



Réponse du Conseil d'Etat à un instrument parlementaire

Question Zurich Simon / Rey Alizée

2022-CE-128

Sécurité des données des patient-e-s : mieux protéger les Fribourgeois-e-s !

I. Question

Des milliers de Neuchâtelois-es ont appris avec effroi que leurs données avaient été publiées sur le darknet. On peut y apprendre que son voisin est séropositif, qu'une connaissance consomme des drogues ou qu'une de ses proches a interrompu une grossesse. On y trouve les résultats des examens médicaux les plus intimes. Ce nouveau vol de données expose à la vue de toutes et tous ce que certaines personnes ne partagent parfois même pas avec leurs proches.

Les cabinets médicaux qui ont été victimes de ces attaques suivaient probablement les directives reçues de la part de leurs prestataires informatiques. Au vu de la recrudescence des attaques, les organisations sanitaires fribourgeoises et les patient-e-s qui recourent à leurs services ne sont pas à l'abri. Il devient donc urgent de prévoir des mesures de soutien efficaces.

Nous posons dès lors au Conseil d'Etat les questions suivantes :

1. Que le Conseil d'Etat entend-il faire pour renforcer la sécurité des données des patient-e-s fribourgeois-es ?
2. Evalue-t-il des exigences supplémentaires liées à la planification hospitalière ou un soutien accru à certains acteurs, comme les cabinets médicaux p. ex. ? Si non, pourquoi le Conseil d'Etat n'estime-t-il pas pertinent d'agir par ces biais-là ? Si oui, qu'entend-il faire concrètement ?
3. L'HFR dispose-t-il des moyens nécessaires pour assurer une sécurité suffisante des données traitées ?
4. La Police cantonale dispose-t-elle des ressources nécessaires pour mener les enquêtes ?
5. Que le Conseil d'Etat recommande-t-il de faire aux personnes – patient-e-s et organisations de santé – qui ont été victimes d'une attaque ?

1^{er} avril 2022

II. Réponse du Conseil d'Etat

En préambule, le Conseil d'Etat rappelle que la sécurité des données désigne toutes les mesures techniques et organisationnelles prises pour éviter la perte, la manipulation, l'accès non autorisé et la falsification de données et d'informations. Elle comprend la confidentialité, l'intégrité et la disponibilité des données. La protection des données garantit, quant à elle, à toute personne, le droit d'être protégée contre l'emploi abusif des données qui la concernent (art. 13 al. 2 Constitution fédérale).

De façon générale, la réalisation des mesures liées à la sécurité et à la protection des données est de la responsabilité des unités ou organes qui traitent les données. Elle est régie, au niveau cantonal, par la loi sur la protection des données (LPrD) et, au niveau fédéral, par la loi fédérale sur la protection des données (LPD). Les deux législations prévoient l'obligation pour les responsables du traitement (qui sont en principe les détenteurs/trices de données) d'en assurer la sécurité (art. 8, 12b – 12e et 17 LPrD et art. 7 et 10a al. 2 LPD). Ainsi, la législation sur la protection des données inclut des mesures concernant la sécurité des données. Pour ce qui concerne spécifiquement les cabinets médicaux qui sont régis par la LPD, le médecin est le/la responsable du traitement, ceci même lorsqu'il/elle sous-traite tout ou une partie des prestations informatiques (art. 3 let. i LPD). Ce statut implique un certain nombre d'obligations quant à la sécurité des données, notamment la définition des droits d'accès ou le devoir d'information envers les patient-e-s en cas de menace ou d'attaque informatique. Un des enjeux principaux lié à ce devoir d'information est de permettre aux patient-e-s de se protéger des conséquences directes du piratage et de réduire le risque d'autres dommages consécutifs.

S'agissant de la surveillance, ce sont les préposé-e-s fédéral-e et cantonal-e à la protection des données qui sont chargés de surveiller l'application de la législation en vigueur et d'émettre des recommandations en la matière, en sus des conseils.

