et il a été révélé en décembre dernier que les hôpitaux laissent des millions d'images médicales sensibles exposées en ligne[53]. Le problème est international. L'hôpital universitaire de Düsseldorf a été visé par une attaque numérique en septembre 2020 et une patiente serait décédée à raison de la discontinuité des soins[54]. Des cyberattaques ont aussi ciblé la logistique des vaccins[55]. Au-delà

---

[45] Ministère des solidarités et de la santé, Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé, Rapport public 2020.

[46] J.-F. Parguet (ministère de la santé), « Approche institutionnelle », *in* L. Morlet-Haïdara (dir.), *Les cyberattaques dans les établissements de santé : enjeux et protections*, Université de Paris, colloque du 17 mai 2021. - Ministère des solidarités et de la santé, Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé, Rapport public 2020.

[47] M. Masson, « Cyberattaques : les hôpitaux sommés de payer des rançons, l'Occitanie n'est pas épargnée », 13 février 2021 : https://www. midilibre.fr/2021/02/13/cyberattaques-les-hopitaux-sommes-de-payer- des-rancons-loccitanie-nest-pas-epargnee-9370352.php

[48] S. Plas, « L'hôpital d'Albertville en proie à une cyberattaque », *Le Figaro.fr*, 23 déc. 2020 : « Détectée lundi 21 décembre, aux alentours de 4 heures du matin, la cyberattaque, provoquée par un virus de type « rançongiciel » a rendu indisponible *« un certain nombre d'équipements, de serveurs, de logiciels, ainsi qu'une partie du réseau informatique »*, comme l'indiquait l'hôpital dans un communiqué, mercredi ».

[49] C. Renault, « C'est un tsunami, il faut tout réinventer » : dans l'enfer de l'hôpital de Dax, cible d'une cyberattaque, *Le Figaro.fr*, 12 févr. 2021 : le CH des Landes a été victime d'une cyberattaque massive, dite au rançon logiciel : le logiciel malveillant a crypté les données et paralysé le système informatique. – « Une attaque informatique paralyse une partie de l'hôpital de Dax », *Le Figaro.fr*, 10 févr. 2021 : « Une cyberattaque de grande ampleur a fortement impacté l'hôpital de Dax, le 9 février 2021. Un logiciel malveillant a coupé l'ensemble des appareils électroniques tels que les téléphones et ordinateurs, impactant les services de soins ».

[50] « Après celui de Dax, l'hôpital de Villefranche paralysé par un rançongiciel », *Le Monde.fr*, 15 févr. 2021 : « Les hôpitaux représentent une des cibles privilégiées des attaques informatiques et ce particulièrement avec la pandémie, qui pousserait « plus facilement les hôpitaux à payer la rançon au vu du besoin critique de continuité d'activité » explique l'Anssi, le gendarme de la cybersécurité en France »).

[51] « Un hôpital des Pyrénées-Atlantiques visé à son tour par une cyberattaque », *Le Monde.fr*, 8 mars 2021.

[52] S. Montaron, « Des données de soignants des HCL vendues par un pirate du web », 26 févr. 2021 : https://www.leprogres.fr/faits-divers-justice/2021/02/24/des-donnees-de-soignants-des-hcl-vendues-par-un-pirate-du-web

[53] D. Palmer, « Les hôpitaux laissent des millions d'images médicales sensibles exposées en ligne », 15 déc. 2020 : https://www.zdnet.fr/actualites/les-hopitaux-laissent-des-millions-d-images-medicales-sensibles-exposees-en-ligne-39914957.htm

[54] L. Andrieu, « Cyberattaques contre les hôpitaux : appât du gain pour les hackers, danger de mort pour les patients », *Le Figaro.fr*, 21 nov. 2020.

