Focus sur l'application du RGPD et la gestion de la pandémie

Dans le cadre du Printemps de la Recherche Clinique, la conférence du 25 mars dernier a mis à l'honneur le RGPD et son application par les entreprises et les autorités face à la pandémie, au travers des interventions d'Erik Boucher de Crevecoeur, référent santé pour la CNIL, et de la société MYDATA-TRUST, qui animait la session. Plusieurs sujets ont été traités concernant la conduite des études cliniques pendant la pandémie, le Brexit et le transfert de données.

La conférence était animée par Xavier Gobert, CEO MYDATA-TRUST, société spécialisée dans le RGPD et la recherche clinique, avec les interventions complémentaires d'Aline Jouniaux et Hélène Lecuivre, DP Lawyers MYDATA-TRUST. Avec, en ouverture, la présentation d'Erik Boucher de Crevecoeur, ingénieur expert en technologie de l'information à la CNIL, référent sur les questions de santé, qui est revenu sur l'application du RGPD au cours de l'année écoulée.

RGPD et pandémie

Premier constat : la multiplication des violations de données en 2020, avec une pression croissante notamment sur les établissements de santé

Erik Boucher de Crevecoeur a cité quelques chiffres issus du rapport d'activité de la CNIL, à sortir prochainement. En soulignant en premier lieu une très forte augmentation des notifications de violation de données pour deux raisons : la multiplication des attaques en 2020, mais aussi une question de maturité et de prise de conscience des différents acteurs de la nécessité de rapporter les incidents touchant les Données à caractère personnel (DCP).
En effet, il y a eu une forte augmentation des attaques par rançongiciels qui sont des virus qui chiffrent les données de la victime sur son ordinateur afin de les rendre inaccessibles sauf paiement d'une rançon pour obtenir la clé de déchiffrement. « Céder à ce type de chantage est fortement déconseillé par la CNIL et l'ANSSI, car cela ne fait que renforcer le développement de ce type de business, » rappelle Erik Boucher de Crevecoeur. Le développement du télétravail pendant la pandémie a favorisé ce type d'attaque qui a représenté près de 500 notifications à la CNIL l'an dernier, soit 20% des problèmes concernant les DCP. De plus, on a constaté une augmentation de 83% des notifications dans le secteur de la santé et de l'action sociale (presque le double) liées notamment à la prise de conscience des besoins de notification par les acteurs. Ce qui représente une augmentation des notifications ayant trait à une perte de disponibilité des données de +59%.

Les rançonlogiciels sont vraiment devenus très prégnants sur les établissements de santé, qui conjuguent un fort besoin de disponibilité et des systèmes d'information (SI) complexes. Ce qui pose des problèmes au jour le jour. Il est difficile par exemple d'arrêter un système d'information pour une mise à jour de sécurité ou une maintenance lorsque l'établissement tourne au maximum de ces capacités 24/24h. La gestion des habilitations et des droits d'accès au SI a souvent été faite dans l'urgence, la solution de facilité étant d'élargir les droits afin d'éviter les blocages. La sécurisation des données est donc en baisse faute de gérer les mises

à jour et les droits d'accès au cours de cette crise. Face aux rançons business menées par les mafias, le minimum est d'être protégé en amont et d'avoir des sauvegardes en bonne et due forme et déconnectées du réseau. En 2020, la thématique prioritaire des contrôles de la CNIL était la « sécurité des données de santé », reconduite l'année suivante à la suite de la multiplication des attaques.

Dans sa grille de lecture, le RGPD distingue 3 niveaux de risque à estimer au cas par cas.
En cas d'incident de sécurité qui se caractérise comme violation des données à caractère personnel, le RGPD précise « qui » et « quand » notifier en fonction du niveau de risque.
S'il est jugé que la violation des données n'a pas d'impact sur la personne concernée ou que l'impact est négligeable, il suffira de consigner la violation dans le registre interne tenu par l'organisme. Si l'impact est jugé certain pour les personnes, il faut notifier la CNIL dans les 72h après la prise de connaissance. Enfin, si la violation peut présenter des risques très élevés comme la divulgation de patrologies associées à des personnes, il faut en plus prévenir (notifier) les personnes concernées. « Au-delà de la transparence, l'enjeu est de donner aux personnes une indication de l'ampleur des données qui ont été accédées de manière illégitime et se prémunir des conséquences, » note-t-il. L'association d'une pathologie à une adresse mail peut conduire à une tentative de chantage ou simplement à l'envoi de courriels non désirés. Si les personnes sont prévenues elles peuvent plus facilement réagir en conséquence et être plus vigilantes.

