REVISTA DE DIREITO DA SAÚDE COMPARADO

Recebido em: 07/05/2025 Aceito em: 02/06/2025
DOI: https://doi.org/10.56242/direitodasaudecomparado;2025;4;6;5-10

La sécurité des données de santé

Cyril Aufrechter
Doctorant à l'Institut Droit et Santé.

Résumé

Introduction. I. L'obligation de cybersécurité. A. Eléments règlementaires et jurisprudentiels: l'exemple du droit français. B. La mise en œuvre du respect de cette obligation. II. La gestion de crise. III. Conclusion.

Introduction

Les spécialistes de la cybersécurité constatent régulièrement des fuites de données de santé particulièrement importante, comme celle contenant l'identité complète d'environ un demi-million de français avec, notamment, leur état de santé, leur mot de passe, leur numéro de sécurité sociale, leur adresse, et des commentaires comme « grossesse », ou « tumeur au cerveau »[1]. Une faille de sécurité particulièrement embarrassante qui est l'occasion de rappeler l'importance de l'obligation de sécurité, comment s'y conformer, mais aussi le comportement à adopter en cas de crise.

De manière générale, dans le secteur de la santé, les risques sont particulièrement importants. Ainsi, les attaques informatiques contre les hôpitaux sont courantes, comme en témoigne les épisodes subis par plusieurs d'entre eux récemment. En France, les hôpitaux de Dax et de Villefranche ont été victimes d'un cryptovirus qui a fortement impacté le système informatique et entrainé la mise en place de procédure dégradée[2]. Tel a également été le cas à Paris[3]. Et bien sûr, le Brésil n'est pas épargné[4]. La cybersécurité est donc un sujet crucial au niveau mondial.

La hausse exponentielle des attaques contre les acteurs du secteur de la santé impose de rappeler les obligations des responsables de traitements concernant la cybersécurité, et d'indiquer l'importance de la gestion de crise et surtout, de s'y préparer.

[1] D, Bancal, Plus de 400.000 données de patients français vendus dans le blackmarket, 14 février 2021. https://www.zataz.com/plus-de-400-000-donnees-de-patients-francais-vendus-dans-le-blackmarket/.
[2] Cyberattaque à l'hôpital : après Dax, celui de Villefranche "fortement impacté", 16 février 2021. https://www.lci.fr/societe/cyberattaque-a-l-hopital-apres-dax-celui-de-villefranche-sur-saone-fortement-impacte-2178482.html.
[3] 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.
[4] https://incyber.org/article/bresil-le-ministere-de-la-sante-victime-dune-cyberattaque-dampleur/.

Si cet article aborde la règlementation française conformément au RGPD, la manière de gérer la crise ne diffère pas selon les pays.

I. L'obligation de cybersécurité

A. Eléments règlementaires et jurisprudentiels: l'exemple du droit français

Assurer la sécurité des données personnelles est une obligation légale, au titre de l'article 32 du RGPD selon lequel *« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque »*.

De plus, les prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil[5] sont considérés comme étant des opérateurs de services essentiels (ou OSE) et sont donc soumis à la directive NIS 2, ce qui renforce leurs obligations.

L'obligation d'assurer la sécurité des données personnelles a été sanctionnée à plusieurs reprises par la CNIL. En théorie, la sanction maximale que la CNIL peut infliger est une amende administrative pouvant aller jusqu'à 10 millions d'euros ou jusqu'à 2 % du chiffre d'affaires annuel mondial, le chiffre le plus important étant retenu[6]. En pratique, si ce montant n'a pas encore été atteint, une entreprise hors secteur de la santé s'est vu sanctionner à hauteur de 400 000 euros par une délibération que la CNIL a rendue publique[7]. Des médecins libéraux se sont également vu sanctionner à hauteur de 3000 et 6000 euros en raison d'un manquement à la sécurité ayant pour origine une mauvaise configuration de leur box Internet, un mauvais paramétrage de leur logiciel d'imagerie médicale, et un défaut de chiffrement des images médicales conservées sur leurs serveurs ainsi qu'un défaut de notification des failles de sécurité à la CNIL[8].

L'obligation d'assurer la sécurité des données de santé n'est pas sanctionnée qu'en France. Ainsi, le 18 juin 2019, l'Autorité de protection des données néerlandaise a sanctionné un établissement hospitalier à hauteur de 460 000 euros pour défaut de contrôle des accès aux dossiers médicaux des patients. En l'espèce, le dossier médical d'un patient avait été consulté par environ 85 personnes non autorisées[9].

