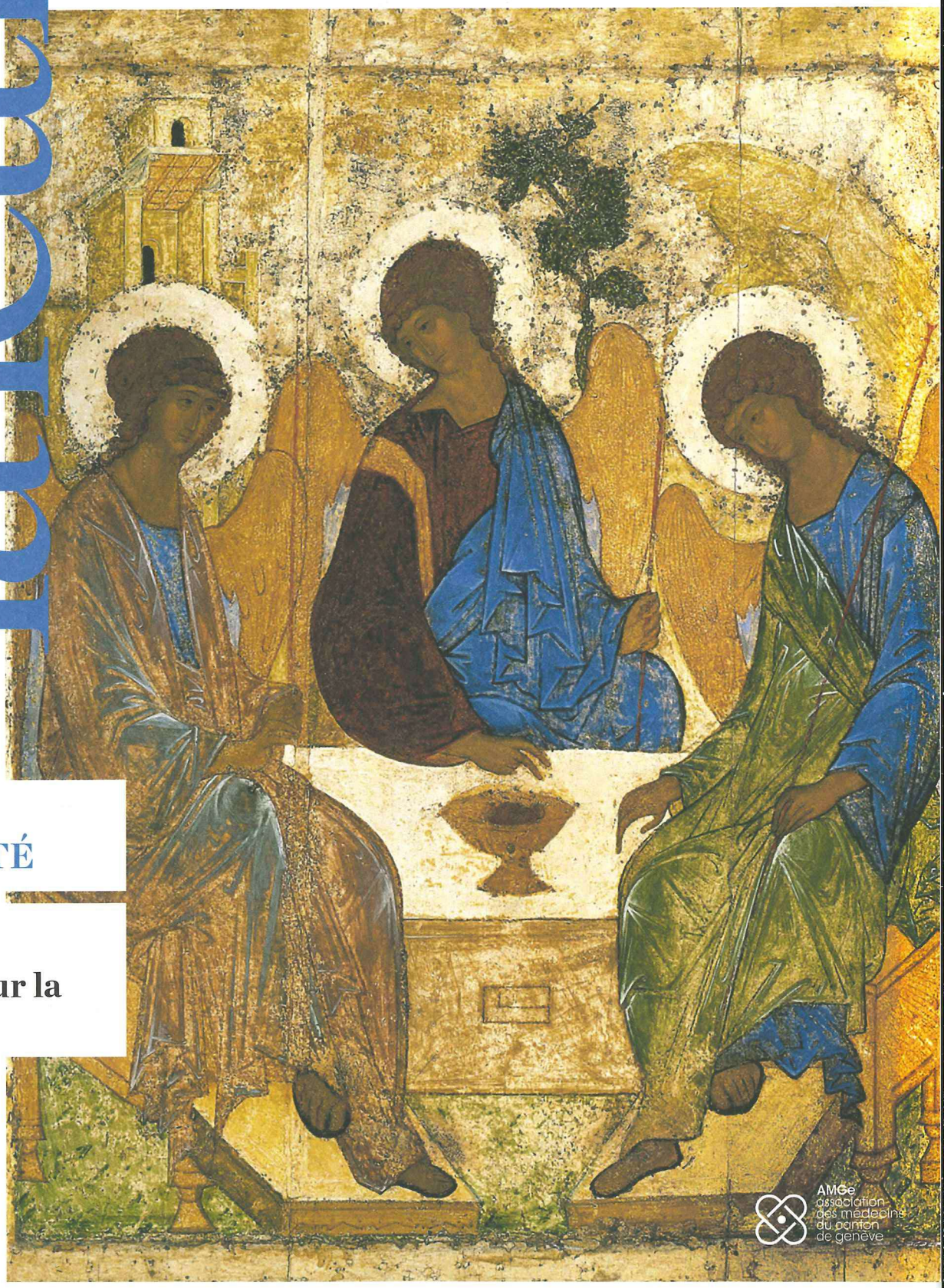
12/2022-01/2023
N° IX

la lettre

Éclairages
SMGe-AMGe



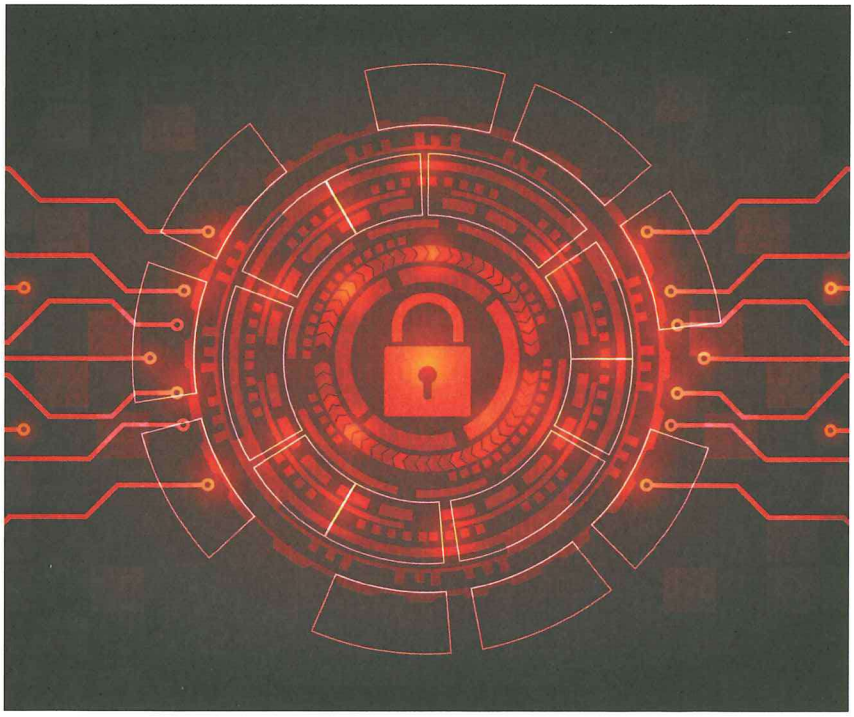
CYBER-SÉCURITÉ

ICÔNES
Fenêtre sur la lumière

AMGe
association des médecins du canton de genève

Cyber-attaque par rançongiciel: aspects juridiques

Depuis 2016, on observe une forte croissance des attaques par rançongiciel contre des PME suisses actives dans le domaine de la santé. De telles attaques visent non seulement des centres hospitaliers, mais aussi des cabinets médicaux et des médecins individuels, voire des centres de facturation. Le fait que le domaine de la santé soit une cible de choix pour les *hackers* tient en particulier au fait que les données de patients ont une valeur marchande très forte sur le *dark web*.



La présente contribution a pour but de présenter succinctement les obligations légales qui incombent au médecin, ainsi que les conséquences légales qu'il est susceptible d'encourir en cas de cyber-attaque par rançongiciel[1].

Obligations légales découlant des législations sur la protection des données

Lorsqu'on envisage le risque d'une attaque par rançongiciel, trois obligations découlant des législations de protection des données apparaissent fondamentales: l'obligation d'assurer la sécurité des données, les obligations spécifiques en matière de sous-traitance et les obligations en cas de violation de la sécurité des données.

La protection des données étant régie par de nombreuses lois[2], on se concentrera, afin de simplifier le propos, sur la nouvelle Loi fédérale sur la protection des données (nLPD) qui entrera en vigueur en septembre 2023[3].

Obligation d'assurer la sécurité des données

En amont de toute cyber-attaque, le médecin, ainsi que ses sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru[4]. Cette obligation se fonde sur une approche basée sur les risques. Plus le risque d'une atteinte à la sécurité des données est élevé, plus les exigences auxquelles doivent répondre les mesures à prendre seront élevées.

Pour déterminer concrètement quelles sont les mesures organisationnelles et techniques appropriées, on se référera notamment (i) aux art. 1 à 6 de la nouvelle Ordonnance sur la protection des données (nOPDo), (ii) aux publications

des autres auteurs du présent numéro, ainsi que (iii) aux recommandations publiées par le Centre national pour la cybersécurité NCSC à destination du secteur de la santé le 28 juillet 2022[5].

Cela étant, comme les technologies et les méthodes des *hackers* évoluent constamment, il est nécessaire de réévaluer régulièrement si les mesures mises en place demeurent adéquates.

