NEWSLETTER E-SANTE

NUMÉRO 3 • NOVEMBRE 2022

ÉQUIPE

Alexandre FIEVEE
Avocat associé

Alice ROBERT
Avocat senior

SOMMAIRE

DISPOSITIFS MEDICAUX ET CYBERSECURITE : DES RECOMMANDATIONS DE L'ANSM

Le 23 septembre 2022, l'ANSM a publié des recommandations sur la « cybersécurité des dispositifs médicaux intégrant du logiciel au cours de leur cycle de vie ».

Ces recommandations, rédigées par un comité scientifique spécialisé temporaire, avaient fait l'objet d'une consultation publique qui s'est achevée le 30 septembre 2019.

Elles interviennent face au constat d'une « *cybersécurité très hétérogène au sein des fabricants de DM* [dispositifs médicaux] » alors que les dispositifs médicaux doivent « *s'adapter aux nouvelles menaces engendrées par les progrès technologiques* ».

Ces recommandations constituent des « *bonnes pratiques* » qui n'ont pas de valeur normative.
Elles concernent essentiellement les fabricants de logiciels dispositifs médicaux ou de dispositifs médicaux connectés « *afin qu'ils prennent les mesures nécessaires pour réduire au maximum les risques d'attaque à l'encontre de leurs DM et ainsi prévenir la compromission des données et l'utilisation détournée des DM qu'ils mettent sur le maché* ».

Les fabricants sont invités à prendre de telles mesures aussi bien au stade de la conception, du développement, de la mise en service/1ère utilisation, qu'à celui de la surveillance « *post-marché* » et de la fin de vie du DM concerné.

Certaines recommandations concernent également d'autres parties prenantes comme les utilisateurs, les patients, les établissements de santé en cas de « *responsabilité conjointe* ».

L'accent est mis sur « *la disponibilité* » et « *l'intégrité* » des dispositifs médicaux intégrant du logiciel en s'appuyant sur « *les méthodologies d'analyses de risques développées dans le monde du DM et celui de la SSI* » avec l'objectif « *d'atteindre un niveau de risque minimum acceptable* ».

La confidentialité et la protection des données sont également évoquées en faisant référence au Référentiel Général de Sécurité (RGS) et naturellement au RGPD. Les recommandations détaillent, en particulier, « *la protection des données en lecture contre une divulgation non autorisée et de protection des accès à des éléments techniques* ».

A noter qu'il s'agit davantage de grands principes et non de mesures techniques détaillées pour tenir compte « *de l'évolution rapide des dispositifs médicaux et des attaques* ».

Source : ici

ENTREPOTS DE DONNEES DANS LE DOMAINE DE LA SANTE, LA CHECK-LIST DE LA CNIL

Il y a un an, la CNIL publiait un référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données dans le domaine de la santé. Le 28 septembre dernier, l'autorité française de protection des données a publié une « check-list » visant à aider les responsables du traitement à vérifier facilement leur conformité audit référentiel.

1. De quels entrepôts parle-t-on ?

Pour mémoire, ce référentiel ne s'applique pas à tous les entrepôts de données de santé, mais seulement à ceux qui reposent sur l'exercice d'une « *mission d'intérêt public* », au sens de l'article 6.1.e du RGPD.

Ainsi, un établissement privé de soins, qui met en œuvre un entrepôt s'inscrivant dans le cadre de l'exécution d'une mission d'intérêt public, peut être couvert par ce référentiel. Et s'il respecte l'intégralité des critères visés dans ce document, il pourra se contenter d'adresser à la CNIL un simple engagement de conformité.

En revanche, si tous les critères ne sont pas respectés, l'entrepôt devra faire l'objet d'une autorisation.

« *Dans cette hypothèse*, précise la CNIL, *il est conseillé à l'organisme qui sollicite une autorisation d'inclure dans son dossier un document au sein duquel il met en avant et justifie les écarts par rapport au référentiel.* »[1]

Tel sera notamment le cas d'un entrepôt constitué à des fins de recherche sans exécution d'une mission d'intérêt public, à moins que cet entrepôt, conformément aux termes de l'article 65 de la loi « Informatique et Libertés », repose sur le consentement des personnes concernées ou s'il a pour objectif la dématérialisation des dossiers médicaux. En tout état de cause, la CNIL recommande vivement à tout organisme de faire en sorte que l'entrepôt ainsi constitué réponde aux critères visés dans le référentiel.

