La mise en place de mesures de sécurité techniques et organisationnelles : *not just a checklist !*

Zarmine Hussain, le 14 mars 2023

Le Conseil de l'Hôpital de la région d'Uppsala se voit imposer une amende administrative de SEK 1'600'000 par l'autorité suédoise de protection des données pour violation des exigences de la sécurité des données. En cause, la transmission par courriel de données médicales à des destinataires situés dans des pays tiers, ainsi que le stockage de données sensibles sur l'application de messagerie électronique Microsoft Outlook.

L'affaire suédoise

En date du 7 mai 2019, les autorités régionales d'Uppsala en Suède ont notifié à l'autorité suédoise de protection des données (l'*Integritetsskyddsmyndigheten*, l'IMY) une violation de données survenue dans leur juridiction en 2019. Sur la base de cette notification, l'IMY a entamé une investigation concernant la transmission de données médicales par l'Hôpital Universitaire d'Uppsala (Hôpital) aux patients à l'étranger ainsi qu'aux hôpitaux étrangers qui ont référé ces derniers à l'Hôpital. Il sied de préciser que l'IMY a choisi d'examiner le cas uniquement sous l'angle de la conformité aux exigences de sécurité, sans examiner la conformité aux dispositions sur la communication de données personnelles à l'étranger.

Conformément aux procédures internes de l'Hôpital, une fois le traitement médical d'un patient résidant à l'étranger terminé, tant le patient que l'hôpital étranger qui avait référé ce dernier à l'Hôpital avaient le choix de recevoir le rapport médical par courriel. Ce dernier comportait notamment les informations relatives à la santé du patient, les coordonnées du patient et l'identité du médecin traitant. L'Hôpital a envoyé environ 500 à 1000 courriels mensuels de ce type, concernant environ 300 patients par an de 2014 à 2019.

En outre, ces courriels étaient envoyés sans chiffrement depuis 2014. Ce n'est qu'en septembre 2019 que l'Hôpital a introduit une solution de chiffrement de courriels adéquate. Dans l'intervalle, l'Hôpital a activé le paramètre de chiffrement « *Transport Layer Security* » (TLS) de l'application de messagerie électronique Microsoft Outlook (Outlook). Toutefois, si le service de messagerie web du destinataire ne comprenait pas le TLS, les courriels étaient transmis au destinataire sans chiffrement. Ainsi, l'Hôpital utilisait une mesure de chiffrement qui dépendait des paramètres techniques du destinataire, de sorte que l'Hôpital ne pouvait

pas garantir la transmission chiffrée du courriel et des données personnelles. Par conséquent, les données pouvaient être lues en clair, avec pour conséquence que des personnes non autorisées pouvaient accéder aux données sensibles. Par ailleurs, une fois envoyés, les courriels, y compris les données médicales, demeuraient sur le compte Outlook de l'Hôpital.

L'IMY relève également que le gouvernement local d'Uppsala avait émis une politique concernant le traitement des courriels. Il y interdisait spécifiquement la communication de données sensibles par courriel. Par conséquent, l'Hôpital était au courant des risques posés par son traitement de données et a omis d'implémenter les mesures techniques et organisationnelles nécessaires.

Par conséquent, selon l'IMY, compte tenu notamment du fait qu'un grand nombre de données personnelles sensibles ont été exposées sur Internet pendant une longue période sans protection contre une divulgation ou un accès non autorisé, la violation de la sécurité a été d'une nature si grave qu'elle constitue non seulement une violation de l'art. 32 ch. 1 RGPD, mais également une violation du principe de l'assurance de la confidentialité et de l'intégrité au sens l'art. 5 ch. 1 let. f RGPD.

Au vu de ce qui précède, l'IMY a imposé une amende de SEK 1'600'000 (équivalent à environ EUR 150'000) à l'Hôpital.

Analyse sous l'angle du droit suisse

Le point principal du cas précité qui mérite d'être analysé sous l'angle du droit suisse est celui de la détermination des mesures de sécurité appropriées pour un hôpital universitaire ou toute autre collectivité publique traitant des données sensibles. Bien que les faits du présent cas soulèvent également des questions relatives au secret médical, ces dernières ne seront pas abordées dans la présente contribution.

En transposant les faits en droit suisse, il sied de préciser que les traitements de données personnelles par des organes cantonaux tels que les hôpitaux universitaires sont soumis aux législations cantonales sur la protection des données.

À titre illustratif, les traitements des données personnelles effectués par les hôpitaux universitaires de Genève sont notamment couverts par la Loi genevoise du 5 octobre 2001 sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD ; RS/GE A 2 08) et son Règlement d'application du 21 décembre 2011 (RIPAD ; RS/GE A 2 08.01). L'application de la législation genevoise en matière de protection des données

découle notamment de l'art. 3 al. 1 let. d de la Loi genevoise du 22 septembre 2017 sur l'organisation des institutions de droit public (LOIDP ; RS/GE A 2 24) et l'art. 3 al. 1 let. c LIPAD.

