Communication
Commerce électronique
Pays : France
Périodicité : Mensuel

Date : AVRIL 18
Journaliste : Jeanne BOSSI MALAFOSSE

12

Le traitement des données de santé et le Règlement européen sur la protection des données du 27 avril 2016

Étude

Jeanne BOSSI MALAFOSSE,
avocat associé Delsol Avocats

La collecte et le traitement des données personnelles de santé seront à partir du 25 mai prochain soumis au respect des conditions posées par le Règlement européen sur la protection des données 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*.

1 - Le Règlement général sur la protection des données (ci-après le RGPD) sera applicable le 25 mai 2018. Il introduit de nouveaux concepts et modifie les obligations des acteurs impliqués dans le traitement de données personnelles. Ses objectifs sont multiples, remplaçant la directive de 1995, le RGPD 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.

2 - Si ce nouveau texte européen impacte l'ensemble des activités, il 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 États 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.

L'intégration des nouveaux principes posés par le règlement et l'exercice de cette marge de manœuvre nécessitent l'adaptation de l'actuelle loi Informatique et Libertés [3]. Un projet de loi relatif à la protection des données actuellement en cours de discussion au Parlement va permettre d'adapter le droit national au texte européen (ci-après « le projet de loi ») [4].

1. V. en ce sens *RGPD, cons. 53.*
2. *Ibid.*
3. *L. n° 78-17, 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés.*
4. *AN, Projet de loi n° 490, relatif à la protection des données personnelles* (Procédure accélérée).

3 - Le traitement des données de santé doit donc intégrer aujourd'hui les dispositions du RGPD, celles de la loi n° 78-17 du 6 janvier 1978 relatives à l'informatique, aux fichiers et aux libertés (ci-après loi Informatique et Libertés) et demain, sa modification avec l'adoption du projet de loi en cours. Il doit également prendre en compte l'ensemble des dispositions du Code de la santé publique et du Code de la sécurité sociale susceptibles d'impacter leur collecte et leur traitement.

1. L'impact du RGPD sur le traitement des données de santé

A. - Définition des données de santé et protection applicable

4 - C'est un apport majeur du texte européen que de définir la donnée de santé. – 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 contrôle ou d'un examen médical y compris des échantillons biologiques et des données génomiques, toutes informations médicales : par exemple, une maladie, un handicap, un risque de maladie, une donnée clinique ou thérapeutique, physiologique ou biologique, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un dispositif médical ou d'une exploration *in vivo* ou *in vitro* [5].

Cette nouvelle définition traduit un concept plus large de la donnée de santé, prenant en compte le fait que la prise en charge sanitaire d'une personne emporte également la connaissance de sa situation familiale ou sociale et fait intervenir des acteurs multiples, professionnels de santé et personnels sociaux.

5 - Ce concept élargi de la donnée de santé s'accorde en France avec la notion redéfinie de l'équipe de soins par la loi

5. V. en ce sens, *PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 2016, cons. 35.*

n° 2016-41 du 26 janvier 2016 *(CSP, art. L. 1110-12)* qui regroupe *« un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à [leur] la coordination... »* [6].

Les données de santé sont donc considérées tant par le RGPD [7], que la loi Informatique et Libertés [8] comme des données sensibles dont il convient d'encadrer le traitement par une protection particulière.

6 - **Un principe d'interdiction accompagné de dérogations. –** Le RGPD, comme l'article 8 de la loi Informatique et Libertés, pose le principe d'interdiction du traitement des données sensibles [9].

Ce principe est ensuite assorti d'une série d'exceptions autorisant leur traitement. On retrouve dans le Règlement les exceptions suivantes :

- le consentement explicite de la personne sauf si le droit d'un État membre ou de l'Union prévoit que l'interdiction ne peut être levée par ce seul consentement ;
- l'exécution d'obligations ou de droits dans le domaine de la protection sociale ;
- la sauvegarde des intérêts vitaux de la personne ;
- l'intérêt légitime du responsable de traitement moyennant des garanties appropriées ;
- les motifs d'intérêt public ;
- l'ensemble des traitements nécessaires aux fins de la médecine préventive ou de la médecine du travail, de diagnostics médicaux, de la prise en charge sanitaire ou sociale ou de la gestion des systèmes et des services de santé ou de protection sociale [10].