[55] I. Vergara, « Des cyberattaques ciblent la logistique des vaccins », *Le Figaro.fr*, 14 févr. 2021.

des problèmes de fonctionnement[56], la plupart du temps on ne saura sans doute jamais si des données couvertes par le secret médical ont été volées et éventuellement revendues…

Le 4 mars 2021, la présidence du Tribunal judiciaire de Paris a réalisé un communiqué annonçant qu' « un fichier contenant 491 840 lignes de données personnelles et médicales de patients illégalement collectées et rassemblées a été mis en ligne sur internet. Chaque ligne se rapporte à une personne physique identifiée par son nom, son prénom, sa date de naissance, son numéro de téléphone fixe et/ou portable, son numéro de sécurité sociale, son adresse postale et son adresse électronique. Ces informations sont complétées par d'autres données, comme le nom et les coordonnées du médecin traitant, la date de la dernière visite médicale, le nom de l'assuré social dont le patient est ayant-droit. Des données médicales sont également renseignées, comme le groupe sanguin, le facteur rhésus et l'existence ou non d'une affection de longue durée. Un champ nommé « commentaires » contient des indications libres qui peuvent renvoyer, à nouveau, à d'autres données à caractère personnel (numéro de mutuelle, par exemple). Plusieurs de ces champs contiennent des indications relatives à l'état de santé des patients. Saisi par la voie d'une procédure de référé à l'initiative de la président de la CNIL, le tribunal judiciaire de Paris a ordonné aux quatre fournisseurs internet français (Orange, SFR, Bouygues et Free) de mettre en œuvre sans délai le blocage du site internet où est hébergé le fichier litigieux »[57].

Il s'agirait des données d'une trentaine de laboratoires de biologie médicale, pour des prélèvements effectués entre 2015 et 2020, liées à l'emploi d'un logiciel. Aujourd'hui, une vingtaine d'acteurs achèteraient et revendraient des données de santé. Et « face à une demande grandissante, « *les cybercriminels se démènent pour fournir ces données* »[58]. Des spécialistes annoncent qu'un numéro de sécurité sociale aurait une valeur de 5 à 15 € sur le *darknet* et qu'un seul dossier médical atteindrait près de 50 €, l'un des éléments le plus valorisé[59].

B) Une nouvelle vague de technologies numériques menaçantes

En premier lieu, la technologie *blockchain* est sollicitée dans le domaine pharmaceutique pour améliorer la traçabilité des lots notamment et donc la sécurité sanitaire. Certains ont pensé en faire le support du dossier médical partagé, bien que l'un de ses caractères principaux soit la transparence. La doctrine relève dès lors une double incompatibilité entre la technologie *blockchain* et la protection des données. Cette protection est en principe concentrée sur le responsable de traitement identifié alors que la *blockchain* se veut par nature décentralisée ; en outre, les chaînes de blocs sont intangibles, ce qui contrarie la mise en œuvre des droits des

[56] Le téléphone ne fonctionne plus, on ne peut plus enregistrer les nouveaux patients (aux urgences notamment), ni communiquer avec les différents services, ni imprimer les résultats d'analyses.

[57] TJ Paris, Ordonnance de référé du 4 mars 2021, RG n° 21/51823, Communiqué du Président.

[58] T. Kerkour, « La Cnil enquête après la fuite de centaines de milliers de données médicales de Français », *Le Figaro.fr*, 22 février 2021 : « Sa valeur pourrait atteindre 2000 euros, un montant incertain, l'entreprise n'ayant pas pu avoir accès à la totalité des données. Il n'est pas non plus possible de savoir si ces données ont été vendues, ni à combien d'entités. Cette mise en vente fréquente de données de santé n'est pas sans lien avec la multiplication des attaques contre les services hospitaliers. Les derniers exemples en date étant les hôpitaux de Dax et des Landes frappés début février par des «*rançongiciels*» ».

[59] L. Massel et S. Beccavin (cabinet Marsh), *op. cit.*, *in* L. Morlet-Haïdara (dir.), *Les cyberattaques dans les établissements de santé : enjeux et protections*, Université de Paris, colloque du 17 mai 2021.

personnes à l'égard du traitement[60], comme le droit à l'oubli dont la violation serait ainsi perpétuelle[61]. Une expérimentation est néanmoins en cours depuis 2015 en Estonie qui stocke les dossiers médicaux sur une *blockchain*.

En second lieu, l'intelligence artificielle (IA), intégrée à un robot par exemple, « peut être à l'origine d'infractions ou utilisée pour la commission d'infractions, et de pratiquement toutes les infractions du Code pénal »[62], notamment les infractions diverses en cas d'utilisation de l'IA en matière médicale, liées aux erreurs de diagnostic, aux fautes dans le geste, au secret, ou, plus naturellement, les infractions informatiques des articles 323-1 et suivants du Code pénal desquelles participent l'espionnage informatique, l'entrave au fonctionnement d'un système de traitement automatisé de données et la perturbation informatique[63].

