La protection des données à caractère personnel à l'ère de la santé connectée Un droit européen perfectible ?

Sophie Gambardella

La protection des données à caractère personnel à l'ère de la santé connectée
Un droit européen perfectible ?

Sophie GAMBARDELLA
Docteur en droit[1]
Aix Marseille Université, Université de Toulon, Univ Pau & Pays Adour
CNRS, DICE UMR 7318, CERIC, Aix-en-Provence, France

La montée en puissance d'acteurs au sein des processus décisionnels a souvent provoqué de la défiance dans la doctrine notamment juridique, comme en attestent les débats autour de l'avènement d'un apparent « gouvernement des juges »[2] ou encore d'un prétendu « gouvernement des experts ». A l'heure actuelle, la crainte d'une confiscation du pouvoir décisionnel ne découle plus du rôle joué par une catégorie d'acteurs mais du progrès technique et des nouvelles technologies qui en résultent. L'heure est au « gouvernement de la technologie ». Les réflexions engagées sur l'avenir d'une justice prédictive, le développement de technologies persuasives ou encore la prolifération des objets connectés mettent toutes l'accent sur le bouleversement opéré par les mutations technologiques sur nos processus décisionnels, nos habitudes, nos modes de vie et peut-être même nos modes de raisonnement. Le domaine de la santé n'a pas été épargné par cette colonisation technologique, la santé devient elle aussi connectée.

Le développement de la santé connectée est prolifique et bénéfique. La santé connectée permet des avancées en matière de qualité de la santé, de qualité des soins, d'accès aux soins et, dans le même temps, est une source de réduction des dépenses de santé[3]. La santé connectée offre, en d'autres termes, tout à la fois des perspectives pour le renforcement de la qualité de la santé et pour l'assainissement des finances des systèmes de santé. Si les progrès, dont la santé connectée est porteuse, ne doivent pas être minimisés, les risques inhérents à cette dernière ne peuvent pas non plus l'être. En premier lieu, la santé connectée modifie la relation médecin-patient traditionnelle. Dans le cadre de la relation de santé, un certain nombre de données sont produites : certaines sont issues des examens médicaux ; d'autres du patient lui-même. Or, si la relation patient-médecin est majoritairement dématérialisée, les données produites par le patient lui même telles que son ressenti, son émotionnel peuvent échapper au médecin. Est-ce alors un problème pour la qualité des soins ? Dans la mesure où ces informations peuvent permettre de réfléchir sur les causes d'une maladie, d'une épidémie, elles sont nécessaires pour assurer une meilleure prise en charge du patient mais aussi pour améliorer la prévention médicale. Un raisonnement quasi mathématique priverait alors peut-être le corps médical d'informations fondamentales pour penser les causes de certaines affections. En deuxième lieu, la santé connectée tend à priver l'individu de son droit de ne pas savoir. En effet, un certain nombre d'applications, sans forcément être des dispositifs médicaux, indiquent, par exemple, aux individus les risques pour leur santé en fonction de leur activité physique, de leur âge ou encore de leur poids. A travers ces informations, ces technologies prédéfinissent ainsi le comportement à venir de l'individu et le prive alors d'une part de son libre arbitre. Il s'agit là surement davantage d'une question éthique que d'une question juridique qu'il ne fera ainsi pas partie de nos développements. Enfin, un autre risque

[1] Cette recherche a été menée dans la cadre du projet APPRISE financé par la Fondation universitaire A*MIDEX.
[2] L'expression « gouvernement des juges » est apparue sous la plume d'Edouard Lambert en 1921. Edouard LAMBERT, *Le gouvernement des juges et la lutte contre la législation sociale aux Etats-Unis. L'expérience américaine du contrôle judiciaire de la constitutionnalité des lois*, Paris, Giard, 1921, rééd, Préface F. Moderne, Paris, Dalloz, 2015, 276 p.
[3] Pierre SIMON et Dominique ACKER, « La place de la télémédecine dans l'organisation des soins », Rapport Mission thématique n° 7/PS/DA, Ministère de la Santé et des Sports, Direction de l'Hospitalisation et de l'Organisation des Soins, 2008. Disponible à l'adresse suivante : http://www.sante.gouv.fr/IMG/pdf/Rapport_final_Telemedecine.pdf