[5] Il s'agit de *« toute personne physique ou morale ou toute autre entité qui dispense légalement des soins de santé sur le territoire d'un État membre »*.
[6] RGPD, Article 83.
[7] Délibération de la formation restreinte n° SAN – 2019-005 du 28 mai 2019 prononçant une sanction pécuniaire à l'encontre de la société SERGIC.
[8] Délibération de la formation restreinte no SAN-2020-014 du 7 décembre 2020 concernant Monsieur [...] et Délibération de la formation restreinte no SAN-2020-015 du 7 décembre 2020 concernant Monsieur [...].
[9] Autorité de protection des données néerlandaise, Un hôpital condamné à une amende pour sécurité interne insuffisante des dossiers des patients, 16 juillet 2019. https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers.

Enfin, l'article L.226-17 du Code pénal sanctionne d'une peine de 5 ans d'emprisonnement et de 300 000 euros d'amende le défaut de mise en place de mesures de sécurité proportionnées au risque. Cette peine peut être appliquée à un dirigeant d'entreprise en cas de faute personnelle. Si cette sanction n'a pratiquement jamais été utilisée, ce risque ne doit pas pour autant être négligé.

Il ne faut pas oublier que si assurer la sécurité des données de santé est une obligation légale, cela est indispensable pour conserver la confiance des personnes concernées. Une confiance d'autant plus importante que la valeur des données de santé n'est pas négligeable, et que depuis le premier confinement suite a la COVID-19, les cyberattaques ont connu une augmentation exponentielle[10]. De fait, personne n'est à l'abri d'une faille de sécurité : tout responsable de traitement doit mettre en place des mesures de cybersécurité pour limiter les risques.

B. La mise en œuvre du respect de cette obligation

Mettre en place des mesures de cybersécurité signifie mettre en place des mesures proportionnées tant au risque qu'au responsable de traitement. Ainsi, un médecin libéral et un laboratoire pharmaceutique ne sont pas dans l'obligation de mettre en place les mêmes mesures de sécurité. Ces deux types de responsables de traitement ne font en effet pas face aux mêmes types de risques, et n'ont pas les mêmes moyens pour y faire face. De fait, s'ils doivent pour finir lutter contre les failles de sécurité et les attaques, et suivre des principes identiques, ils ne peuvent mettre en place des mesures strictement identiques. De prime abord, donner des règles générales concernant la cybersécurité est possible, mais elles doivent nécessairement être modulées en fonction du système d'information de chaque type de responsable de traitement.

Les risques peuvent concerner tant la confidentialité des données, que leur intégrité et leur disponibilité, et ils peuvent être non seulement externes, mais aussi internes[11]. Le risque est également proportionnel aux données en question, ainsi qu'à leur quantité.

La première chose à faire afin de respecter l'obligation de s'assurer de la sécurité des données traitées est de quantifier le risque en cause, afin de savoir contre quelles menaces le responsable de traitement doit et/ou veut se prémunir. Pour cela, il faut mener une analyse de risques. Il existe pour cela des méthodologies normalisées comme l'ISO 27005 ou le NIST Risk Management Framework. Cette analyse doit se faire au niveau du système d'information global pour prendre en compte les éventuels sous-traitants qui pourraient être une porte d'entrée vers le système du responsable de traitement. Sans une telle analyse, il y a un risque soit de mettre en place des moyens disproportionnés qui engendreront des coûts trop importants, soit d'être trop exposé à une attaque. Il y a donc un équilibre à trouver dans la gestion de la cybersécurité. Avoir une politique de sécurité des systèmes d'information mise à jour régulièrement[12] concourt à la sécurisation du système d'information. Des mesures de bons sens peuvent y être imposées, comme l'usage de

[10] E, Leclère, Cybercriminalité: avec le confinement, les attaques ont augmenté de 30 000 %, 5 mai 2020. https://www.franceinter.fr/justice/cybercriminalite-avec-le-confinement-les-attaques-ont-augmente-de-30-000.
[11] CNIL, Sécurité des données: les mesures d'hygiène pour protéger votre système d'information. https://www.cnil.fr/fr/securite-des-donnees-les-mesures-dhygiene-pour-proteger-votre-systeme-dinformation.
[12] ANSSI, PSSI. Guide d'élaboration de politiques de sécurité des systèmes d'information. https://www.ssi.gouv.fr/guide/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation/.

mots de passe solides, la sauvegarde régulière des données, l'usage d'antivirus, la séparation des usages personnels et professionnels, et la limitation de l'usage des WiFi publics ou inconnus[13]. Le chiffrement des données les plus sensibles peut également permettre de réduire les risques[14]. La cybersécurité et la protection des données personnelles doivent également être prévues dans la charte informatique et dans le règlement intérieur.