C) Un rempart normatif insuffisant : la faible portée des sanctions inadaptées et peu appliquées

Là où Madame Abravanel-Jolly soulignait quelques années auparavant, dans sa thèse relative à la protection du secret[64], que celui-ci est défendu par le recours à la notion de responsabilité et surtout par un véritable droit subjectif à son respect, et que les limites d'intérêt général constituent, pour leur part, de vraies limites à la protection du secret, la numérisation fulgurante de la société, en particulier celle de la santé, n'a pas été accompagnée de sanctions adaptées.
Les pénalistes s'inquiètent également de ce que « les poursuites pour violation du secret médical se font rares alors qu'elles ne requièrent ni préjudice ni plainte de la victime puisque l'infraction protège, au-delà de l'intérêt du patient, l'intérêt collectif des professions »[65]. Mais, sur fond de corporatisme notamment, les révélations sont rares. Selon Monsieur Parguet, haut fonctionnaire défense et sécurité du ministère de la santé, beaucoup d'acteurs privés n'annoncent pas les attaques ou seulement contraintes et forcées. En effet, « personne ne s'en vante ! »[66], alors qu'on ne serait qu'au début, en fréquence, des risques cyber.

---

[60] T. Douville, « Blockchain et protection des données à caractère personnel », AJ contrat 2019, p. 316 ; « Blockchain et santé, Blockchains : entre mystères et fantasmes », Cour de cassation, 14 janv. 2021.

[61] R. Bigot, « *La blockchain et l'assurance, la blockchain ou l'assurance ? »*, in *Comprendre et anticiper la révolution numérique en assurance*, colloque du 19 mai 2017, 20 ans du Master II Assurance, Université de Caen Normandie – Faculté de droit, 19 mai 2017, *in* Actualités du droit, Wolters Kluwer France, Tech&Droit, oct. 2017 ; RLDI nº 142, nov. 2017, nº 5109, pp. 66-72. – *Adde* C. Férarl-Schuhl, *Cyberdroit. Le droit à l'épreuve de l'internet, Dalloz*, coll. Praxis, 7e éd., 2018, n° 532.46 : « il existe un risque de conflit avec le principe même de la *blockchain* puisque cette technologie suppose la conservation des données dans les registres sans pouvoir les effacer ».

[62] R. Mesa, « Intelligence artificielle et droit pénal : quels responsables, quelles infractions, quelles responsabilités ? », RLDI n° 181, mai 2021, p. 34 : « s'agissant de la responsabilité pénale du concepteur de l'IA, cette responsabilité devrait être la responsabilité de principe toutes les fois que l'IA fonctionne de manière autonome, c'est-à-dire sans intervention extérieure et sur la base des seules données émanant de son concepteur ».

[63] *Ibid.*

[64] S. Abravanel-Jolly, *La protection du secret en droit des personnes et de la famille*, th. Defrénois, t. 10, 2005.

[65] M. Bénéjat-Guerlin, « Que reste-t-il de la protection pénale du secret médical ? », *AJ pénal* 2017, p. 368.

[66] J.-F. Parguet (ministère de la santé), « Approche institutionnelle », *in* L. Morlet-Haïdara (dir.), *Les cyberattaques dans les établissements de santé : enjeux et protections*, Université de Paris, colloque du 17 mai 2021.

Le secret médical est avant tout une infraction pénale[67]. S'ajoutent aux sanctions prévues au titre de la violation du secret professionnel[68], les infractions permettant de sanctionner les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques[69]. Ainsi, le fait de procéder ou de faire procéder à un traitement de données de santé sans mettre en œuvre les mesures de sécurité et de confidentialité appropriées est puni de 5 ans d'emprisonnement et de 300 000 euros d'amende (C. pén., art. 226-17) »[70].
Monsieur Raschel confirme que « la question des informations à caractère secret a été renouvelée avec la numérisation des informations médicales »[71]. D'un point de vue strictement pénal, et avec une nuance en présence de bénévoles dans l'équipe de soins[72], la divulgation/révélation est l'élément matériel du délit ; c'est elle qui consomme l'infraction. C'est donc elle qu'il faut prendre en compte généralement. Mais « l'article 226-13 du Code pénal institue un délit et à défaut de précision ce délit doit être considéré comme intentionnel. Cependant un simple dol général est retenu (conscience de méconnaître la loi pénale). *A contrario,* une révélation involontaire, par négligence ou maladresse (papiers qui traînent sur le bureau d'un médecin quand il reçoit le patient suivant, paroles non maîtrisées, salle d'attente

---

[67] CSP, L. 1110-4.