Obligations en cas de sous-traitance
Il est admis que le médecin peut externaliser certaines tâches, notamment informatiques, à un ou des sous-traitants[6].

En amont de toute cyber-attaque, le médecin doit ainsi s'assurer de manière active que le sous-traitant respecte la loi dans la même mesure que lui. En particulier, celui-là doit veiller à choisir soigneusement son mandataire, à lui donner les instructions adéquates et à exercer la surveillance nécessaire au vu des circonstances[7].

Obligation d'annoncer et documenter les violations de la sécurité des données
En cas de cyber-attaque et si la violation de la sécurité des données entraîne vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le médecin doit l'annoncer dans les meilleurs délais au Préposé fédéral à la protection des données et à la transparence (PFPDT)[8].

À notre sens, une telle annonce sera en principe toujours nécessaire pour le médecin victime d'un rançongiciel car il conviendra de partir du principe, dans le doute, que la cyber-attaque entraîne un risque élevé pour la personnalité ou les droits fondamentaux des patients. Le médecin devra également annoncer le cas aux patients concernés lorsque cela est nécessaire à leur protection ou lorsque le PFPDT l'exige[9].

« Une cyber-attaque fait peser des conséquences juridiques potentiellement très lourdes sur le médecin. Pour s'en prémunir, il lui appartient de prendre toutes les mesures nécessaires pour assurer une sécurité adéquate des données de ses patients au regard des risques encourus. »

À noter que le médecin doit également documenter les violations de la sécurité des données et conserver cette documentation pendant au moins deux ans à compter de la date d'annonce au PFPDT[10].

Risques juridiques encourus par le médecin

Sanctions en raison d'une violation du secret médical ?
Si les hackers exfiltrent les données de patients puis les publient sur Internet, il y a une divulgation d'informations couvertes par le secret médical à des tiers non autorisés. Se pose alors la question de savoir si le médecin peut se voir reprocher une éventuelle violation du secret médical.

Du point de vue du droit pénal, la violation du secret médical est réprimée par l'art. 321 du Code pénal (CP) qui prévoit une peine privative de liberté de trois ans au plus ou une peine pécuniaire.

Une violation de l'art. 321 CP peut être réalisée par omission notamment lorsqu'un défaut de surveillance peut être reproché au médecin[11]. Cependant, il n'y a violation du secret médical au sens de l'art. 321 CP que si le médecin agit intentionnellement ; s'il agit par négligence, il ne commet aucune infraction pénale. En matière de violation du secret médical, la frontière entre intention et négligence est parfois difficile à tracer[12]. À notre sens, une violation de l'art. 321 CP ne devrait pas pouvoir être reprochée au médecin si ce dernier a pris des mesures de sécurité informatique adéquates, mais que celles-ci n'ont pas permis d'empêcher la cyber-attaque ayant entraîné la divulgation à des tiers non autorisés d'informations couvertes par le secret médical.

Du point de vue du droit disciplinaire, la violation du secret médical est sanctionnée par un corpus de règles dispersées. On se limitera à mentionner ici l'art. 43 al. 1 de la Loi sur les professions médicales (LPMéd)[13], ainsi que les normes associatives auxquelles les médecins se soumettent, telles l'art. 34 des Statuts de l'Association des médecins du Canton de Genève[14]. Ces normes prévoient des sanctions comprenant l'avertissement, le blâme, l'amende, et une interdiction de pratiquer temporaire ou définitive. Contrairement à ce qui prévaut en droit pénal, la violation du secret médical par négligence peut conduire au prononcé de sanctions disciplinaires à l'encontre du médecin[15].

Sanction en raison d'une violation de l'obligation d'assurer la sécurité des données ?
Sont punis, sur plainte, d'une amende de 250 000 francs au plus les personnes privées qui, intentionnellement, ne respectent pas les exigences minimales en matière de sécurité des données conformément à l'art. 8 nLPD[16].

Pour les mêmes raisons qu'exposées ci-dessus en lien avec l'art. 321 CP, une condamnation pénale du médecin pour violation des exigences minimales de sécurité découlant de l'art. 8 nLPD en raison d'une attaque par rançongiciel ne devrait pas pouvoir lui être reprochée s'il a mis en place des mesures de sécurité adéquates.