Quel que soit l'incident de sécurité, les DCP concernées ou non, le code de la santé publique indique que l'ARS et l'ANSSI doivent être averties. Si l'incident concerne des DCP, il faut en plus prévenir la CNIL et les personnes concernées. Tout cela doit être notifié par le responsable de traitement de l'organisme dans le registre prévu à cet effet.

Second point : les dossiers « recherche COVID-19 » traités en urgence par la CNIL

La CNIL s'est mise en situation de ne pas pénaliser l'environnement de la recherche et du traitement du COVID-19, mais a néanmoins réalisé son travail. Elle est ainsi restée vigilante sur la conformité des dossiers déposés en urgence, en particulier le respect des droits des personnes, notamment leur droit d'opposition discrétionnaire ou la justification de collation de données pertinentes et en rapport avec le besoin et la finalité (origine ethnique, orientation sexuelle...). Un autre point est la bonne mise en place de mesures de sécurité appropriées dans la gestion des habilitations afin de limiter l'accès aux informations aux personnes ayant le « droit d'en connaître ».

Dans la réalisation d'études cliniques, il a géré la conciliation entre les besoins pressants des chercheurs et la protection de la vie privée des patients concernant les modalités d'information des personnes. Une certaine souplesse a été acceptée pour les personnes hors d'état d'être informées au moment de leur admission dans un établissement de santé : on a ainsi différé l'accord d'inclusion dans une étude, au moment de leur réveil, avec la garantie d'effacement des données en cas d'opposition. Une autre facilité a été la possibilité d'informer seulement un titulaire de l'autorité parentale pour les mineurs, moyennant la transmission d'une note d'information à l'autre représentant légal (qui ne pouvait pas être là au moment de l'inclusion).

Dans ce contexte particulier, il y a des précautions à prendre dans le cadre du monitoring à distance qui s'est développé

On s'intéresse à l'accès à distance aux données (des contrôles qualité par exemple) à partir du domicile d'un ARC (Assistant de Recherche Clinique). Les agences sanitaires européennes et l'EMA ont adopté des lignes directrices sur la gestion des essais cliniques notamment la réalisation du « monitoring à distance ». Le rappel a été fait de privilégier le monitoring « sans consultation des données sources » dès que cela est possible.

Que dire sur l'aspect juridique de l'information des patients ? Des pistes ont été évoquées et semblent dégager un consensus : une étude existante passant en monitoring à distance serait considérée comme une modification substantielle devant faire l'objet d'un avis du CPP (Comité de Protection des Personnes). Le « monitoring à distance » n'est pas décrit dans le périmètre des Méthodologies de référence telles que rédigées aujourd'hui. La CNIL l'envisage à titre dérogatoire, dans ce contexte, s'il est le seul écart et assorti de mesures. « On n'a pas besoin d'autorisations spécifiques et on reste dans l'épaisseur du trait de la méthodologie de référence, note-t-il. Mais cela pose des questions juridiques et techniques. Outre les questions du CPP, une information préalable sur le monitoring à distance doit être faite en plus de l'information générale relative à l'étude. Pour les études en cours, il faut également mettre à jour la note d'information et la remettre aux personnes concernées. »

Un autre point est la possibilité de consultation à distance des données sources d'un patient sous réserve de conditions strictes. En particulier, une note d'information aux personnes doit faire apparaître clairement cette notion de monitoring. L'objectif étant de clairement documenter l'aspect juridique de la non-opposition du patient dans son dossier médical par des moyens parfois plus souples comme l'appel téléphonique ou le mail.