Le Règlement vise également les traitements pour des motifs d'intérêt public dans le domaine de la santé publique ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, ainsi que la recherche scientifique.

Ces dérogations sont similaires à celles qui figurent actuellement à l'article 8 de la loi Informatique et Libertés [11].

7 - Le projet de loi relatif à la protection des données visant à adapter la loi Informatique et Libertés au règlement européen choisit de rassembler dans un même chapitre IX tous les traitements de données personnelles de santé quelle que soit leur finalité.

Il fait une distinction entre les traitements de données de santé qui ne sont pas soumis au chapitre IX mais restent redevables du respect des dispositions du Règlement européen et ceux qui y sont soumis à la condition de poursuivre un intérêt public complété lors de la discussion parlementaire d'une précision importante visant à appliquer plus finement le RGPD en intégrant à l'intérêt public, la finalité d'une garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux.

Les premiers traitements visés sont ceux indiqués aux 1° à 6° du projet d'article 8-II et les traitements permettant d'effectuer des études à partir des données recueillies dans le cadre de l'administration des soins en application du 6° du II de l'article 8 lorsque ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif ; les traitements mis en œuvre aux fins d'assurer le service des prestations ou le contrôle par les organismes d'assurance maladie obligatoire et complémentaire ; les traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale ; les traitements effectués par les agences régionales de santé, par l'État et par la personne publique désignée par lui en application du premier alinéa de l'article L. 6113-8 du Code de la santé publique.

Si cette orientation est compréhensible et peut répondre à un souci de clarification, le choix en revanche de traiter sous une même section unique intitulée « *Dispositions Générales* », l'ensemble des traitements, qu'il s'agisse de prodiguer des soins ou de mener une recherche est de nature à introduire une confusion et conduit le Gouvernement à imposer aux premiers des obligations qui sont caractéristiques des seconds.

Le projet d'article 54 introduit un régime de formalités préalables plus lourd (l'autorisation) dès lors qu'on ne peut attester de la conformité de son traitement à des référentiels et règlements types établis par la CNIL en concertation avec l'Institut national des données de santé, ce qui contredit l'esprit d'allégement porté par le Règlement.

Comme pour toute donnée personnelle, les traitements de données de santé doivent respecter les conditions de licéité posées par le RGPD et le responsable de traitement doit mettre en œuvre des mesures techniques et organisationnelles propres à assurer le respect des principes de protection des données personnelles.

B. - Le respect des principes de protection des données personnelles appliqués aux données de santé

8 - L'utilisation des données de santé doit s'accorder avec le respect des cinq grands principes de protection des données personnelles tels que rappelés par le RGPD [12].

Pour leur application chaque acteur devra être en mesure de prouver à tout moment que les traitements qu'il met en œuvre respectent ces principes *(accountability)*. Associé à l'obligation d'intégrer en amont des projets les principes de protection des données *(Privacy by design)*, il instaure une nouvelle façon d'appréhender la protection des données personnelles.

Le traitement des données de santé n'échappe pas à cette nouvelle façon de gérer la protection des données et, au surplus, la réalisation d'études d'impact permettant d'analyser les risques pour les droits et libertés fondamentales est exigée pour les traitements à grande échelle de données de santé [13].

9 - Mais il est intéressant de noter qu'à côté de ces éléments communs à l'ensemble des traitements de données personnelles, le Règlement comporte certaines dispositions qui apparaissent nouvelles et peuvent être utiles à l'heure des nouvelles techniques de *data mining* particulièrement utilisées dans le cadre du *Big Data* et l'intelligence artificielle.

10 - Le RGPD introduit par exemple 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.

