LES DONNÉES DE SANTÉ ET LE RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES

JEANNE BOSSI MALAFOSSE
Avocat associé, DELSOL Avocats

La collecte et le traitement des données personnelles de santé sont soumis depuis le 25 mai 2018 au respect des conditions posées par le Règlement général sur la protection des données (RGPD) du 27 avril 2016. Ils doivent d'ores et déjà se déployer dans un contexte juridique national complexe et mouvant mais supposé apte à relever les défis du Big Data.

Le RGPD introduit de nouveaux concepts et modifie les obligations des acteurs impliqués dans le traitement de données personnelles. Il renforce les droits des personnes et vise à assurer une application homogène et cohérente des règles de protection des données personnelles.
Le règlement instaure le principe d'*accountability* aux termes duquel chaque acteur devra être en mesure de prouver, à tout moment, que les traitements qu'il met en œuvre respectent les principes de protection des données personnelles. Associé à l'obligation d'intégrer, en amont de l'ensemble des projets, les principes de protection des données *(Privacy by design)*, le règlement instaure une nouvelle façon d'appréhender la protection des données personnelles.
Le nouveau texte européen reconnaît que certaines données « méritent une protection plus élevée »[1] dont les données de santé et les données génétiques. Leur traitement est soumis aux dispositions du Règlement mais les Etats membres bénéficient d'une marge de manœuvre pour maintenir ou introduire « des conditions supplémentaires y compris des limitations en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé »[2], reflétant ainsi des organisations sanitaires différentes.
Il introduit une nouvelle définition des données de santé[3] qui vise l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée quelque soit la source de production de la donnée (un professionnel de santé ou un dispositif médical par exemple).
Sont ainsi considérées comme des données de santé, toutes informations relatives à l'identification du patient dans le système de soin ou le dispositif utilisé pour collecter et traiter des données de santé, toutes informations obtenues lors d'un examen médical y compris des échantillons biologiques et des données génomiques et toutes informations médicales (une maladie, un handicap, une donnée clinique ou thérapeutique, physiologique ou biologique)[4].
Le RGPD pose un principe d'interdiction du traitement des catégories particulières de données parmi lesquelles figurent les données de santé[5]. Il énumère toutefois, par exception, les finalités de traitement possibles et encadre leur traitement (article 9)[6]. *(voir encadré)*
Les conditions de chacune de ces exceptions peuvent ainsi être invoquées pour fonder la licéité du traitement envisagé qui est alors soumis au respect des principes prévus par le RGPD. Toutefois, compte tenu de la spécificité de chaque organisation nationale, le règlement renvoie au droit des États membres le soin de définir des conditions supplémentaires pour le traitement de ces données.

> Chaque acteur devra être en mesure de prouver, à tout moment, que les traitements qu'il met en œuvre respectent les principes de protection des données personnelles

LES CONDITIONS DU TRAITEMENT DES DONNÉES DE SANTÉ DANS LE RGPD

Le respect des principes de protection des données personnelles repose sur la logique de l'*accountability*.
La conformité au RGPD peut, dans certains cas énumérés par le RGPD, être conduite par un délégué à la protection des données (DPO) sous la responsabilité du responsable de traitement, obligatoire lorsque les activités de base de l'organisme consistent en des traitements à grande échelle de données sensibles, dont les données de santé (article 37).

> Le nouveau texte européen reconnaît que certaines données « méritent une protection plus élevée » dont les données de santé et les données génétiques

Le DPO interviendra notamment pour assister le responsable de traitement dans la conduite de l'étude d'impact sur la vie privée exigée par exemple pour les traitements à grande échelle de données de santé. Elle permet d'identifier des mesures de sécurité techniques et organisationnelles appropriées, propres à réduire le risque[8].
Par ailleurs, le RGPD prend en compte de nouvelles capacités d'analyse des données. Il introduit la notion de finalité compatible avec celle pour laquelle les données ont été collectées, ce qui est de nature à faciliter la réutilisation des données lorsqu'elles ont été collectées de manière licite, sans pour autant affaiblir les droits des personnes.
Le RGPD assouplit également l'obligation d'information de la personne concernée, lorsque « la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés » sous réserve de l'adoption de mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée[9]. Cette disposition trouve toute son utilité dans le domaine de la recherche où elle permet d'envisager une utilisation secondaire des données.
En parallèle, le nouveau réglement renforce le droit des personnes face à l'utilisation des nouvelles techniques d'analyse des données, comme le profilage, dont il encadre l'utilisation[10]. Les personnes bénéficient du droit de ne pas faire l'objet d'une prise de décision individuelle automatisée produisant

LES FINALITÉS DE TRAITEMENT POSSIBLES

Parmi celles-ci, on peut notamment citer les cas suivants :

a- la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée,

b- le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée,

c- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement,

d- le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3,

e- le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel.