Si les entrepôts concernés par le référentiel sont ceux qui reposent sur l'exercice d'une « *mission d'intérêt public* », il doivent par ailleurs répondre à l'une des finalités suivantes : (i) la production d'indicateurs et le pilotage stratégique de l'activité, sous la responsabilité du médecin responsable de l'information médicale (département de l'information médicale – DIM) (p. ex : analyses médico-économiques de parcours de soins, évaluation de la qualité et de la pertinence des prises en charge) ; (ii) l'amélioration de la qualité de l'information médicale ou l'optimisation du codage dans le cadre du programme de médicalisation des systèmes d'information (PMSI) ; (iii) le fonctionnement d'outils d'aide au diagnostic médical ou à la prise en charge ; (iv) la réalisation d'études de faisabilité (pré-screening).

A noter que les traitements de données de santé à caractère personnel mis en œuvre à des fins de recherche, d'études ou d'évaluation dans le domaine de la santé, à partir des données contenues dans l'entrepôt, constituent des traitements distincts qui doivent faire l'objet des formalités nécessaires au titre des articles 66, 72 et suivants de la loi « Informatique et Libertés »[2].

2. A quoi sert la « check-list » ?

La « check-list » a pour objectif d'aider chaque organisme, responsable du traitement, à vérifier facilement la conformité de son projet d'entrepôt. Pour ce faire, elle reprend les différentes exigences du référentiel sous forme d'affirmations auxquelles le responsable de traitement répond par « vrai » / « faux », ou, le cas échéant « non applicable ». Toute réponse négative (« faux ») à l'une des questions signifie que le traitement envisagé n'est pas conforme au référentiel et qu'il devra faire l'objet, s'il est maintenu en l'état, d'une autorisation de la CNIL, et ce préalablement à sa mise en œuvre.

A vous de jouer…

Source : ici

[1] https://www.cnil.fr/fr/la-cnil-adopte-un-referentiel-sur-les-entrepots-de-donnees-de-sante

[2] Les données peuvent également être réutilisées à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé. Ces traitements devront faire l'objet des formalités adéquates : s'ils sont conformes à une méthodologie de référence, ils peuvent être mis en œuvre à la condition que leur responsable adresse préalablement à la Commission une déclaration attestant de cette conformité. A défaut, ils devront solliciter une « autorisation recherche » sur le fondement de l'article 66.III de la loi « Informatique et Libertés ».

CERTIFICATION HDS : VERS UN NOUVEAU REFERENTIEL

Le 2 novembre dernier, l'Agence numérique en santé a publié un nouveau projet de référentiel de certification HDS. Certaines nouvelles exigences proposées ne seront pas sans incidence sur l'activité d'hébergement de données de santé.

Pour mémoire, l'hébergement de données de santé est encadré par le Code de la santé publique. Il ressort notamment de l'article L.1111-8 dudit code que toute personne physique ou morale à l'origine de la production ou du recueil de données de santé à caractère personnel à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social doit recourir à un hébergeur certifié ou agréé lorsqu'elle externalise la conservation de données dont elle est responsable.

La procédure de certification repose sur une évaluation de conformité à un référentiel de certification dont la dernière version a été approuvée par arrêté du 11 juin 2018. Ce référentiel définit les exigences applicables à la certification « HDS » incluant le respect d'un certain nombre de règles et de normes, dont des normes ISO. Concrètement l'hébergeur choisit un organisme certificateur qui devra être accrédité par le COFRAC (ou équivalent au niveau européen), lequel procédera à un audit de conformité au référentiel. Le certificat est délivré pour une durée de 3 ans, étant précisé qu'un audit de surveillance annuel est effectué.

Ce référentiel vient d'être révisé par l'Agence numérique en santé sous l'égide de la Délégation ministérielle du numérique en santé. Un nouveau projet a ainsi été publié le 2 novembre dernier. Il est soumis à consultation publique jusqu'au 9 décembre prochain.