6. Cette compréhension large du secteur de la santé, intégrant le secteur sanitaire, médico-social ou social est également reprise dans le projet de recommandation du Conseil de l'Europe sur les données de santé qui devrait être publiée en 2018.
7. *RGPD, art. 9.*
8. *L. n° 78-17, 6 janv. 1978, art. 8.*
9. *Règl. (UE) n° 2016/679, 27 avr. 2016, cons. 10.*
10. V. liste exhaustive, *PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 2016, art. 9, § 2.*
11. S'y ajoute l'anonymisation à bref délai.
12. Une finalité de traitement déterminée et légitime, des données pertinentes (principe de proportionnalité), une durée de conservation déterminée, le respect du droit des personnes et de leur information et la mise en place de mesures de sécurité de nature à garantir la confidentialité des données.
13. *RGPD, art. 35.*

11 - **Notion de pseudonymisation consacrée.** – S'agissant de la nature des données collectées, le RGPD consacre la notion de pseudonymisation dont il donne une définition [14]. Même si elles restent des données personnelles, les données pseudonymisées peuvent faciliter la collecte de données dans des cas où le recueil de données directement nominatives eut été plus compliqué.

12 - Concernant les droits des personnes, le RGPD permet d'assouplir l'obligation d'information de la personne concernée dans certains cas précis. C'est notamment le cas 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. Cette disposition est particulièrement utile dans le domaine de la recherche où elle permet d'envisager une utilisation secondaire des données et dans des cas où il serait trop contraignant de retrouver la personne pour l'informer.

Dans un souci d'équilibre caractéristique du texte, le RGPD renforce les droits des personnes concernées face à l'utilisation de nouvelles techniques d'analyse des données. Ainsi, le droit de la personne de ne pas faire l'objet d'une prise de décision individuelle automatisée produisant des effets juridiques la concernant ou l'affectant de manière significative est appliqué de manière plus stricte quand il porte sur des données sensibles, dont les données de santé [15].

13 - Sur la sécurité des données, le règlement préconise qu'elle soit adaptée à la nature sensible des données. Le RGPD prévoit que l'application d'outils de soft *law* (code de conduite, certification) pourra servir d'instruments pour démontrer le respect des exigences en matière de sécurité.

Notons que le projet de loi actuellement en discussion au Parlement donne à la CNIL la possibilité d'établir et de publier des règlements types en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données de santé relevant du chapitre IX [16].

La nouvelle obligation de notification d'une violation de données [17] dès lors, qu'elle est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques s'accorde avec l'obligation prévue par le Code de la santé publique qui impose, aux établissements de santé et 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 [18].

Pour assurer la mise en œuvre et le respect de ces principes, la désignation d'un délégué à la protection des données (DPO) est obligatoire pour les responsables de traitement et sous-traitants mettant en œuvre des traitements de données sensibles, notamment des données de santé, à grande échelle [19].

À l'ensemble de ces exigences s'ajoute une réglementation spécifique propre aux données de santé, définie en France et illustrant la marge de manœuvre laissée aux États membres.

2. La marge de manœuvre laissée au droit national : un niveau de sécurité élevé dans un environnement juridique complexe

A. - L'échange et le partage des données de santé

14 - Le traitement de données personnelles de santé tel qu'il est défini dans le RGPD s'intègre en France à un cadre juridique prévu par le Code de la santé publique modifié récemment par l'adoption de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

Ainsi, la nouvelle définition de données de santé proposée par le règlement doit être lue avec la notion de l'équipe de soins, désormais redéfinie et adaptée à la réalité de l'échange et du partage des données personnelles. À cet effet, le nouvel article L. 1110-4 du Code de la santé publique précité tout en réaffirmant le secret de la vie privée redessine le régime de l'échange et du partage des données personnelles de santé en l'articulant avec une notion élargie d'équipe de soins *(CSP, art. L. 1110-12)*.

15 - À cette nouvelle définition de l'équipe de soins est associée une harmonisation des régimes d'information et de consentement. Au sein d'une équipe est réservé le régime de l'information préalable de la personne concernée et de la reconnaissance de son droit d'opposition, l'exigence du recueil du consentement de la personne étant réservée au partage d'informations en dehors de cette équipe.

16 - L'article L. 1110-4-1 du Code de la santé publique vise le nécessaire respect par les responsables de systèmes d'information des 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* [20].