engendré par l'avènement de la santé connectée, qui suscite sans conteste la plus grande attention de la communauté juridique, est celui de la protection des données à caractère personnel. La réflexion engagée sur la protection des données à caractère personnel résulte d'un double refus de la part des juristes. Tout d'abord, il s'agit de refuser de considérer que le respect de la vie privée serait une notion dépassée et que le temps serait à l'ouverture de l'accès à tout type de données. Ensuite, il s'agit de refuser de croire en un comportement bienveillant des responsables de traitement de données ou encore des hébergeurs qui les conduirait à protéger d'eux-mêmes nos données à caractère personnel. Ces deux options étant écartées, la protection de ces données doit alors nécessairement être réalisée à travers un renforcement du cadre juridique. Autrement dit, le volume massif des données produites dans le cadre de la santé connectée interroge, dès lors, sur notre capacité à sécuriser suffisamment le traitement des données à caractère personnel pour assurer le respect de la vie privée des individus.

La recherche d'un équilibre entre ouverture de l'accès aux données et protection de la vie privée a particulièrement marqué l'actualité de l'Union européenne en 2016 dans la mesure où après quatre ans de négociations, le Parlement européen a enfin adopté le RGPD général sur la protection des données[4] qui vient remplacer l'ancienne directive 95/46/CE[5]. Le règlement général sur la protection des données (UE) 2016/679 (ci-après « le RGPD ») ne sera applicable au sein des Etats membres qu'à partir de mai 2018, ce qui leur laisse le temps nécessaire pour adapter leurs législations nationales. Dans la présente étude, l'objectif est alors de confronter le RGPD européen aux problématiques posées par la santé connectée en matière de protection des données à caractère personnel. L'échange et le partage de données dans le cadre de la e-santé pose, en effet, plusieurs questions au juriste : quelle est la nature des données générées par la santé connectée ? Ces données doivent-elles être protégées pour assurer le respect de la vie privée ? Qui est responsable de la protection de ces données ? L'identification et la classification des données concernées par la santé connectée sont une entreprise nécessaire pour pouvoir protéger efficacement les individus des dérives auxquelles pourrait conduire le traitement de leurs données. Or, là réside une première difficulté. Les contours même de la définition des données à caractère personnel nécessitent, en effet, d'être redessinés dans un contexte de santé connectée où le croisement des données est facilité. De plus, la santé connectée produit des données dites sensibles telles que les données de santé qu'il faut pouvoir aussi identifier car elles nécessitent une protection juridique renforcée pour parvenir au respect de la vie privée de la personne concernée. En pratique, l'exercice de qualification juridique de la nature de la donnée est donc un préalable incontournable pour définir le régime juridique applicable à ces données et donc les droits et obligations du responsable du traitement et du sous-traitant (I). De la qualification des données dépendra ainsi le régime juridique applicable lors de leur traitement. Le RGPD s'inscrit, de ce point de vue, dans la continuité de la directive 95/46 CE dans la mesure où il en reprend les principes essentiels tels que l'interdiction de traitement des données sensibles mais il va, dans le même temps, plus loin que la directive en renforçant les droits des personnes concernées et les obligations des responsables de traitement et des sous traitants (II).

[4] 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), *Journal officiel de l'Union européenne L119* du 4 mai 2016.

[5] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Journal officiel des Communautés européennes n° L 281* du 23 novembre 1995, pp. 0031-0050.

I – La qualification juridique des données issues de la santé connectée : une navigation à vue

Avant de s'atteler à déterminer les critères d'identification de la nature des données générées dans le cadre de la santé connectée, il est nécessaire d'avoir conscience que la santé connectée ne produit pas uniquement des données à caractère personnel. Lorsque, par exemple, un objet connecté indique l'heure, cette donnée en elle-même ne constitue pas une donnée à caractère personnel. Toute donnée n'est donc *a priori* pas « donnée à caractère personnel ». Reste à savoir comment identifier parmi cet ensemble de données celles qui relèvent du champ d'application du RGPD (1) et celles qui, au sein de ce règlement, bénéficient d'une protection juridique renforcée (2).

1. L'identification des données à caractère personnel issues de la santé connectée

La première distinction à opérer parmi les données, sans qu'elle soit pour autant la plus aisée, consiste à identifier les données à caractère personnel parmi l'ensemble des données existantes dans la mesure où la collecte et le traitement des données à caractère personnel sont soumises à un régime juridique particulier – celui du RGPD – afin d'assurer le respect de la vie privée du titulaire de ces données.