1- Voir en ce sens considérant 53 du RGPD.
2- Ibid.
3- Règlement (UE) 2016/679 du Parlement européen et du Conseil 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (RGPD).
4- Voir en ce sens, PE et Cons. UE, règl. (UE). n°2016/679, 27 avr.2016, consid. 35.
5- Article 9 du RGPD « Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits ».
6- Article 35 du RGPD.
8- Dans le domaine de la recherche médicale, la CNIL avait d'ores et déjà anticipé ces principes en rédigeant des méthodologies de références, qui fixent des mesures de sécurité minimales et impliquent la réalisation d'une analyse de risque qui préfigure la réalisation de l'étude d'impact telle qu'exigée par le règlement.
9- Article 14, paragraphe 5, point b) du RGPD.
10- Article 22 du RGPD.

des effets juridiques la concernant ou l'affectant de manière significative. Lorsque le profilage implique des données de santé, ce traitement est conditionné au recueil du consentement de la personne concernée ou à des motifs d'intérêt public et à condition que « des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ne soient en place ».

Enfin, le RGPD introduit l'obligation de notification des violations de données personnelles[11]. Cette nouvelle obligation s'ajoute à l'obligation actuelle de signalement des incidents de sécurité des systèmes d'information de santé prévue à l'article L.1111-8-2 du code de la santé publique qui prévoit l'obligation pour les établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins, de signaler des incidents de sécurité des systèmes d'information de santé auprès de l'ASIP Santé.

Lorsque le profilage implique des données de santé, ce traitement est conditionné au recueil du consentement de la personne concernée ou à des motifs d'intérêt public

LA NÉCESSAIRE PRISE EN COMPTE DU DROIT NATIONAL POUR LE TRAITEMENT DES DONNÉES DE SANTÉ

« Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé »[12]. Les acteurs devront ainsi se référer au code de la santé publique, ainsi qu'à la loi nationale sur la protection des données personnelles.

Les règles propres à l'échange et au partage des données de santé sont à souligner. Le code de la santé publique rappelle le droit au respect de la vie privée et au secret des informations pour la personne concernée (article L1110-4). Il définit de façon précise l'équipe de soins[13] qui permet le partage au bénéfice d'un même patient les données de santé utiles à sa prise en charge dans les domaines sanitaire, médico-social et social, et rend opposables les référentiels de sécurité et d'interopérabilité définis par l'ASIP Santé et approuvés par voie d'arrêté pris par le ministre en charge de la santé après avis de la CNIL et publiés au Journal Officiel[14].

Le code de la santé publique rappelle le droit au respect de la vie privée et au secret des informations pour la personne concernée

Les conditions du traitement des données à des fins de recherche sont actuellement visées au chapitre IX de la loi Informatique et Libertés[15] et définissent un régime d'autorisation pour tous les traitements de données personnelles réalisés à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé. Cette procédure doit être lue avec les dispositions de l'article 193 de la loi du 26 janvier 2016 de modernisation de notre système de santé qui crée également un nouveau régime juridique d'accès aux bases de données médico-administratives avec la création du Système national des données de santé (SNDS)[16]. Ces procédures font intervenir le nouvel Institut national des données de santé (INDS) et le comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (le CEREES) quand il ne s'agit pas de recherches impliquant la personne humaine.

Dans ce dernier cas, il convient de prendre en compte le cadre réglementaire des recherches impliquant la personne humaine[17], récemment revu par la loi Jardé et qui doit également s'intégrer au régime d'autorisation des articles 53 et suivants de la loi Informatique et Libertés.

Si le RGPD est désormais le texte de référence en matière de protection des données, il devra être appliqué avec les dispositions de la nouvelle loi Informatique et Libertés qui traitera des sujets sur lesquels le règlement a renvoyé au droit des États membres. Le traitement des données de santé en fait partie.

11- Les violations de données personnelles sont définies aux articles 33 et 34 du RGPD comme toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données; elle impose au responsable de traitement de la notifier dans les meilleurs délais à l'autorité de protection des données et, si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés, à la personne concernée.

12- Article 9 du RGPD.

13- Article L1110-12 du code de la santé publique.

14- Les référentiels de sécurité et d'interopérabilité font référence :
- aux règles de certification de l'identité des professionnels de santé impliqués dans les systèmes d'information,
- aux règles de certification de l'identité des patients eux-mêmes en reconnaissant désormais au numéro de sécurité sociale le caractère d'identifiant national de santé (article L1110-8-1 du code de l santé publique),
- aux niveaux des moyens d'authentification retenus pour les acteurs en fonction de l'analyse de risque du système d'information,
- à l'encadrement de l'activité d'hébergement des données de santé (article L111à-8 du code de la santé publique),
- au cadre national d'interopérabilité des systèmes d'information.
Ces référentiels sont définis et détaillés dans la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).

15- Articles 53 et suivants.

16- SNIIRAM, PMSI, causes médicales de décès, CNSA, échantillon AMC.

17- Articles L1121-1 et suivants du code de la santé publique.