La deuxième chose à faire est d'avoir une procédure de gestion de crise. Cette procédure permet de savoir ce qu'il faut faire lorsqu'il y aura un incident de sécurité (notifications aux autorités, plaintes, gestion de la communication interne et externe). Cela permettra de ne pas avoir besoin de s'interroger sur ce qu'il faut faire lorsqu'une crise se produira, car il s'agit d'une situation particulièrement stressante. Il faut donc avoir des guides pour cadrer les actions et éviter d'aggraver la situation par des mesures inappropriées. Il faut également prendre en compte les réactions possibles des personnes concernées pour éviter par exemple des mouvements de paniques, ou des actions pouvant entacher durablement la réputation des responsables de traitement et/ou de leurs sous-traitants.

Les risques doivent également être gérés. Tel est notamment le cas du manque de sensibilisation des équipes, l'absence de maitrise des systèmes d'informations, ou un manque de respect des mesures de cybersécurité[15]. Cependant, avoir conscience de ces risques peut permettre de le limiter, par exemple par la mise en place de formations des équipes.

Plus largement, la mise en place d'audits prenants en compte l'intégralité du système d'informations, permettant de tester les mesures techniques et organisationnelles, sont nécessaires. Ces audits peuvent en effet permettre de déceler d'éventuelles failles ou à tout du moins des faiblesses, ce qui permettra d'apporter les correctifs nécessaires.

En toutes hypothèses, il est particulièrement important d'être en mesure de gérer la crise dans toutes ses dimensions.

II. La gestion de crise

Une faille de sécurité, ou violation de données[16], concernant les données est particulièrement critique. Cet évènement est donc particulièrement stressant en raison des conséquences potentiellement graves, tant pour le responsable de traitement que pour les personnes concernées. Si la crise a été anticipée, sa gestion sera facilitée : les équipes connaitront la procédure à suivre, ce qui évitera de se poser des questions pouvant ralentir les réactions, augmenter les inquiétudes et favoriser la prise de mauvaises décisions. Pouvoir s'en remettre à cette procédure sera rassurant

[13] Cybermalveillance, Les 10 mesures essentielles pour assurer votre sécurité numérique, 6 janvier 2021. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique.

[14] CNIL. 4 réflexes pour mieux protéger votre identité en ligne, 19 octobre 2017. https://www.cnil.fr/fr/4-reflexes-pour-mieux-proteger-votre-identite-en-ligne.

[15] ANSSI, L'ANSSI et le BSI alertent sur le niveau de la menace cyber en France et en Allemagne dans le contexte de la crise sanitaire : https://www.ssi.gouv.fr/actualite/lanssi-et-le-bsi-alertent-sur-le-niveau-de-la-menace-cyber-en-france-et-en-allemagne-dans-le-contexte-de-la-crise-sanitaire/

[16] Défini par l'article 4.12 du RGPD comme étant : *« une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »*.

pour le responsable de traitement, qui pourra mieux gérer la situation.

La gestion de la crise devant inclure toutes ses dimensions, elle ne doit pas être effectuée que par le service informatique. Celui-ci devra, potentiellement avec l'aide d'un prestataire ou des services de l'État, analyser le mode d'action des attaquants pour pouvoir s'assurer qu'ils ne sont plus implantés dans le système, et prendre les mesures nécessaires pour rétablir l'intégrité du système d'information. Il devra aussi être en mesure de fournir le plus d'éléments possible (preuves de la violation de données, récupération des sauvegardes au besoin, ...). De fait, le DSI et RSSI seront indispensables.

De plus, si la preuve de la violation sera établie par le service informatique, les juristes devront s'assurer que celle-ci a été établie légalement, notamment conformément au principe de loyauté de la preuve. Les questions de l'éventuel engagement de la responsabilité d'un prestataire et de la déclaration de sinistre devront également être étudiées. Il est également envisageable de porter plainte.

Être certain que la règlementation a été respectée et continue de l'être peut éventuellement avoir pour effet de rassurer les équipes, car si les mesures nécessaires ont été prises, les juristes pourront confirmer que le risque juridique est très limité. Il s'agira ainsi d'une information positive dans un contexte difficile.