En date du 6 juillet 2022, un avant-projet de loi modifiant la LIPAD (AP-LIPAD) a été mis en consultation par le Conseil d'État genevois jusqu'au 17 octobre 2022. Dans la mesure où – au moment de la rédaction de la présente contribution – le projet de loi définitif n'a pas encore été publié, la présente analyse se fonde uniquement sur l'AP-LIPAD.

L'AP-LIPAD s'inspire de la nouvelle Loi fédérale du 25 septembre 2020 sur la protection des données du 25 septembre 2020 (nLPD) qui, pour rappel, entrera en vigueur le 1er septembre 2023 (cf. www.swissprivacy.law/168). L'AP-LIPAD a notamment pour objectif de conférer à la loi genevoise un « niveau de protection adéquat » au sens du RGPD. Par conséquent, certaines dispositions étant calquées sur celles de la nLPD, leur interprétation en est facilitée.

Selon l'art. 37 al. 1 LIPAD, les données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques appropriées. Selon l'art. 37 al. 2 LIPAD, les institutions prennent, par le biais de directives ainsi que de clauses statutaires ou contractuelles, les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent ou font traiter. L'art. 37 LIPAD est précisé par les art. 13 et 13A RIPAD.

L'AP-LIPAD approfondit les exigences en matière de sécurité des données. L'art. 37A AP-LIPAD est globalement calqué sur l'art. 8 nLPD et matérialise l'approche fondée sur les risques. En d'autres termes, plus le risque d'une atteinte à la sécurité des données est élevé, plus les exigences auxquelles doivent répondre les mesures à prendre le sont également. Les exigences minimales en matière de sécurité des données seront déterminées par le Conseil d'État par voie réglementaire (art. 37A al. 3 AP-LIPAD). À notre avis, l'on peut raisonnablement s'attendre à ce que ces exigences minimales soient calquées sur les exigences de l'art. 3 de l'Ordonnance fédérale du 31 août 2022 sur la protection des données (OPDo).

Conformément à l'art. 3 al. 2 let. a OPDo, le responsable du traitement doit, pour assurer notamment l'intégrité des données personnelles, prendre des mesures appropriées afin que les personnes non autorisées ne puissent pas lire, copier, modifier, effacer ou détruire des données personnelles lors de leur communication.

S'agissant spécifiquement du secteur médical, il sied également de rappeler que la Loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP ; RS 816.1), l'Ordonnance du

22 mars 2017 sur le dossier électronique du patient (ODEP ; RS 816.11), ainsi que l'Ordonnance du 22 mars 2017 du DFI sur le dossier électronique du patient (ODEP-DFI ; RS 816.111), énoncent un certain nombre de règles et d'exigences et techniques précises, notamment relatives au transfert des données médicales contenues dans le dossier électronique du patient (cf. art. 10 ODEP) et à la sécurité de ces données (cf. notamment les art. 10 al. 3 ODEP et 12 ODEP). Dans la mesure où une institution ne serait pas directement soumise aux normes précitées, ces dernières peuvent néanmoins être utilisées comme base afin de déterminer les règles de sécurité appropriées pour la communication électronique de données médicales.

Plusieurs enseignements nous paraissent pouvoir être tirés du cas suédois faisant l'objet de la présente contribution :

- Les responsables du traitement devraient faire preuve de proactivité et anticiper l'inefficacité d'une mesure de chiffrement telle que dans le cas de l'Hôpital suédois, en particulier lorsque des données sensibles sont en jeu.
- Dans l'hypothèse où un établissement public, qu'il soit médical ou non, instaurerait une telle mesure de sécurité défaillante, l'on peut s'attendre à ce que cela soit considéré notamment comme une violation des prescriptions de l' 37A AP-LIPAD.
- Dans la mesure où les problèmes de chiffrement rencontrés par l'Hôpital suédois peuvent survenir facilement, il devrait en règle générale être recommandé, comme bonne pratique, que les hôpitaux (qu'ils soient publics ou privés), ainsi que les autres entités qui traitent des données sensibles, mettent en place un système permettant le téléchargement à distance des données sensibles par la personne concernée et/ou par des tiers autorisés, conformément par exemple aux tendances des initiatives relatives au dossier électronique du patient.

À titre d'observation conclusive, on relèvera encore que la décision de l'IMY soulève, à notre sens, une problématique fondamentale du droit de la protection des données : le seuil de diligence du responsable du traitement. À travers sa décision, l'IMY semble exiger du responsable du traitement de prendre en compte des paramètres dont il n'a aucune maîtrise et d'anticiper les faiblesses de sa contrepartie. En imposant une telle diligence accrue, on pourrait s'interroger sur la tendance de déresponsabiliser la personne concernée ainsi que sur l'éventuelle efficacité d'un cadre réglementaire qui semble devenir de plus en plus difficile à respecter, respectivement qui engendre des coûts croissants, pour les responsables du traitement.

Proposition de citation : Zarmine HUSSAIN, La mise en place de mesures de sécurité techniques et organisationnelles : *not just a checklist !*, 14 mars 2023 *in* www.swissprivacy.law/208

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.