[68] C. pén., art. 226-13 et C. pén., art. 266-14.

[69] Partie législative, Livre II, Titre II, Chapitre VI, Section 5 ; C. pén., art. 226-16 et s.

[70] A. Laude (dir.), *Lamy Droit de la santé*, 2021, n° 621-125 : « Sont punis des mêmes peines le fait, notamment, de : y compris par négligence, procéder ou faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi (C. pén., art. 226-16) ; hors les cas où le traitement a été autorisé dans les conditions prévues par la loi informatique et libertés (L. n° 78-17, 6 janv. 1978, JO 7 janv., mod.), procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (C. pén., art. 226-16-1) ; ne pas procéder à la notification d'une violation de données à caractère personnel à la CNIL ou à l'intéressé (C. pén., art. 226-17-1) ; collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite (C. pén., art. 226-18) ; hors les cas prévus par la loi, mettre ou conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel relatives à la santé (C. pén., art. 226-19) ; conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement (C. pén., art. 226-20) ; par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, détourner ces informations de leur finalité (C. pén., art. 226-21). Les personnes morales encourent le quintuple de l'amende susvisée, soit 1 500 000 euros (C. pén., art. 131-38) ».

[71] E. Raschel, *Etude : La responsabilité pénale des professionnels de santé*, Lexbase 2020 : « Les données personnelles du patient bénéficient de la protection de la loi « Informatique et libertés » qui les considère comme des données sensibles : le principe est l'interdiction des fichiers sauf exceptions limitativement énumérées (aux fins de recherche, de médecine préventive...). La loi « Santé » a élargi le périmètre des données stockées ainsi que les prestataires (CSP, art. L. 1111-8). En contrepartie, le législateur français renforce les garanties de l'individu (anonymat, droit d'information, droit à l'oubli) et confirme les sanctions pénales : les personnes traitantes sont assujetties au secret professionnel dans les conditions de l'article 226-13 du Code pénal et relèvent de l'article 226-21 sur le détournement de fichiers ».

[72] S. Hennion, *op. cit.*, RDSS 2020, p. 129 : « l'interprétation stricte des lois pénales ne permet guère d'étendre à un bénévole des sanctions prévues pour un professionnel lorsque cette qualification constitue un élément même de l'infraction. Le partage des informations peut sans nul doute s'effectuer dans le cadre de l'équipe de soins. Il aura lieu dans le périmètre défini de l'objet de l'intervention du bénévole. Mais l'activité altruiste ne relève pas des mêmes chemins de responsabilité que ceux du professionnel ».

non insonorisée…) n'est pas punissable pénalement »[73], ce qui est transposable en présence d'usage d'outils numériques.
Le secret et sa protection ont glissé vers la violation des données à caractère personnel et le jeu des notifications[74], par le responsable de traitement ou son sous-traitant, de la sécurité violée. La question est de savoir si une violation de sécurité constitue aussi une violation du secret ? Des représentants de la CNIL admettent qu'en France les acteurs sont peu transparents sur les obligations de notifications, de déclarer les failles mais aussi d'en informer les patients concernés[75], qui à leur tour ne peuvent porter plainte. La CNIL reconnaît que son but prioritaire est l'accompagnement[76], pour ne pas entacher la politique de circulation des données défendue corps et âme par l'Agence du Numérique en Santé[77] notamment. Or la CNIL indique que malgré le faible nombre de révélations (2825 notifications en 2020), 27 % de ces notifications reçues concernent des violations impactant plus de 1000 personnes et 69 % de celles-ci concernent des pertes de confidentialité[78] !
En outre, les sanctions ne sont qu'administratives : la CNIL a prononcé fin 2020 « des amendes de 3000 et 6000 euros à l'encontre de deux médecins libéraux. Les deux médecins, dont la CNIL n'a pas souhaité rendre l'identité publique (contrairement aux sanctions qui, elles, ont été publiées, "afin d'alerter les professionnels de santé sur leurs obligations et la nécessité de renforcer leur vigilance sur les mesures de sécurité apportées aux données personnelles qu'ils traitent"), ont manqué à leur obligation de : sécurité des données (art. 32 du RGPD) ; notifier la violation de données à la CNIL (art. 33 du RGPD) »[79]. On est très loin des condamnations infligées à Google et Amazon quant au dépôt ou à la lecture de cookies sur l'équipement de

[73] E. Raschel, *op. cit.*, Lexbase 2020 .