D'un point de vue technique, le DPO (Data Protection Officer) décrit dans le RGPD doit être consulté et apporter des recommandations. Il faut documenter le registre avec les garanties supplémentaires mises en place. Il est important que cela soit tracé au moment de la mise en place de ces conditions particulières. Par ailleurs, l'AIPD (l'Analyse d'Impact relative à la Protection des Données) de l'étude doit être mise à jour.

Du coté de l'ARC, qui accède aux données à distance, il y a la nécessité d'avoir des mesures de confidentialité renforcées et une formation spécifique de contrôle qualité. L'ARC doit s'engager sur un accord de confidentialité complémentaire, ne pas effectuer d'impression d'écran ou de photo, consulter dans un endroit clos sans passage de tiers et utiliser uniquement du matériel informatique maîtrisé fourni et sécurisé par le promoteur. Au-delà de la sécurisation de l'environnement de travail déporté de l'ARC, les mesures de sécurité générales pour les systèmes de santé restent pertinentes. Des règles de sécurité renforcées doivent ainsi être cadrées avec l'ARC.

Au-delà de la sécurité basique sur l'environnement de travail, il y a des questions techniques d'accès aux données. L'hébergement, le traitement et l'administration doivent se faire par des outils du périmètre juridique de l'Union européenne. L'utilisation d'hébergeurs reconnus HDS (Hébergeur de Données de Santé) est fortement recommandée. Les échanges doivent être chiffrés (EAS 256, TLS) selon l'état de l'art. Les ARC doivent utiliser des comptes nominatifs

avec des profils spécifiques limités en lecture seule et donnant uniquement accès aux données nécessaires.

En outre, la vidéoconférence est une solution technique en voie d'être adoptée pour ce qui correspond le mieux à une visite physique de l'ARC au centre d'investigation. Celle-ci est possible en respectant des mesures adaptées : utilisation d'une solution de vidéoconférence certifiée (par l'ANSSI par exemple), pas de prise en main à distance, installation dans l'UE, supervision permanente des connexions du coté du centre d'investigation, comptes nominatifs, mots de passes conformes et traçabilité des données pendant 6 mois.

Un fort développement des entrepôts de données santé (EDS) avec l'utilisation des circuits d'appariements dans de nombreuses études au cours de la pandémie

Parmi l'ensemble des données, certaines pourront alimenter des bases de données pour servir à d'autres études dans le cadre de l'utilisation de données massives (big data). « Pour la CNIL, les entrepôts de données de santé (EDS) sont des bases de données de santé massives constituées et utilisées dans l'intérêt public, principalement à des fins de recherches ultérieures, précise Erik Boucher de Crevecoeur. L'un des premiers entrepôts de données de santé hospitaliers a été celui de l'AP-HP et, plus récemment, le CHU de Rennes a fait l'objet d'une délibération à la CNIL. » La CNIL a récemment matérialisé sa doctrine sous la forme d'un projet de référentiel EDS, avec l'ambition de pouvoir se dispenser de demande spécifique à condition de se déclarer conforme au référentiel. Ce référentiel est actuellement soumis à consultation publique auprès des différents acteurs.

Chaque EDS doit avoir sa propre gouvernance sous la forme d'un comité scientifique et éthique chargé d'évaluer les projets de recherche et de donner les autorisations d'accès aux données de l'entrepôt. Un EDS doit intégrer la protection de la vie privée dès la conception de l'entrepôt (*privacy by design*) avec un accès restreint, une pseudonymisation du cœur de l'entrepôt avec une table de correspondance si nécessaire, une limitation des extractions ainsi qu'une traçabilité et une surveillance natives.

En outre, les circuits d'appariements déterministes avec le Système National des Données de Santé (SNDS) se font au travers de l'identifiant pivot NIR (Numéro d'Inscription au Répertoire – numéro de sécurité sociale) qui fait le lien avec les données d'étude. La CNIL a identifié de nombreux écueils de sécurité (exemple de l'emploi d'un tiers de confiance inutile…) ce qui a conduit à la réalisation d'un guide pratique de circuit conforme auquel il faut se référer (TIR indépendant et proposition de circuits types).

Comment 2020 a-t-il impacté le RGPD ?