Ainsi, pour les institutions de santé publique fribourgeoises (établissements médico-sociaux et hôpitaux mandatés), le droit cantonal s'applique et c'est l'Autorité cantonale de la transparence, de la protection des données et de la médiation (ATPrDM), par le biais de sa préposée cantonale à la protection des données et de sa Commission, qui a pour tâches de conseiller les organes concernés. En particulier lors de l'étude de projets de traitement de données personnelles l'ATPrDM renseigne les personnes sur leurs droits, collabore avec les autorités cantonales de protection des données et celles de la Confédération, tient le registre des fichiers et examine l'adéquation du niveau de protection assuré à l'étranger. S'agissant de la surveillance, la préposée effectue notamment des vérifications systématiques auprès des organes concernés. A noter qu'il n'y a aucune obligation légale actuelle à ce qu'un traitement de données soit soumis à l'ATPrDM avant son déploiement. Toutefois, une fois le déploiement effectué, l'ATPrDM peut à tout moment faire un contrôle. C'est à ce moment qu'elle va notamment évaluer le concept de sûreté de l'information et protection des données (SIPD), les bases légales et les contrats, notamment ceux relatifs à la sous-traitance.

Au vu de ce qui précède, tout traitement de données personnelles effectué par un organe public est de la responsabilité du/de la responsable du traitement (à savoir la cheffe/le chef de l'entité). Il/elle a ainsi la responsabilité de mettre en œuvre les dispositions de la LPrD pour les données dont il/elle a la charge.

Pour le secteur privé dont font partie les cabinets médicaux, c'est la législation fédérale qui s'applique (LPD) ; l'Etat n'a pas de compétence de surveillance ou d'intervention. Comme indiqué plus haut, l'autorité compétente pour toutes les questions relatives à la protection des données dans ce domaine est le préposé fédéral à la protection des données et à la transparence. De façon générale, le préposé conseille les personnes privées en matière de protection des données (art. 28 LPD).

Dans le cas où un individu suspecte que ses données personnelles aient été traitées d'une manière illicite par une autre personne (suspicion d'atteinte à la personnalité), celui-ci peut porter plainte selon l'article 15 LPD. Dans l'idéal, il cherchera au préalable le dialogue avec le/la responsable du traitement. Selon ce même article, l'individu peut requérir en particulier que le traitement des données, notamment la communication à des tiers, soit interdit ou que les données soient rectifiées ou détruites devant le tribunal. Selon l'article 29 LPD, le préposé fédéral peut aussi établir les faits lui-même d'office, s'il pense qu'une méthode de traitement est susceptible de porter atteinte à la personnalité d'un nombre important de personnes.

En conclusion, lors de cyberattaques à l'encontre de cabinets privés, comme cela fut le cas dans le canton de Neuchâtel en avril 2022, ce sont généralement des failles dans la sécurité qui sont exploitées par les pirates informatiques pour accéder aux données. Des failles au niveau technique (par exemple, logiciels pas mis à jour, pas de blocage des pièces jointes à risque dans les courriels, trop de droits sur les systèmes, filtrage réseau pas assez strict, authentification trop faible, etc.) sont ainsi la plupart du temps mis en cause et non pas le respect des mesures de protection des données. Cet aspect technique relève de la sécurité des données et donc de la responsabilité des fournisseurs et de leurs utilisateurs/trices, selon les bases contractuelles qui les lient. Dans un contexte où les menaces informatiques sont de plus en plus nombreuses et évoluent rapidement, il est du devoir du médecin, en tant que responsable du traitement, de rester à jour sur les normes et recommandations en matière de sécurité informatique pour éviter d'être une cible facile pour les pirates informatiques.

1. Que le Conseil d'Etat entend-il faire pour renforcer la sécurité des données des patient-e-s fribourgeois-es ?

Comme indiqué en introduction, le Conseil d'Etat rappelle, que pour le secteur privé, l'Etat n'a pas la compétence ni la responsabilité de contrôler ou de surveiller les pratiques en matière de sécurité et de protection des données, qui sont du ressort fédéral.

Néanmoins, à la suite des événements du 1^{er} avril 2022, le Conseil d'Etat précise que la Direction de la santé et des affaires sociales (DSAS) a adressé le jour-même (1^{er} avril 2022) une information à tous les médecins installés en cabinet dans le canton de Fribourg. L'objectif de cet envoi était de leur rappeler que la sécurité de leur système primaire était du ressort des fournisseurs et des utilisateurs/trices. La DSAS a, dans ce sens, invité les médecins à suivre les recommandations de leur fournisseur en ce qui concerne la protection et la sécurité des données.

Pour ce qui concerne le secteur public, comme précisé en introduction, ce sont les entités qui sont responsables du traitement des données et de la mise en œuvre de la LPrD. L'Autorité de surveillance en protection des données agit ici dans la limite de ses compétences, notamment via la surveillance de la protection des données, les conseils aux institutions et la sensibilisation à la population. Dans le cadre des formations continues proposées à l'Etat de Fribourg, la préposée cantonale donne par exemple un cours sur cette thématique à la Haute école de gestion Fribourg (HEG). L'Autorité intervient également lors de formations organisées par l'association

fribourgeoise pour l'organisation des cours interentreprises (AFOCI) destinés aux stagiaires et apprenti-e-s de l'Etat de Fribourg. En outre, à la demande, elle peut sensibiliser et former certaines entités de manière ciblée.