Au sein du Conseil de l'Europe, dès les années 70, le Comité des ministres, conscient des défis que le développement du traitement automatique des données allait poser en matière de protection des droits de l'Homme, adopte successivement deux résolutions relatives à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques l'une dans le secteur privé[6] et l'autre dans le secteur public[7]. Dans ces deux textes, le Conseil de l'Europe pose certains des principes communs en matière de protection des données à caractère personnel, notamment en matière de durée de conservation des données et d'information des personnes concernées mais il faut attendre que soit adoptée la *Convention STE n° 108 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* pour trouver la première définition des données à caractère personnel. L'article 2 de la Convention définit les données à caractère personnel comme « toute information concernant une personne physique identifiée ou identifiable (« personne concernée ») ». Au sein de l'Union européenne, la directive 95/46 reprend mot pour mot la définition de la Convention n°108 en y ajoutant une précision. La catégorie des données à caractère personnel englobe en effet « toute information concernant une personne physique identifiée ou identifiable (personne concernée) » de manière directe ou indirecte[8]. Le RGPD reprend, quant à lui, la définition de la directive 95/46/CE[9]. La modification apportée à la définition de la Convention 108 du Conseil de l'Europe vient élargir le champ d'application des textes de protection des données à caractère personnel. Le fait que même les informations qui concernent une personne physique identifiée ou

[6] Résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé, adoptée par le Comité des Ministres du Conseil de l'Europe le 26 septembre 1973, lors de la 224ème réunion des Délégués des Ministres.

[7] Résolution (74) 29 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public, adoptée par le Comité des Ministres du Conseil de l'Europe le 20 septembre 1974, lors de la 236ème réunion des Délégués des Ministres.

[8] Selon la directive « est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »

[9] 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), *JOUE* L119 du 4 mai 2016.

identifiable de manière indirecte soient considérées comme des données à caractère personnel permet d'inclure dans cette catégorie les données pseudonymisées. Selon le groupe de l'article 29, « la pseudonymisation n'est pas une méthode d'anonymisation. Elle réduit simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée et constitue par conséquent une mesure de sécurité utile »[10]. Dès lors, le croisement de plusieurs données pseudonymisées peut permettre de ré-identifier la personne concernée. Le considérant 26 du RGPD confirme d'ailleurs de manière claire que les données pseudonymisées sont couvertes par le texte dans la mesure où elles peuvent être ré-identifiées par le responsable du traitement mais parfois aussi par des tiers qui peuvent les combiner avec des informations émanant d'autres sources. En revanche, selon le considérant 26 du RGPD, l'anonymisation des données fait sortir ces dernières du champ d'application du RGPD sur la protection des données à caractère personnel car cette technique assure que la personne concernée ne pourra pas être identifiée. Le groupe de l'article 29 a, toutefois, rendu un avis afin de préciser à quels critères la technique d'anonymisation doit répondre pour que les données ainsi traitées échappent au régime juridique de la protection des données personnelles.

Certaines données considérées comme anonymisées pourraient, en effet, entrer dans le champ d'application du RGPD si elles ne répondent pas aux trois critères d'anonymisation dégagés par le groupe de l'article 29 dans son avis 5/2014. Selon le groupe, la fiabilité de chaque technique d'anonymisation doit être évaluée sur la base de trois critères : 1) Est-il toujours possible d'isoler un individu ? 2) Est-il toujours possible de relier entre eux les enregistrements relatifs à un individu ? 3) Peut-on déduire des informations concernant un individu ? Il nous semble ainsi que certaines données même anonymisées ne peuvent remplir ces trois critères dans la mesure où elles possèdent des caractéristiques intrinsèques qui conduisent à l'identification d'une personne précise. Prenons par exemple le cas d'une maladie rare. Si le nombre de patients à l'échelle mondiale est réduit et que la maladie ne touche que les personnes d'un même sexe, le risque d'identification d'un des patients existe malgré la mise en œuvre d'une méthode d'anonymisation des données. Il en serait de même, selon le groupe de l'article 29 avec les profils génétiques donc « d'une manière générale, il ne suffit donc pas de supprimer directement des éléments qui sont, en eux-mêmes, identifiants pour garantir que toute identification de la personne n'est plus possible. Il sera souvent nécessaire de prendre des mesures supplémentaires pour empêcher l'identification »[11]. Ce point est particulièrement important car il nécessite que les responsables de traitement qui désirent rendre anonymes des données s'interrogent sur la meilleure méthode à utiliser en fonction du contexte et des finalités du traitement auxquels sont destinées les données rendues anonymes pour que celles-ci ne demeurent pas des données à caractère personnel. Enfin, il faut tout de même garder à l'esprit que le fait que les données rendues anonymes ne soient pas couvertes par le règlement général sur les données à caractère personnel ne signifie pas pour autant que l'utilisation de ces données n'est soumise à aucune obligation juridique. D'autres textes juridiques peuvent s'appliquer à l'utilisation de ces données comme par exemple, la directive « vie privée et communications électroniques »[12].