[74] RGPD, art. 4.12 et art. 32.

[75] G. Gautreneau (Ingénieur expert au service de l'expertise de la CNIL), « Approche institutionnelle », *in* L. Morlet-Haïdara (dir.), *Les cyberattaques dans les établissements de santé : enjeux et protections*, Université de Paris, colloque du 17 mai 2021.

[76] *Ibid.*

[77] J. Lucas et E. Sohier, Agence du Numérique en Santé (ANS), « Approche institutionnelle », *in* L. Morlet-Haïdara (dir.), *Les cyberattaques dans les établissements de santé : enjeux et protections*, Université de Paris, colloque du 17 mai 2021.

[78] G. Gautreneau, *op. cit.*, *in* L. Morlet-Haïdara (dir.), *Les cyberattaques dans les établissements de santé : enjeux et protections*, Université de Paris, colloque du 17 mai 2021.

[79] D. Duval-Arnoud, *op. cit.*, Dalloz Référence, 2019-2020, n° 135.750 : « La CNIL a en effet constaté qu'étaient librement accessibles les serveurs informatiques d'imagerie médicale permettant la consultation et le téléchargement d'IRM, scanners, radios, etc., ainsi que les noms, prénoms, date de naissance et date de consultation de près de 7000 patients. De plus, pour l'un des médecins, les données personnelles hébergées sur la base de données du logiciel d'images sont restées accessibles sans aucune authentification pendant une durée d'un peu moins de cinq ans, "prolongeant le risque que des tiers non autorisés accèdent aux données et puissent éventuellement les compromettre", a souligné la CNIL. L'autre médecin avait laissé l'accès aux données personnelles hébergées sur le disque dur de son ordinateur fixe, sans aucune authentification, pendant une durée d'environ quatre mois. Rappelons que la CNIL met à disposition un téléservice de notification de violation de données personnelles en cinq étapes (Délib. CNIL n° SAN-2020-014, 7 déc. 2020 Délib. CNIL n° SAN-2020-015, 7 déc. 2020). – « La CNIL prononce des amendes de 3000 et 6000 euros à l'encontre de deux médecins libéraux », Ed. législatives, 18 déc. 2020.

l'utilisateur[80]. La doctrine de la CNIL n'est donc pas étrangère à l'admission de secrets de « second rang » et de portée est moindre[81].
Que reste-t-il des autres sanctions ? Le secret professionnel relève des obligations déontologiques[82]. On ne trouve que de très rares décisions disciplinaires, sans sanction, ou globalement de faible portée : un avertissement ou une interdiction temporaire d'exercer de 1 à 3 mois[83]. Quant aux condamnations civiles, à des dommages et intérêts, de rares cas sont transigés mais la plupart des patients n'osent pas porter leur réclamation devant le juge, pour ne pas étaler davantage leur intimité, ne pas risquer des frais importants en contrepartie d'une indemnisation modique de ce type de préjudice.
On ne peut donc qu'espérer, peut-être un peu naïvement, que « Tant que la relation entre les professionnels du soin, du social et du médico-social et les patients demeurera, tant qu'elle ne

---

[80] A. Renard, « Cookies : la CNIL inflige 100 millions d'euros d'amende à Google et 35 millions d'euros d'amende à Amazon », Délib. CNIL n° SAN-2020-012, 7 déc. 2020, Google LLC et Google Ireland Ltd Délib. CNIL n° SAN-2020-013, 7 déc. 2020, Amazon Europe Core, Ed. législatives, 10 déc. 2020.