Le 1er point concerne l'activité dite « d'administration et d'exploitation d'applications du système d'information contenant des données de santé », une des 5 activités d'hébergement concernées par la certification qui n'est pas sans poser de difficultés d'appréciation. Le projet de référentiel en propose une définition délicate à appréhender qui exclut notamment certains pans de l'activité de la nécessité d'une certification HDS :

« [Cette activité] comporte :

- *L'encadrement et la gestion des accès occasionnels des tiers mandatés par le client de l'organisation, par exemple à des fins d'audit, d'expertise, de déploiement ou de maintenance, amenés à accéder via le Socle d'Infrastructure HDS à l'Application métier. Les accès des Utilisateurs finaux et du responsable de traitement ne sont pas concernés. Ces tiers mandatés ne sont pas tenus d'être certifiés HDS.*
- *Le maintien en condition de sécurité du Socle d'Infrastructure HDS et le centre de support au client. Ces services doivent être adaptés à la criticité des données de santé et aux obligations qui incombent au Responsable de traitement.*

- *La documentation tenue à jour de la cohérence et de la complétude des garanties de sécurité apportées par les différents acteurs contribuant à la mise en œuvre du service, telle que décrite au chapitre 7 du référentiel de certification. ».*

Avec la définition proposée, des éditeurs de solution SAAS traitant des données de santé à caractère personnel, notamment, n'auraient plus besoin d'être certifiés HDS.

Le second point concerne les clauses qui doivent figurer dans le contrat d'hébergement. D'une part, le projet de référentiel reprend les exigences imposées par le Code de la santé publique qui n'étaient pas exactement reprises dans le référentiel en vigueur. Le respect de ces exigences constituera alors un point de contrôle de l'organisme certificateur. D'autre part et surtout, les lieux d'hébergement proposés au client par l'hébergeur doivent être localisés dans des pays membres de l'Espace Economique Européen, ou des pays assurant un niveau de protection adéquat en vertu d'une décision d'adéquation, à l'exclusion des autres garanties (clauses contractuelles types ou BCR).

A noter que s'il reste possible de faire intervenir un opérateur soumis au Cloud Act, dans la mesure où le projet de référentiel exige seulement que l'hébergeur procède à une analyse de risques de divulgation ou d'indisponibilité des données du fait d'une réglementation extraterritoriale, ce point va certainement évoluer au regard des travaux, notamment européens, sur la protection des données vis-à-vis de telles lois.

En termes de calendrier, ce nouveau référentiel pourrait être adopté au printemps 2023 avec des premières certifications en octobre 2023. Selon l'Agence numérique en santé, un guide de transition clarifiant les délais de mise en conformité sera élaboré, en partenariat avec le COFRAC, d'ici quelques mois.

A suivre…

Source: ici

L'IA AU SERVICE DE LA SANTE : UNE DES STRATEGIES PROPOSEES PAR LE CONSEIL D'ETAT

Le 30 août 2022, le Conseil d'état a publié une étude plaidant pour la conduite d'une stratégie de l'IA au service de la performance publique et de l'intérêt général, y compris en santé.

Cette étude de 360 pages, intitulée « *Intelligence artificielle et action publique : construire la confiance, servir la performance* », a été réalisée à la demande du Premier ministre.

Selon le Conseil d'Etat, cette étude doit se concevoir comme une « *contribution à une stratégie de l'IA publique qui reste largement à structurer et à formaliser par les pouvoirs publics* ».

De façon générale, le Conseil d'Etat a dressé le constat suivant :

- Aucun domaine de l'action publique n'est pas « *imperméable* » au système d'IA (« SIA ») : tel est notamment le cas de la santé avec l'aide à la prescription médicale, les alertes sanitaires, la robotique médicale ;

- les SIA sont déployés de façon très progressive, mais avec des inégalités selon les administrations et, généralement, dans le cadre d'une utilisation seulement expérimentale ;

- les objectifs poursuivis et les bénéfices attendus des SIA sont nombreux pour « *améliorer la qualité du service public* ».