Lancé en mai 2018, le RGPD avait un an et demi de pratique en 2020, année qui devait être celle de « la maturité » selon Xavier Gobert. Certaines étapes avaient déjà été fixées :
- Le Royaume-Uni devait quitter l'UE en 2019, avec 2020 comme année de transition où les deux parties devaient s'entendre sur différents points, notamment les transferts de données et la façon dont le Royaume-Uni allait considérer les données européennes.
- En juillet, était attendue une décision de la Cour de justice de l'Union européenne (CJUE)

concernant la plainte de Maximilian SCHREMS sur le partage des données et le « Privacy Shield ».

Les autorités de contrôle avaient déjà publié leur agenda pour 2020 et, pour la CNIL, le focus était mis sur la sécurité des données de santé, les nouveaux usages des données de géolocalisation et le respect des dispositions applicables aux « cookies ». Certains de ces aspects sont restés d'actualité, d'autres ont été chamboulés. « Les autorités ont compris qu'il fallait user de flexibilité et adopter une interprétation plus large du RGPD, note-t-il. La question est de savoir maintenant ce qui va perdurer au-delà de la crise. »

Les nouvelles conditions pour le transfert des données

Que s'est-il passé au dernier semestre de l'année 2020 ? « En juillet 2020, l'arrêt Maximilian SCHREMS par la CJUE a provoqué la création de deux lignes directrices (guidances) par deux institutions européennes » note Hélène Lecuivre, DP Lawyers MYDATA-TRUST. L'EDPB (European Data Protection Board) peut être vu comme l'autorité européenne des autorités nationales de protection des données en Europe. Ce Board donne des guidances générales en matière d'interprétation du RGPD. En novembre 2020, il a mis en place une ligne additionnelle à la ligne directrice en matière de transfert, puis l'a soumise à consultation publique à laquelle MYDATA-TRUST a participé. Parallèlement à cela, la commission européenne a publié de nouvelles clauses contractuelles types en matière de transfert de données.

Qu'est-ce qu'un transfert de données ? Selon le RGPD, dès lors que l'on se trouve en Europe, on doit mettre en place des mécanismes de transfert de données pour envoyer des données hors de l'UE. « Il y a donc un champ d'action géographique » pointe-t-elle. Pour être plus précis, il s'agit de l'espace économique européen (27 pays de l'union + Islande + Norvège + Liechtenstein). La notion de sortie des données est importante : « le Board a confirmé qu'une donnée sort si elle est rendue accessible à une entité extérieure, continue-t-elle. Par exemple, si l'on a une base de données en Europe et qu'on la rend accessible en dehors de l'Europe, c'est un transfert de données. Si nos données sont hébergées en dehors de l'Europe, on fait aussi un transfert de données. »

Le Board donne une Roadmap en 6 étapes pour analyser les transferts de données :
Etape 1 : comprendre où sont les transferts, voir ci-dessus.
Etape 2 : mettre en place un outil de transfert de données adapté avec une approche en 3 étapes pour permettre le transfert :

- la décision d'adéquation : si le pays est jugé fiable par l'autorité européenne, c'est bon. Dans le cas contraire, des garanties appropriées doivent être mises en place, c'est à dire des engagements contractuels avec les partenaires, qui sont difficiles adopter en dehors des clauses contractuelles types de la commission européenne,
- sinon, en troisième cas, viennent les dérogations comme régime d'exception qui, dans le secteur médical, peuvent être le consentement du patient, l'intérêt public … User d'une dérogation n'est pas autorisé par le Board en cas de transferts répétitifs et réguliers (ce qui est souvent le cas d'un accès à une base de données médicales). Dans le cas de la COVID, l'EDPB s'est prononcé en acceptant la dérogation d'intérêt public pour les transferts nécessaires pendant la pandémie notamment pour le développement des vaccins. « A ce stade, on s'attend à la publication de nouvelles clauses contractuelles types de l'UE dans les

prochains jours, » note-t-elle.

Etape 3 : Analyse de la loi du pays tiers
Selon l'arrêt SCHREMS par la CJUE, l'outil de transfert n'est pas forcément suffisant. SCHREMS a porté plainte contre la décision d'adéquation octroyée aux Etats-Unis car dans ce pays, la NSA ou d'autres autorités publiques avaient un droit d'ingérence (ce qui n'a rien à voir avec l'outil de transfert).