Procès intenté par le patient en responsabilité civile et contractuelle du médecin ?
Plus le patient subira des atteintes graves en raison de la cyber-attaque dont son médecin aura été victime, plus il sera susceptible d'initier un procès en responsabilité civile et contractuelle contre celui-ci pour lui réclamer le paiement de dommages-intérêts.

Le montant des dommages-intérêts réclamés dépendra des circonstances du cas d'espèce, en particulier des griefs soulevés par le patient. La réparation pécuniaire réclamée sera probablement limitée si le patient se plaint d'une violation par négligence du secret médical. Le montant pourra être sensiblement plus élevé si le patient se plaint d'une erreur médicale lui ayant causé de graves séquelles. Le montant atteindra des sommets si le conjoint survivant se plaint d'une erreur médicale ayant causé le décès de son conjoint[17] et réclame le paiement d'une indemnité pour perte de soutien[18].

Conclusion

Une cyber-attaque fait peser des conséquences juridiques potentiellement très lourdes sur le médecin. Pour s'en prémunir, il lui appartient de prendre toutes les mesures nécessaires pour assurer une sécurité adéquate des données de ses patients au regard des risques encourus. Concrètement, le médecin devra démontrer avoir réfléchi à la question, avoir trouvé des solutions et avoir pris les mesures préventives nécessaires. ●

Maître Grégoire Chappuis
Etude Python Avocats (Genève) SA

Référence

1. Le rançongiciel (ou *ransomware*) est un type de logiciel malveillant qui infecte les fichiers et systèmes informatiques de la cible. Ses données sont alors cryptées et ses systèmes informatiques rendus inexploitables jusqu'au paiement de la rançon demandée par les *hackers* (cf. Rapport semestriel 2020/2 [juillet à décembre] du Centre national pour la cybersécurité NCSC du 11 mai 2021, p. 11 ss.).
2. Il peut s'agir de la Loi fédérale sur la protection des données, d'une loi cantonale telle que la Loi genevoise sur l'information du public, l'accès aux documents et la protection des données personnelles et/ou du Règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).
3. Le lecteur est rendu attentif au fait que l'étendue des obligations décrites ci-après peut varier, en particulier si le médecin est soumis au RGPD, ce qui sera souvent le cas pour les patients domiciliés dans un pays de l'Union Européenne.
4. Art. 7 et 8 al. 1 nLPD
5. https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2022/empfehlungen-gesundheitssektor.html (consulté le 23.11.2022)
6. Art. 9 al. 1 et 2 nLPD.
7. Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, Feuille fédérale 2017 p. 6565 ss, p. 6651.
8. Art. 24 al. 1 nLPD. Les points que l'annonce doit couvrir sont prévus à l'art. 24 al. 2 nLPD, ainsi qu'à l'art. 15 nOPDo.
9. Art. 24 al. 4 nLPD.
10. Art. 15 al. 4 nOPDo.
11. Erard, Frédéric, *Le secret médical*, thèse, 2021, n. 461 et 469.
12. Si le médecin estime que la réalisation de l'infraction est possible et s'accommode de cette possibilité, il viole le secret médical par dol éventuel, ce qui constitue une forme de l'intention. En revanche, si le médecin estime que la réalisation de l'infraction est possible mais compte sur le fait qu'elle ne se produira pas, alors il agit par négligence consciente (et non intentionnellement) si la cyber-attaque qu'il a subie a entraîné la divulgation à un tiers non autorisé des données couvertes par le secret. Dans un tel cas, le médecin ne viole pas l'art. 321 CP.
13. L'art. 40 let. f LPMéd réaffirme l'obligation du médecin d'observer le secret médical.
14. Les membres de l'AMGe s'engagent à respecter notamment le Code de déontologie de la Fédération des médecins suisses (FMH), dont l'art. 11 impose aux membres de respecter le secret médical.
15. Erard, Frédéric, op. cit., n. 461, 469 et 709.
16. Art. 61 let. c nLPD.
17. À noter qu'en septembre 2022, les médias ont fait état du premier patient décédé en Europe en raison d'une cyber-attaque : https://www.sante.org/le-blog-sante.org/first-death-caused-by-cyber-attack (consulté le 23.11.2022)
18. Art. 45 al. 3 du Code des obligations.