Le Conseil d'Etat « *plaide* » ainsi pour la conduite « *d'une stratégie de conception et de déploiement* » « *volontariste* » de l'IA au service de la performance publique et de l'intérêt général. Les bénéfices attendus sont toutefois conditionnés à la création de conditions de confiance, au déploiement avec lucidité et vigilance et à l'allocation de ressources et d'une gouvernance adaptées.

Le recours à des experts en données est, en particulier, à examiner. Le Conseil d'Etat prône également un renforcement d'Etalab (coordonnant la conception et la mise en œuvre de la stratégie de l'Etat dans le domaine de la donnée) et du coordonnateur national pour l'IA pour « *faire de l'État un possible prestataire de services et pourvoyeur de ressources, y compris humaines, pour les collectivités territoriales ».* Le Conseil d'Etat préconise également que la CNIL devienne l'autorité contrôle nationale responsable de la régulation des SIA prévue par le futur règlement européen sur l'IA.

Dans son communiqué, le Conseil d'Etat souligne ainsi la nécessité d'« *anticiper la mise en place d'un cadre réglementaire, notamment au niveau européen, à travers la mise en œuvre, dès aujourd'hui, de lignes directrices pragmatiques (…)* ».

Concernant la santé, le Conseil d'Etat indique que, comme certains autres secteurs, elle « *mériterait à* [elle seule] *la rédaction* [d'une étude] ». Pour autant, la santé est prise pour exemple dans le cadre de nombreuses réflexions et propositions de la Haute juridiction administrative.

Une « *fiche* » est également consacrée à la santé en fin d'étude, le Conseil d'Etat précisant qu'il s'agit du champ d'application de l'IA « *qui suscite le plus d'espoirs et de fantasmes* » ! A cet égard, le Conseil d'Etat met en avant le fait que la santé touche directement à la vie, avec des questions éthiques sous-jacentes, et constitue un secteur économique en forte croissance. Le Conseil d'Etat indique également que l'IA « *constitue un changement ambivalent* », notamment en termes de remplacement pour les professions médicales et paramédicales suscitant des réactions diverses sur le sujet. Le Conseil d'Etat souligne encore la nécessité de réfléchir à l'évolution de la relation patient/professionnel de santé, sans omettre en particulier l'information du patient sur le recours à l'IA.

Le Conseil d'Etat évoque, en outre, les problématiques de protection des données de santé, sensibles, et le manque de qualité de ces données pour des SIA.

Par ailleurs, le Conseil d'Etat définit « *cinq grands types d'usage d'IA en santé* » : l'aide au diagnostic, l'aide à la prescription et à la décision médicale post diagnostic, la robotique médicale, l'aide à la gestion du parcours patient et l'appui aux fonctions administratives et médico-économiques.

Le Conseil d'Etat conclut que l'IA en santé est « *un facteur d'attractivité pour les professionnels, dans un cadre de pénurie croissante* ». Selon lui, il convient de « *construire l'IA en impliquant la multitude des acteurs en santé* ». En effet, l'IA ne remplacera pas l'humain « *du point de vue technique, organisationnel ou éthique* » bien qu'elle permette un traitement en masse de l'information « *et de disposer d'un « filet de sécurité » ».*

Dans quelle mesure ces réflexions/propositions seront prises en compte dans notre cadre juridique ?

A suivre…

Source : ici

DOCTRINE

RGPD

L'EHDS : stratégie, objectifs et préoccupations

La proposition de règlement sur l'espace européen des données de santé ou l'EHDS (pour « European Health Data Space »)[1], qui s'inscrit dans le cadre de la stratégie européenne pour les données, a suscité déjà des réactions des « Cnil » européennes. Retour sur une proposition de texte particulièrement novatrice en termes de data.

De nombreux textes en lien avec la « *data* » sont en cours d'élaboration, d'adoption ou viennent tout juste d'être adoptés au niveau de l'Union européenne (UE).

Cet accent mis sur les données s'inscrit dans un mouvement législatif européen plus général relatif au numérique, avec pour objectif ambitieux que l'Europe devienne un acteur au niveau mondial à la pointe de la « *transformation numérique* ». Dans ce cadre, une « *stratégie numérique* » européenne a été définie et menée depuis une petite dizaine d'années.