17 - La réforme récente, sous l'impulsion du règlement eIDAS [21], du cadre juridique reconnaissant la valeur probante des dossiers médicaux numérisés en France est également importante *(CSP, art. L. 1111-25 s.)*. L'ensemble de ces référentiels illustre un niveau de sécurité d'ores et déjà élevé en France qui précède l'adoption du RGPD et dont le respect permettra

14. L'article 4 du RGPD définit la pseudonymisation comme « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* ».
15. La prise de décision automatisée n'est alors possible qu'avec le consentement de la personne, ou pour 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.
16. La CNIL avait d'ores et déjà anticipé ces principes en rédigeant des méthodologies de référence, 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.
17. *RGPD, art. 33.*
18. L'article L. 1111-8-2 du Code de la santé publique dispose que « *Les établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins signalent sans délai à l'agence régionale de santé les incidents graves de sécurité des systèmes d'information. Les incidents de sécurité jugés significatifs sont, en outre, transmis sans délai par l'agence régionale de santé aux autorités compétentes de l'État* ».
19. *Règl. (UE) n° 2016/679, 27 avr. 2016, art. 39, § 2.*
20. Ces référentiels prévoient la nécessité de certifier l'identité des professionnels de santé impliqués dans les systèmes d'information par l'inscription au répertoire partagé des professionnels de santé (RPPS). L'ensemble des professions de santé incluant dorénavant les professionnels du secteur médico-social et social ont également vocation à intégrer un annuaire national. Ils prévoient la certification de l'identité des patients permettant d'assurer l'identito-vigilance au sein des systèmes d'information en reconnaissant désormais au numéro de sécurité sociale le caractère d'identifiant national de santé (INS) mettant ainsi fin à des années de discussion et d'hésitation autour de l'utilisation de cet identifiant qui a toujours eu une place particulière au sein de la loi Informatique et Libertés. Ils encadrent l'activité des hébergeurs de données de santé à caractère personnel qui évolue d'un régime d'agrément vers un régime de certification.
21. Le règlement n° 910/2014 du 23 juillet 2014 vise à « *instaurer un climat de confiance dans l'environnement en ligne* » *(cons. 1)*, « *en fournissant un socle commun pour des interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques* » *(cons. 2)*, s'assurer également que « *concernant l'accès aux services en ligne transfrontaliers proposés par les États membres, l'identification et l'authentification électronique sécurisées sont possibles* » *(cons. 12)*.

demain, aux responsables de traitement, de démontrer leur conformité au règlement.

B. - Le traitement des données de santé dans le cadre de la recherche

18 - Un cadre juridique complexe et actuellement mouvant régit les conditions d'accès aux données de santé pour la recherche. Il implique la mise en œuvre des principes du RGPD, de la loi Informatique et Libertés, et demain, du projet de loi sur la protection des données personnelles (le projet de loi) modifiant la loi Informatique et Libertés.

19 - Les conditions du traitement des données à des fins de recherche sont actuellement visées au chapitre IX de la loi Informatique et Libertés [22] et définissent un régime d'autorisation pour tous les traitements de données à caractère personnel 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), composé des grandes bases de données médico-administratives [23].

Les conditions d'accès au SNDS [24] sont limitées :

- soit à des fins de recherche, d'étude ou d'évaluation contribuant à une finalité mentionnée au III de l'article L. 1461-1 du Code de la santé publique [25] et répondant à un motif d'intérêt public ;

- soit pour l'accomplissement des missions des services de l'État, des établissements publics ou des organismes chargés d'une mission de service public (procédure spécifique d'accès pour les organisations chargées d'une mission de service public).

20 - Ces procédures font intervenir le nouvel Institut national des données de santé (INDS) [26] et le Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (le CEREES) qui se prononce sur la méthodologie retenue, la nécessité du recours à des données à caractère personnel, la pertinence de celles-ci par rapport à la finalité poursuivie et, le cas échéant, la qualité scientifique du projet [27].