Par ailleurs, pour ce qui concerne spécifiquement les hôpitaux mandatés par le canton, la Conférence suisse des directeurs de la santé (CDS) vient d'inclure une recommandation supplémentaire en lien avec la sécurité informatique (cf. réponse à la question 2) dans ses recommandations sur la planification hospitalière.

Finalement, il convient de rappeler que différentes actions sont également entreprises au niveau fédéral. Le Conseil fédéral a ainsi communiqué en mai 2022 que le Centre national pour la cybersécurité (NCSC) deviendrait un office fédéral à part entière. Ce Centre sera doté de ressources supplémentaires, ceci principalement pour le domaine de la protection contre les cyberrisques. Le Conseil fédéral a, par ailleurs, mis en consultation en janvier 2022 un avant-projet de modification de la loi sur la sécurité de l'information relatif à l'introduction d'une obligation de signaler les cyberattaques contre les infrastructures critiques. Il est prévu que le NCSC assume ici le rôle de centrale de signalement. Le projet bénéficie jusqu'à présent du soutien de la plupart des cantons, des milieux économiques et scientifiques.

2. Evalue-t-il des exigences supplémentaires liées à la planification hospitalière ou un soutien accru à certains acteurs, comme les cabinets médicaux p. ex. ? Si non, pourquoi le Conseil d'Etat n'estime-t-il pas pertinent d'agir par ces biais-là ? Si oui, qu'entend-il faire concrètement ?

Selon la loi fédérale sur l'assurance-maladie (LAMal, art. 39) et l'ordonnance (OAMal, art. 58a-b), l'Etat doit assurer la couverture des besoins en soins hospitaliers stationnaires de sa population. C'est dans cette optique qu'il évalue périodiquement les besoins sanitaires de la population et établit, sur préavis de la Commission de planification sanitaire, la planification hospitalière cantonale qui liste les hôpitaux autorisés à fournir des prestations à la charge de l'assurance obligatoire des soins (AOS). La liste est formalisée par des mandats de prestations qui sont octroyés aux différents établissements selon plusieurs critères. Le canton se base ici essentiellement sur les recommandations de la CDS.

Le problème de la sécurité des données des patient-e-s et la protection des données personnelles sur la santé est de plus en plus au centre de l'attention, notamment dans le contexte de l'introduction du dossier électronique du patient (DEP). C'est dans cette optique que la CDS a inclus une nouvelle recommandation sur la protection des données personnelles sur la santé dans ses Recommandations sur la planification hospitalière¹.

Le canton de Fribourg suit attentivement les recommandations de la CDS en matière de planification hospitalière et veillera à appliquer ces révisions dans le cadre des mandats de prestations qui seront élaborés lors de la prochaine planification.

Pour ce qui concerne le domaine des soins médicaux en ambulatoire, la loi cantonale sur la santé (LSan) précise que le traitement des données sur la santé est régi par la législation sur la protection des données, qui relève, pour ce domaine, du niveau fédéral. L'Etat veille cependant à assurer, dans

¹[Recommandations révisées de la CDS sur la planification hospitalière du 20 mai 2022](#), voir recommandation no 16

les limites de ses compétences, la communication et la sensibilisation autour de la sécurité pour ce secteur.

3. *L'HFR dispose-t-il des moyens nécessaires pour assurer une sécurité suffisante des données traitées ?*

Comme mentionné en introduction, tout traitement de données personnelles effectué par un organe public est de la responsabilité du/de la responsable du traitement (à savoir la cheffe/le chef de l'entité).

Les moyens nécessaires à l'assurance de la sécurité des données pour l'hôpital fribourgeois (HFR) tout comme pour le Réseau fribourgeois de santé mentale (RFSM) étaient réglés, jusqu'en 2022, au niveau cantonal, par l'ordonnance sur la gestion de l'informatique et des télécommunications dans l'administration cantonale.