Pour l'actuelle décennie, la « *stratégie numérique* » poursuit plusieurs finalités telles que (i) la technologie au service de la personne, (ii) une économie juste et compétitive et (iii) une société ouverte, démocratique et durable. Le partage des données constitue l'un des grands axes de cette stratégie numérique donnant lieu à ce que l'on pourrait appeler une « *sous-stratégie* » : la stratégie européenne pour les données.

Présentée en février 2020, la stratégie européenne pour les données vise à renforcer l'utilisation des données et à créer un véritable marché unique des données dans le dessein d'apporter d'importants avantages aux citoyens et aux entreprises. Les buts sont clairs : mettre au point de nouveaux produits et services, améliorer les services fournis par le secteur public et générer de la productivité.

Pour ce faire, la stratégie européenne pour les données repose sur trois séries de textes : le règlement dit « *Data Governance Act* », la proposition de règlement appelée « *Data Act* » et dix règlementations sectorielles (santé, mobilité, énergie, industrie, environnement, agriculture, finance, etc.) relativement à des espaces européens commun de données dont fait partie l'EHDS.

Pour mémoire, le « *Data Governance Act* »[2] est entré en vigueur le 23 juin dernier et sera applicable à compter du 24 septembre 2023. Le règlement a pour objectif de faciliter le partage et la réutilisation de données – et ce, qu'il s'agisse de données à caractère personnel ou non - entre les secteurs (de l'économie, privé/public) et les Etats membres. Texte de gouvernance des données, le « *Data Governance Act* » définit essentiellement des processus et des mécanismes visant à faciliter la réutilisation des données protégées détenues par le secteur public, à assurer un fonctionnement fiable des services d'intermédiation de données et à favoriser la mise à disposition de données dans l'intérêt de la société.

Le « *Data Act* »[3] est, quant à lui, encore au stade d'une proposition de règlement datant du 23 février 2022. L'objectif de ce deuxième texte est de rendre davantage de données disponibles pour une utilisation conforme aux règles et aux valeurs de l'UE. Le « *Data Act* » complète ainsi le « *Data Governance Act* » en précisant les acteurs et les règles pour créer de la valeur à partir des données. A cette fin, le « *Data Act* » établit principalement des règles concernant l'utilisation des données générées par les appareils de l'Internet et de l'objet (objets connectés).

La proposition de règlement sur l'EHDS a été dévoilée le 3 mai dernier. Il s'agit de la première application du « *Data Governance Act* » et du « *Data Act* » dans un secteur : la santé. Le texte prévoit la mise en place de mesures propres à ce secteur afin de permettre le déploiement d'un espace européen commun des données dans ce domaine. C'est aussi une « *pierre angulaire* » dans la construction d'une Union européenne de la santé forte. Le but est d'« *exploiter le potentiel des données de santé pour les citoyens, les patients et l'innovation* »[4].

L'EHDS, un exemple d'approche sectorielle d'accès et de partage des données à l'échelle de l'UE

Un contexte particulier pour répondre à des objectifs ambitieux

La proposition de règlement sur l'EHDS a pour objectif de répondre au challenge de l'accès et du partage des données de santé dans toute l'UE. Plus précisément, l'EHDS vise à répondre à un constat global de difficultés rencontrées tant par les citoyens/patients que par les professionnels de santé, les autorités ainsi que les chercheurs, les organismes et les entreprises de l'UE, en termes de soins et d'innovations sanitaires

S'agissant des citoyens de l'UE, les difficultés portent sur l'accès, le contrôle et la transmission de leurs données de santé (carnet de santé, de vaccination, résultats d'analyse...) dans leur pays de résidence et, surtout, au-delà. Pour les professionnels de santé, les problématiques concernent surtout la compatibilité de format et d'éparpillement des données de santé de leurs patients. Les autorités de contrôle/régulation et les autorités politiques rencontrent, quant à elles, des difficultés pour disposer de données de santé numériques et exploitables. De la même manière, le domaine de la recherche et de l'innovation a de plus en plus besoin de pouvoir s'appuyer sur des données de santé fiables, en particulier pour la prévention et le traitement de maladies rares.