Cette procédure mise en place récemment soulève des interrogations de nature différente relevant tout à la fois de sa complexité, du régime plus contraignant imposé aux acteurs du privé et de son esprit décalé par rapport à la responsabilisation des acteurs mis en avant par le RGPD.

À cette situation s'ajoute le cadre réglementaire des recherches impliquant la personne humaine récemment revu par la loi Jardé [28] et qui doit également s'intégrer au régime d'autorisation des articles 53 et suivants de la loi Informatique et Libertés [29].

21 - La notion d'intérêt public, qui n'obéit pas à une définition juridique précise, introduit également une subjectivité dans son appréciation et une inquiétude légitime de la part des acteurs qui s'inquiètent de l'importance désormais accordée à ce critère qui n'existait pas jusqu'à présent pour apprécier la conformité d'un projet de recherche aux règles de protection des données personnelles.

À ce titre, la souplesse d'interprétation de cette notion introduite récemment par la CNIL à propos des entrepôts de données de santé, qu'ils soient menés par des organismes publics ou privés, devra être maintenue pour permettre le développement des outils de *Big Data* [30].

22 - Il semble que ces craintes aient été entendues par le Parlement dans le cadre des discussions sur le projet de loi d'adaptation au RGPD qui prend désormais en compte à côté de la finalité d'intérêt public l'autre finalité prévue par le Règlement relative à « *la garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux* [qui] *constitue une finalité d'intérêt public* » y compris pour la recherche.

Ces évolutions visant à faciliter l'accès aux données de santé dans le respect des droits de la personne doivent s'accompagner d'une politique visant à organiser l'urbanisation des systèmes d'information de telle façon qu'à côté de la fonction de production du soin, une fonction de production de la connaissance vienne contribuer à élever le niveau de la santé publique. ■

Mots-Clés : RGPD - Données de santé
Données de santé - RGPD

22. *L. n° 78-17, 6 janv. 1978, art. 53 s.*
23. Sniiram, PMSI, causes médicales de décès, CNSA, échantillon AMC.
24. *D. n° 2016-1871, 26 déc. 2016, relatif au traitement de données à caractère personnel* dénommé « SNDS ».
25. *CSP, art. L. 1461-1, « III.– Le système national des données de santé a pour finalité la mise à disposition des données, dans les conditions définies aux articles L. 1461-2 et L. 1461-3, pour contribuer :*
1° À l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité ;
2° À la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale ;
3° À la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales ;
4° À l'information des professionnels, des structures et des établissements de santé ou médico-sociaux sur leur activité ;
5° À la surveillance, à la veille et à la sécurité sanitaires ;
6° À la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale ».
26. Le groupement d'intérêt public INDS a été créé par arrêté du 20 avril 2017 et a pour missions de :
– veiller à la qualité des données de santé et aux conditions générales de leur mise à disposition, garantissant leur sécurité et facilitant leur utilisation ;
– assurer le guichet unique pour les demandes d'accès aux données aux fins de recherche ;
– émettre un avis sur le caractère d'intérêt public que présente une recherche, une étude ou une évaluation ;
– faciliter la mise à disposition d'échantillons ou de jeux de données agrégées mentionnées dans des conditions préalablement homologuées par la Commission nationale de l'informatique et des libertés (CNIL) ;
– contribuer à l'expression des besoins en matière de données anonymes et de résultats statistiques, en vue de leur mise à la disposition du public.
27. Ce comité prend la suite du Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé avec des missions similaires.
28. *L. n° 2012-300, 5 mars 2012, relative aux recherches impliquant la personne humaine.*
29. La CNIL dispose fort heureusement d'un pouvoir de simplification important dont elle a déjà fait usage (méthodologies de référence et autorisations uniques).
30. *CNIL, délib. n° 2017-013, 19 janv. 2017 autorisant l'Assistance publique – Hôpitaux de Paris à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité un entrepôt de données de santé, dénommé « EDS » (demande d'autorisation n° 1980120). – CNIL, délib. n° 2017-285, 26 oct. 2017 autorisant la société OpenHealth Company à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la constitution d'un entrepôt de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.*