Etape 4 : Mise en place de mesures additionnelles
Il s'agit d'analyser les lois des pays tiers (voir droit d'ingérence aux Etats-Unis ci-dessus) et, en fonction, de mettre en place des mesures additionnelles qui peuvent d'être d'ordre technique (chiffrement, pseudonymisation), contractuel ou organisationnel, afin d'être en adéquation avec les conceptions démocratiques européennes.

Etape 5 : Le transfert

Etape 6 : Réévaluation – amélioration continue

« Le transfert des données est un élément important à maîtriser pour être en conformité avec le RGPD, conclut Hélène Lecuivre. La bonne maîtrise des transferts de données donne un avantage concurrentiel. C'est donc un choix stratégique de sélectionner des partenaires qui comprennent et maîtrisent les transferts de données. » « Le conseil que l'on donne à nos clients est de documenter le plus possible, ajoute Xavier Gobert. En cas d'inspection, un cas documenté et expliqué ne débouchera pas sur une amende. »

Le BREXIT et son impact sur la protection des données

« En juin 2016 est voté le BREXIT, rappelle Aline Jouniaux. En mai 2018 entre en vigueur le RGPD, transposé dans la loi nationale britannique en Data Protection Act. » Le 31 janvier 2020 marque la sortie officielle du Royaume-Uni de l'UE et le début de la période transitoire d'une année supplémentaire qui a lui permis de continuer à suivre le droit de l'UE, à accéder au marché intérieur et à la libre circulation des biens, des services et des personnes, comme s'il était encore membre. Le 1er janvier 2021, le Royaume-Uni n'est plus un membre de l'UE, ce qui a pour conséquence la mise en place d'un RGPD UE et d'un RGPD UK. A cette date, l'accord de commerce et de coopération est mis en œuvre. « Si le RGPD de l'Union européenne et le RGPD du Royaume-Uni sont deux RGPD qui s'appliquent séparément, ils se révèlent dans la pratique être des copier/coller pour les entreprises » pointe-t-elle.

A partir de la mise en place de l'accord de commerce et de coopération au 1er janvier 2021, Aline Jouniaux distingue plusieurs cas de figures :
- En cas de transfert de l'UE vers le Royaume-Uni, ce qui prime pour l'instant est la libre circulation des données car l'accord octroie un délai supplémentaire de six mois mois, jusqu'au 1er juillet 2021, pendant lequel le Royaume-Uni ne sera pas considéré comme un pays tiers en cas de transfert de DCP. Après ces six mois, il y a deux possibilités : soit la commission européenne a publié une décision d'adéquation avant le terme et le Royaume-Uni bénéfice encore de la libre circulation des données ; soit le Royaume-Uni devra, en tant que pays tiers, avoir recours aux outils standards de transfert comme le suivi des garanties appropriées, les

garanties contractuelles types, etc.
- En cas de transfert du Royaume-Uni vers l'UE, c'est plus simple puisque le Royaume-Uni a reconnu les pays membres de l'UE comme adéquats, donc il y a une libre circulation des données en vertu de l'article 45 du RGPD.

Quelle est la situation à l'heure actuelle ? « A la mi-février, un draft de la décision d'adéquation a été mis en place par la commission européenne, annonce-t-elle. On est dans l'attente de l'avis du comité européen de protection des données (EDPB) et d'une approbation des représentants de chaque pays membre de l'UE avant l'expiration du délai de 6 mois (1er juillet 2021) ».

« Ce que l'on peut dire en conclusion, c'est que le RGPD a résisté à la crise sanitaire. En reconnaissant son caractère sans précédent, de nombreuses autorités de protection des données ont fait preuve de souplesse » note Xavier Gobert qui poursuit sur plusieurs conseils à l'attention des entreprises :

- N'oubliez pas que les informations sur la santé constituent une catégorie spéciale d'informations en vertu des lois sur la protection des données.
- Ne recueillez pas plus d'informations juste parce que vous le pouvez.
- Le recueil doit être dûment justifié.
- Soyez innovants sans oublier les conditions de transfert.
- Les technologies innovantes ne vont pas disparaître.