Plus encore, la crise sanitaire de la Covid-19 a révélé l'importance et le développement des services e-santé et ses enjeux notamment au regard de la protection de la vie privée et des cyberattaques croissantes dans ce secteur.

Dans un tel contexte, la proposition de règlement sur l'EHDS a pour finalité d'uniformiser au niveau européen les règles, les standards, les pratiques, les infrastructures pour pouvoir replacer le citoyen/patient « *au centre* » via le contrôle et l'utilisation de ses données de santé électroniques dans toute l'UE et, plus généralement, faciliter l'utilisation et le flux des données de santé électroniques pour les produits et services, la recherche et l'innovation ainsi que la politique publique en matière de santé.

L'utilisation primaire des données de santé électroniques

La première série de règles proposées par la proposition de règlement sur l'EHDS[5] concerne principalement les citoyens/patients de l'UE afin de faciliter le « *contrôle* » de leurs propres données de santé électroniques tant dans leur pays d'origine que dans les autres pays membres de l'UE « *dans le contexte de soins de santé* ». C'est ce que le texte appelle « *l'utilisation primaire* ».

Concrètement, il s'agit pour les citoyens européens de bénéficier d'un droit d'accès à leurs données de santé électroniques et ce, de façon simplifiée, immédiate et gratuite dans un format facilement lisible, consolidé et accessible. A l'instar des droits des personnes concernées au titre du RGPD et en allant plus loin, les citoyens européens doivent pouvoir « *contrôler* » leurs données de santé et notamment les compléter, les rectifier, connaître la manière dont elles sont utilisées et pour quelles finalités, mais aussi restreindre leur accès à certains destinataires. Les citoyens européens auront également la possibilité de partager leurs données de santé électroniques avec d'autres professionnels de santé de tous les Etats membres de l'UE pour de meilleurs services de soins.

Pour ce faire, un certain nombre de règles « *techniques* » sont proposées telles que (i) l'émission et l'acceptation de documents de santé (dossiers des patients, résultats de laboratoires, prescriptions électroniques, etc.) dans un format européen commun auquel les Etats membres devront veiller, (ii) l'obligation de se conformer à des mesures d'interopérabilité et de sécurité (iii) ou encore la certification des fabricants de système médicaux électroniques qui respectent ces règles.

A cela s'ajoute la désignation dans chaque Etat membre d'une autorité de santé numérique, l'ensemble d'entre elles participera alors à une infrastructure de services électroniques transfrontières pour aider les patients à partager leurs données dans toute l'UE (MyHealth@EU).

En d'autres termes, tout professionnel de santé de l'UE pourrait accéder à des antécédents médicaux de tout citoyen/patient de l'UE qui viendrait le consulter.

L'utilisation secondaire des données de santé électroniques

La proposition de règlement sur l'EHDS contient une deuxième série de règles[6] intéressant les chercheurs, les innovateurs et les autorités publiques en créant un cadre juridique pour qu'ils puissent utiliser, dans certaines conditions strictes, des données de santé électroniques « *de qualité élevée* » dans un environnement sécurisé respectant la vie privée. Il s'agit de « *l'utilisation secondaire* » des données de santé.

L'objectif affiché est de libérer, dans une certaine mesure, « *l'économie des données de santé* » au profit de nouveaux produits et services de l'e-santé. Les données de santé constituent effectivement une véritable « *mine d'or* », selon la Commission : « *D'après les estimations, la valeur de la réutilisation des données de santé se chiffrerait entre 25 et 30 milliards d'euros par an. Elle devrait atteindre quelque 50 milliards d'euros dans les dix années à venir* ». Plus récemment, une étude du Cabinet Veltys - remise au Health Data Hub - a fait état d'un gain d'environ 7,3 milliards d'euros par an pour l'économie française grâce à l'exploitation des données de santé[7]

Les données éligibles à l'utilisation secondaire sont, en particulier, les données figurant dans les dossiers médicaux électroniques, les données génétiques, les données de santé

électroniques générées par la personne via notamment les dispositifs médicaux ou les applications bien-être et autres applications de santé numériques, les données de santé électroniques provenant d'essais cliniques. En revanche, ces données doivent être pseudonymisées, c'est-à-dire sans possibilité d'identification du patient concerné. Par exemple, tel est le cas d'une maladie, d'un symptôme ou d'un traitement particulier sous réserve de ne pas pouvoir identifier de patient(s).