[81] V. Olech, *op. cit.*, n° 400 : « Le secret professionnel, soit le secret comme « moyen » juridique, semble de moins en moins privilégié pour assurer la préservation des données. Les critères, considérés par la doctrine, comme traditionnellement attachés à la désignation des personnes qui y sont astreintes, ne permettent plus d'expliquer certaines évolutions législatives. Il n'est pas certain, par ailleurs, que la nature des informations soit réellement importante dès lors qu'il est impossible d'évaluer avec certitude la portée de la désignation prévue à l'article L. 1110-4 du Code de la santé publique. L'on constate toutefois que les acteurs techniques et les personnes réutilisant les données sont explicitement soumis au secret professionnel. Ils ne semblent néanmoins pas bénéficier de l'option de conscience offerte aux professionnels de santé ou à ceux de l'action sociale et médico-sociale. Nous avons considéré qu'il s'agissait de secrets de « second rang » puisque leur portée est moindre. La norme est ainsi réduite à un instrument, il n'est plus tenu compte de ses fondements axiologiques. La doctrine de la CNIL n'est pas étrangère à cette évolution. La confiance, critère de la confidentialité, doit être créée à l'égard de tous les acteurs. Tandis que le secret professionnel était institué en raison de la confiance nécessaire que le professionnel devait inspirer en raison de rôle social, le secret professionnel est désormais un outil de confiance dans le traitement des données et dans les technologies numériques. ».

[82] C. santé publ., art. R. 4127-1 et s. – Les données couvertes par le secret correspondent à « tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris » (C. santé publ., art. R. 4127-4). Tous les professionnels intervenant dans le système de santé sont tenus au secret (C. santé publ., art. L. 1110- 4). Il peut donc s'agir notamment des médecins traitants, des médecins-conseils d'assurance... La divulgation d'une information à caractère secret par une personne qui en est dépositaire, notamment par sa profession, est punie d'un an d'emprisonnement et de 15 000 euros d'amende (C. pén., art. 226-13). De plus, le fait d'obtenir ou de tenter d'obtenir la communication des informations protégées en violation du secret médical fait encourir les mêmes sanctions (C. santé publ., art. L. 1110-4, V).

[83] C. Lantero, *La responsabilité ordinale*, Lexbase, 2020 : « Sont ainsi constitutifs de manquement au respect du secret professionnel : le fait de transmettre le compte rendu opératoire d'une intervention d'esthétique à l'avocat de son patient, document qui, en application des règles sur le secret professionnel, rappelées notamment à l'article R. 4127-4 du Code de la santé publique, aurait dû être adressé au seul patient (CDN, 24 avril 2009, n° 10031 : **avertissement**) ; le fait de publier des photographies de patients pour montrer son travail de chirurgie esthétique sur un site internet constitue (entre autres) un manquement au respect du secret professionnel (CDN, 15 mars 2010, n° 10320 : **3 ans d'interdiction dont deux avec sursis**) ; le fait d'écrire dans la presse sur la personnalité des gens, fussent-il des terroristes connus (CE, 27 janvier 2016, n° 392033, inédit : que « dès lors qu'il avait rencontré M. R. dans le cadre d'un entretien mené, au titre d'une expertise psychiatrique, dans l'exercice de sa profession de médecin psychiatre, M. D. était tenu au secret médical à son égard et qu'il n'en était délié ni par le refus de l'intéressé de se soumettre à son examen ni par la circonstance que certains éléments de la personnalité de M. R. avaient déjà fait l'objet d'informations à la disposition du public » (**interdiction d'exercer pendant 1 mois**) ; le fait de transmettre au directeur de l'ARS des éléments non anonymisés du dossier médical d'une de ses patientes et de mentionner pour les autres des éléments permettant de lever l'anonymat (CDN, 16 avril 2019, n° 13986 : **pas de sanction** néanmoins) ».

sera pas remplacée par un autre type d'interaction, hors du réel, c'est-à-dire tant que se formera une rencontre entre des individus, les règles juridiques, dont le secret professionnel, continueront à produire du sens. Quant à l'influence des dispositifs techniques de l'information et de la communication sur le « secret médical », il convient de prendre acte que le secret compris comme un moyen de préservation des données est, au moins partiellement, *transféré* dans l'architecture des objets pour empêcher l'accès des tiers, mais également les mésusages – c'est-à-dire les révélation involontaires – et, dans une certaine mesure, les révélations volontaires »[84].

[84] V. Olech, *op. cit.*, n° 487.