L'équipe juridique d'un prestataire dont la responsabilité peut être engagée a également un rôle important. Elle doit en effet indiquer le risque juridique en cause causé par le manquement, permettant d'agir en conséquence. Des actions à effectuer pour un prestataire ayant commis un manquement (par exemple un défaut de sécurité qui aurait dû être détecté) peuvent inclure une assistance renforcée avec le responsable de traitement pour gérer la crise. L'objectif sera en effet de s'assurer que malgré le manquement en cause, la responsabilité du prestataire ne soit pas engagée si possible et qu'un accord soit trouvé entre les parties pour régler la situation à l'amiable. Le service informatique du prestataire devra également aider à prendre la mesure de la faille de sécurité et sa gestion. Dans tous les cas, les partenaires de l'entité touchée par cette attaque devront également être prévenus pour qu'ils s'assurent de ne pas avoir été touchés par celle-ci, ou ne pas le devenir. Prévenir les partenaires qu'il y a eu une cyber-attaque est également une bonne pratique. En effet, si ce n'est pas obligatoire, faire courir le risque que l'attaque se reproduise chez les partenaires peut avoir des impacts sur la confiance. Personne n'aime apprendre par les médias qu'il coure un risque de cyber-attaque par ricochet, et qu'il n'a pas été prévenu par la personne leur faisant courir ce risque.

Tout au long de la crise, l'équipe chargée de la protection des données devra être en mesure d'échanger avec les autorités. Il peut s'agir simplement d'une notification, mais cette autorité peut demander des informations supplémentaires, et il est nécessaire que le responsable de traitement soit en mesure de démontrer que la situation est prise au sérieux. Les obligations de notifications sont précisées par des lignes directrices qui indiquent par exemple que cette procédure est nécessaire si des données médicales critiques concernant les patients d'un hôpital sont rendues indisponibles, temporairement, car cela peut présenter un risque pour les personnes concernées, des opérations pouvant être annulées et des vies mises en danger[17].

Un autre service indispensable dans la gestion de la crise est la communication. Cette

[17] CEPD, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE)2016/679 - Adoptées le 3octobre2017Version révisée et adoptée le6février2018.

communication doit d'abord être interne, et avoir vocation à informer le personnel sur la situation et le rassurer. En effet, la situation sera potentiellement stressante pour l'ensemble du personnel qui peut ne plus être en mesure d'utiliser les outils informatiques. Une bonne communication interne peut alors permettre d'éviter de fragiliser les équipes et les rassurer sur le suivi des opérations. Elle peut et doit également permettre de s'assurer que les canaux de communication sont contrôlés : si des employés donnent des informations sur une attaque en cours, cela peut à la fois gêner l'enquête, et risquer de déstabiliser un peu plus le responsable de traitement. Tel peut également être le cas si de fausses informations sont diffusées (y compris de bonne foi).

La communication externe est également indispensable. Il s'agira, en coordination avec les autres services, de faire l'éventuelle notification aux personnes concernées en des termes clairs concernant l'attaque subie, ainsi que les procédures en cours. Mais il peut également s'agir de gérer les relations avec les personnes concernées qui reviendraient vers le responsable de traitement avec des interrogations (le cas échéant avec le service juridique, y compris le DPO). Le grand public étant informé de l'existence du RGPD et de possibilités de poursuites judiciaires, il faut assurer un suivi des réseaux sociaux pour éviter que la situation ne devienne incontrôlable suite à des rumeurs, de fausses informations ou simplement une mauvaise compréhension de la situation. De plus, la gestion des relations avec la presse peut également être nécessaire.

La gestion de la crise ne sera pas strictement identique suivant la nature et la taille de l'entreprise, ou suivant que le DPO soit interne ou externe, ou en l'absence de DPO. Il ne s'agit donc que de lignes directrices qu'il faut adapter à chaque entreprise, et se préparer régulièrement à une attaque informatique pour éviter un risque de déstabilisation globale de l'entreprise.

III. Conclusion

L'obligation d'assurer la sécurité des données de santé est donc complexe et sa mise en œuvre diffère selon les personnes en assurant la gestion. Il n'y a pas une solution unique, car un médecin seul dans son cabinet, une entreprise ou un hôpital n'ont pas les mêmes moyens, et ne font pas face aux mêmes types de menaces, d'où l'importance de l'analyse de risque qui fournit les éléments permettant cet ajustement du dimensionnement. Cependant, dans tous les cas, un manquement grave aux obligations de garantir la sécurité des données sera sanctionné proportionnellement à la taille du responsable de traitement, mais toujours sévèrement.

La gestion de crise quand elle concerne le vol de données doit être conçue pour prendre en compte toutes les dimensions : les services informatique, juridique et communication devront travailler ensemble de manière coordonnée. Cela ne peut se faire sans préparation.

Les attaques informatiques sont en très forte hausse, notamment contre les acteurs du secteur de la santé. Mieux vaut donc se préparer pour éviter les multiples conséquences d'un vol de données de santé qui pourraient impacter la pérennité de l'entité qui est responsable de traitement que de se retrouver en pleine tempête avec des équipes obligées d'improviser.