Ces données peuvent être traitées à des fins d'utilisation secondaire « *dans l'intérêt de la société* ».

Le projet de texte liste les finalités pouvant être poursuivies pour l'utilisation secondaire, celles-ci étant essentiellement liées à la recherche, l'innovation, l'élaboration de politiques, la sécurité des patients, la médecine personnalisée, les statistiques officielles ou les activités règlementaires. Des finalités interdites sont également indiquées telles que la prise de décision préjudiciable à une personne physique basées sur ses données, les publicités, les modifications des primes d'assurances, la création de produits ou services dangereux ou interdits.

Les demandes d'accès aux données de santé électroniques éligibles se feront selon une procédure d'autorisation auprès d'un organisme responsable de l'accès aux données désigné par chaque Etat membre.

Une seconde infrastructure décentralisée sera mise en place pour ce type de projets d'utilisation secondaire « *HealthData@EU* », infrastructure à laquelle l'ensemble des organismes responsables d'accès aux données de l'UE seront connectés.

A noter qu'un consortium regroupant 16 partenaires d'une dizaine de pays de l'UE et dirigé par le Health Data Hub a été sélectionné par la Commission européenne pour travailler sur projet pilote de l'EHDS[8]. En particulier ce consortium aura pour mission « *de développer et déployer un réseau de plateformes sources de données (...) en connectant les plateformes des pays participants, et d'évaluer la faisabilité, l'intérêt et la capacité à déployer une telle infrastructure à l'échelle de toute l'Union* ». Des tests seront effectués « *à travers des cas d'usage concrets de recherche* ».

La gouvernance et le RGPD

La proposition de règlement contient aussi des mesures de gouvernance dont la création d'un comité de l'espace européen des données présidé par la Commission ayant notamment pour mission (i) de faciliter la coopération entre les Etats membres et (ii) d'aider à la coordination des pratiques des autorités de santé numérique et des organismes responsables de l'accès aux données de santé.

Les données personnelles de santé étant au cœur de l'EHDS, se pose naturellement la question de l'articulation de ce nouveau projet de règlementation avec le RGPD que l'EHDS « *complète* » selon les propres termes de ce dernier.

La Commission européenne a effectivement pointé les difficultés (en particulier en raison des limites d'interopérabilité) pour les personnes physiques d'exercer leurs droits sur leurs données de santé « *malgré les dispositions (...) du RGPD* », mais aussi « *le manque d'uniformité dans la mise en œuvre et l'interprétation du RGPD par les États membres* » qui « *crée des incertitudes juridiques considérables qui engendrent des obstacles à l'utilisation secondaire des données de santé* »[9].

L'EHDS « *vise donc à compléter les droits et garanties prévus dans le RGPD, de sorte que ses objectifs puissent effectivement être atteints* ».

La Commission précise aussi que « *la proposition est conçue dans le respect total (...) du RGPD* », l'article 1.4 de l'EHDS précisant que ce texte s'applique sans préjudice du RGPD.

L'EHDS, un objet de préoccupations des « Cnil » européennes

Saisis par la Commission européenne, le Comité européen de la protection des données (le « *CEPD* ») et le Contrôleur européen de la protection des données (l'« *EDPB* ») ont adopté, le 12 juillet 2022, un avis sur l'EHDS, dans lequel ils ont souhaité attirer l'attention sur « *un certain nombre de préoccupations majeures* » concernant la proposition de règlement sur l'EHDS.

Si le CEPD et l'EDPB comprennent (i) que faciliter l'utilisation des données de santé électroniques (tant pour l'utilisation primaire que secondaire), pourrait contribuer de manière significative aux intérêts publics, ainsi qu'aux intérêts des patients et (ii) que le texte vise par ailleurs à renforcer le contrôle et les droits de ces derniers sur leurs données, ils notent aussi que « *les dispositions de cette proposition ajouteront une couche supplémentaire à la collection déjà complexe (à plusieurs niveaux) de dispositions (que l'on trouve à la fois dans la législation de l'UE et des Etats membres) sur le traitement des données relatives à la santé (dans le secteur des soins de santé)* ». Il s'agit donc, selon ces deux autorités, de clarifier les interactions entre cette proposition et le RGPD afin d'assurer une application cohérente des deux textes et notamment en ce qui concerne les droits des personnes concernées.