Cette ordonnance a été remplacée, en juillet 2021, par l'ordonnance sur la gouvernance de la digitalisation et des systèmes d'information de l'Etat (art. 2 al. 2) qui précise désormais que diverses institutions publiques fribourgeoises, dont l'HFR et le RFSM, bénéficient d'une autonomie organisationnelle. Cette autonomie les habilite à déterminer leur stratégie informatique et à gérer leurs systèmes informatiques de façon indépendante. Selon cette même ordonnance, les unités autonomes ou des tiers peuvent conclure des conventions avec le Service de l'informatique et des télécommunications (SITel) en vue de bénéficier des prestations de celui-ci. Les dispositions transitoires prévoient un délai de deux ans pour que les prestations informatiques actuellement fournies aux unités autonomes soient formalisées dans de nouvelles conventions. Ainsi, la résiliation de la Convention cadre liant l'HFR au SITel est intervenue en date du 31 décembre 2020 avec effet au 31 décembre 2022. Une reconduction de cette convention afin de permettre la migration dans les meilleures conditions est en cours de discussion. Néanmoins, à l'issue de cette période de prolongation, l'HFR assumera seul ses obligations en matière de sécurité des données et de protection des données, sauf Convention contraire passée entre le SITel et l'HFR en matière informatique.

En l'état actuel et au moins jusqu'à l'échéance du délai de mise en application de l'ordonnance sur la gouvernance de la digitalisation et des systèmes d'information de l'Etat (1^{er} juillet 2023), les infrastructures informatiques de l'HFR et du RFSM (le réseau, les serveurs et les backups) sont gérées par le SITel, qui est responsable de la sécurité de ces moyens informatiques. Comme évoqué en introduction, dans le cas d'une cyberattaque, ce sont ces moyens qui sont la plupart du temps susceptibles d'être ciblés.

Pour ce qui concerne la protection des données, c'est à l'HFR et au RFSM qu'il incombe de garantir un accès et une utilisation sécurisés des divers systèmes informatiques. Les données médicales des patients et des patientes ne sont accessibles qu'aux collaborateurs et collaboratrices autorisés, en fonction de leur profil (gestion et contrôle des droits d'accès). Ces accès sont nominatifs, répondent aux normes de sécurité actuelles édictées par le SITel, et sont entièrement tracés. Les accès par des partenaires externes (fournisseurs informatiques) sont strictement réglementés et ne sont possibles que via des comptes et plateformes fournis par le SITel.

Il convient ici finalement de rappeler que le NCSC encourage, par le biais de la plate-forme d'échange de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), l'échange d'informations et de connaissances dans le secteur de la santé. Le NCSC fournit par ailleurs des outils d'évaluation de la sécurité pour les hôpitaux (cf. réponse à la question 5).

4. La Police cantonale dispose-t-elle des ressources nécessaires pour mener les enquêtes ?

La Police cantonale fribourgeoise dispose d'inspecteurs/trices spécialisés dédiés aux enquêtes cyber, ainsi que de spécialistes en investigation numérique.

Les ressources aujourd'hui consacrées aux enquêtes cyber permettent d'apporter une réponse appropriée à ces nouveaux phénomènes criminels, mais il est vrai qu'un important potentiel de progression subsiste, s'agissant de l'exploitation et de l'identification des traces numériques au profit des enquêtes.

En 2021, dans le cadre de la demande d'augmentation du nombre de collaborateurs/trices de la Police cantonale, ce défi avait été identifié et une réponse appropriée a pu être proposée par le décret fixant l'effectif des agents et agentes de la Police cantonale, accepté par le Grand Conseil le 5 novembre 2021. La Police cantonale pourra ainsi, cette année encore, mettre en œuvre son dispositif et créer un commissariat spécialement dédié à la lutte contre la cybercriminalité avec une augmentation substantielle du nombre de spécialistes disposant de connaissances et compétences spécifiques en matière digitale.

Le canton disposera ainsi d'une structure renforcée en matière d'infractions cyber, de sauvegarde et d'exploitation de traces numériques ainsi que de formation, non seulement auprès des collaborateurs/trices de la Police cantonale mais aussi auprès de ses partenaires.

Bien recruter et fidéliser ces spécialistes constituent un enjeu majeur pour la police, car leurs compétences sont aujourd'hui recherchées bien au-delà du canton.

Le calendrier du renforcement de ce nouveau commissariat cyber dépend toutefois de contingences logistiques, telles que la recherche et l'équipement de places de travail physiques. La capacité des places de travail au BAPOL (bâtiment de la police de sûreté, à la Place Notre-Dame à Fribourg) a atteint aujourd'hui ses limites. La réalisation du nouveau bâtiment de police judiciaire à Granges-Paccot ne sera pas effective avant plusieurs années. Cette servitude logistique représente un obstacle au développement de la Police de sûreté et plus particulièrement, du futur commissariat cybercriminalité. La délocalisation d'une brigade de la Police de sûreté dans un autre bâtiment de l'Etat de Fribourg permettrait de résoudre cette contrainte.