Par ailleurs, le CEPD et l'EDPB demandent d'exclure, des cas d'utilisation secondaire, les données de santé électroniques générées par les applications de bien-être ou d'autres applications de santé numériques, étant précisé que, si elles devaient être maintenues, leur traitement à des fins d'utilisation secondaire devrait être soumis à un consentement préalable des personnes concernées (au sens du RGPD). En effet, selon les deux autorités, non seulement de telles données « *ne présentent pas les mêmes exigences de qualité*

et les mêmes caractéristiques que celles générées par les dispositifs médicaux », mais en outre « *ces applications génèrent une quantité énorme de données qui peuvent être très invasives puisqu'elles concernent chaque étape de la vie quotidienne des individus* ».

Les deux autorités ajoutent que « *même si les données relatives à la santé pouvaient effectivement être séparées des autres types de données, des déductions telles que les pratiques alimentaires et autres habitudes pourraient facilement être faites, révélant des informations particulièrement sensibles comme l'orientation religieuse* ».

De surcroît, les deux instances ne sont pas favorables à une extension du champ d'application des exceptions du RGPD concernant le droit des personnes, car elle aurait pour effet de limiter la possibilité pour les patients concernés d'exercer un contrôle effectif sur leurs données personnelles (ce qui serait en contradiction avec les objectifs visés dans la proposition de règlement).

En ce qui concerne les finalités d'utilisation secondaire des données (toute forme d' « *activité de développement et d'innovation pour des produits ou des services contribuant à la santé publique ou à la sécurité sociale* » ou « *la formation, le test et l'évaluation d'algorithmes, y compris dans les dispositifs médicaux, les systèmes d'IA et les applications de santé numériques, contribuant à la santé publique ou à la sécurité sociale* »), le CEPD et l'EDPB souhaitent que de tels objectifs, poursuivis dans le cadre des usages secondaires des données, soient mieux délimités, notamment par la démonstration d'un lien suffisant avec les enjeux de protection sociale et de santé publique.

Enfin, le CEPD et l'EDPB demandent qu'une compétence exclusive soit attribuée aux autorités de protection des données dans le traitement de toute question relative à la protection des données de santé électroniques.

La proposition de règlement sur l'EHDS est, à n'en pas douter, un texte novateur, tant sur le fond, s'agissant notamment du premier texte européen dédié à un sujet d'e-santé, que sur la forme, en définissant le cadre juridique du premier espace commun européen de partage de données, en l'occurrence des données de santé.

Les premières observations des « *Cnil* » européennes illustrent toutefois les problématiques que peut susciter ce texte et, en particulier, la difficulté de placer au mieux le curseur entre les enjeux de santé publique et d'innovation, d'une part, et la protection de la vie privée, d'autre part.

Alexandre FIEVEE
Avocat Associé

Alice ROBERT
Avocat senior

Derriennic Associés

Notes

(1) **Proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, COM(2022) 197/2,** 3 mai 2022.

(2) Règlement (UE) 2022/868 « portant sur la **gouvernance des données** ».

(3) **Proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), 23 février 2022.**

(4) **Communication de la Commission au Parlement** européen et au Conseil : « **Un espace européen** des données de santé : **exploiter le potentiel des données de santé pour les citoyens, les patients et l'innovation**

(5) **COM/2022/196 final** ».

(6) **Chapitre II de la proposition de règlement EHDS**

(7) **Chapitre IV de la proposition de règlement EHDS**

(8) https://**www.health-data-hub.fr/actualites/les-donnees-de-sante-un-potentiel-encore-insuffisamment-exploite**

(9) **Communiqué de presse du Health Data hub du** 18 juillet 2022 « **Lancement d'un projet pilote pour l'Espace européen des données de santé : vers de nouvelles opportunités pour la recherche** en santé européenne ».

(10) **Proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, COM(2022) 197/2,** 3 mai 2022, **1. Contexte de la proposition.**