5. Que le Conseil d'Etat recommande-t-il de faire aux personnes – patient-e-s et organisations de santé – qui ont été victimes d'une attaque ?

La meilleure recommandation reste la prévention et la protection des entreprises. Pour diminuer les risques liés à des logiciels malveillants, il est notamment conseillé de :

- > Sauvegarder régulièrement les données sur un support externe et le déconnecter au terme de la sauvegarde ;
- > Maintenir à jour le système d'exploitation, les logiciels et les antivirus. Lorsque cela est possible, privilégier les mises à jour automatiques ;

- > Protéger toutes les ressources accessibles depuis internet (par ex. serveur de terminal, RAS, accès VPN, etc.) avec un deuxième facteur d'authentification ;
- > Bloquer la réception des courriels qui contiennent des fichiers dangereux sur les messageries, en outre les fichiers Office qui contiennent des macros ;
- > Utiliser des mots de passe forts (minimum 10 caractères, dont des chiffres, des majuscules, des minuscules et des caractères spéciaux) ;
- > Vérifier régulièrement que le dispositif n'a pas été infecté en procédant à un scan complet du système ;
- > Former et exercer régulièrement le personnel.

Pour les victimes d'une attaque, il est recommandé de :

- > Si une attaque est en cours, déconnecter les machines infectées du réseau de l'entreprise et d'internet. Contacter tout de suite le service informatique ou le prestataire pour qu'il prenne les mesures adéquates ;
- > Si le système est déjà bloqué, ne pas payer l'éventuelle rançon exigée, ne rien toucher et contacter immédiatement la Police. Si cela est possible, restaurer les données encryptées à partir des sauvegardes effectuées avec l'aide du service informatique et/ou de prestataires spécialisés ;
- > Déposer une plainte pénale ;
- > Chercher à identifier la faille qui a permis le piratage et prendre les mesures pour que cela ne puisse pas se reproduire.

A côté de ces recommandations, différentes actions se font au niveau national afin d'informer et de soutenir les différents acteurs et actrices du domaine sanitaire dans la sécurité et la protection des données.

Le réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK) a par exemple publié, en collaboration avec le NCSC et Swiss Cyber Experts, une check-list contenant des recommandations destinées aux responsables de la sécurité des systèmes d'information d'une organisation². Par ailleurs, une initiative soutenue par la Confédération suisse et la NCSC a permis la création d'un test en ligne simple et rapide qui, bien qu'il ne remplace pas un audit de sécurité, permet à toute entreprise d'identifier les faiblesses et les points d'amélioration (<https://cybero.ch/cyber-security-check/>).

D'autres organisations nationales offrent également un support en matière de sécurité informatique pour les différents acteurs et actrices du domaine sanitaire. Ainsi, dans le domaine hospitalier, un catalogue d'exigences minimales à respecter pour l'acquisition et l'exploitation de systèmes tiers, comme des dispositifs médicaux, a été élaboré par des spécialistes de la sécurité informatique des hôpitaux en collaboration avec H+³. De façon similaire, la FMH soutient ses membres dans la transformation numérique et a également publié un set d'exigences minimales pour la sécurité informatique des cabinets médicaux⁴. Finalement, Curaviva a publié différents documents permettant notamment aux institutions de dresser un état des lieux par rapport à la sécurité et à la

² [Cyberattaque – que faire? Aide-mémoire à l'intention des CISO \(admin.ch\)](#)

³ [Cyber Security \(hplus.ch\)](#)

⁴ [Sécurité informatique | FMH](#)

protection des données mais également de consolider ou améliorer leurs dispositifs dans ces domaines⁵.

En dernier lieu, il est pertinent de relever que, pour ce qui concerne spécifiquement les cabinets médicaux, différentes pistes de réflexion concernant la sécurité des données ont été discutées suite à la cyberattaque du 1^{er} avril 2022, dans le cadre d'une Conférence sur la cybersécurité en cabinet organisée le 11 mai par la société médicale de la Suisse romande (SMSR). Parmi ces pistes figuraient notamment l'amélioration de l'information et de la communication entre cabinets et fournisseurs de prestations informatiques, une éventuelle révision des bonnes pratiques en matière de sécurité informatique, ainsi qu'un renforcement de la formation pré/post-graduée dans ce domaine.

20 septembre 2022

⁵ [CURAVIVA - Home](#)