[10] Groupe de travail « article 29 » sur la protection des données, Avis 05/14 sur les Techniques d'anonymisation adopté le 10 avril 2014, 0829/14/FR, WP216.
[11] *Ibid*.
[12] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

Dans le cadre de la santé connectée, une partie des données générées sont donc, lors de leur premier traitement[13], des données à caractère personnel. Par la suite, certaines d'entres elles le demeureront et d'autres sortiront du cadre juridique du règlement général sur la protection des données à caractère personnel si elles ont été anonymisées de manière adéquate. Au sein des données qui demeureront des données à caractère personnel, une partie seront, par ailleurs, considérées dans le cadre du RGPD comme dans la directive 95/46/CE comme étant des données sensibles, qui nécessitent une protection juridique renforcée.

B. L'identification des données de santé issues de la santé connectée

La certitude que le traitement de certaines données à caractère personnel était potentiellement plus susceptible de porter atteinte à la vie privée des personnes concernées que le traitement d'autres données est vite apparue. Il paraissait ainsi nécessaire de protéger plus spécifiquement ces données au contenu sensible pour la vie privée. Au niveau européen, la catégorie des données sensible apparaît pour la première fois dans un texte juridique à l'article 6 de la Convention n°108 du Conseil de l'Europe qui les définit comme « [d]es données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle (…) ».

L'article 8 de la directive 95/46/CE, qui deviendra l'article 9 du RGPD, invite lui aussi à identifier cette catégorie particulière de données. Il fait entrer dans la catégorie des données sensibles celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle. La définition de la directive 95/46/CE est plus large que celle de la Convention et le RGPD élargit encore la catégorie dans la mesure où son article 9 y ajoute, à la vue de l'évolution technologique, les données génétiques ainsi que les données biométriques. Aussi bien la Convention n°108 que la directive et le règlement général européen sur la protection des données à caractère personnel considère que les données de santé font partie de la catégorie particulière des données dites sensibles qui nécessitent une protection juridique renforcée. Or, la santé connectée va, par nature, être génératrice de données de santé – un professionnel de santé peut, par exemple, consulter depuis son téléphone des informations médicales sur un patient et de la même manière, un patient peut stocker sur un dispositif mobile des données personnelles de santé et les transmettre à un professionnel de santé par ce biais. Il s'avère ainsi nécessaire d'identifier ces données afin de leur accorder une protection juridique renforcée. En d'autres termes, que recouvre finalement la catégorie juridique des données de santé ?

Si les données de santé sont considérées comme des données personnelles sensibles, aucun texte juridique ne définissait la notion jusqu'à présent. La donnée de santé s'appréhendait alors généralement comme toute donnée susceptible de révéler l'état pathologique ou non de la personne. La Cour de justice de l'Union européenne, dans l'arrêt *Lindquist*[14], avait ajouté qu'eu égard à l'objet de la directive 95/46 – la protection des données à caractère personnel – « l'expression « données relatives à la santé » employée dans ladite disposition appelle une interprétation large de sorte qu'elle comprenne des informations concernant tous les aspects,

[13] La collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction

[14] CJUE, arrêt du 6 novembre 2003, Demande de décision préjudicielle de la Suède dans l'affaire « Procédure pénale contre Bodil Lindqvist », affaire C-101/01, European Court Reports 2003 I-12971, §50-51.

tant physiques que psychiques, de la santé d'une personne ». La définition a finalement été précisée par le RGPD européen de 2016 sur la protection des données personnelles qui retient une interprétation large de la notion conformément à la jurisprudence de la Cour. Selon l'article 4 du règlement, est dorénavant considérée comme donnée de santé « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ». Cette définition fait ainsi entrer dans la catégorie des données dites « sensibles », toutes les données relatives aux interactions entre un patient et le système de santé. Par ailleurs le considérant 35 du RGPD permet d'interpréter plus précisément cette définition dans la mesure où il ajoute que sont considérées comme des données de santé : « 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. Cela comprend :

- des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique ; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ;
- des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques ;
- et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic *in vitro* »[15].

Même si dans le RGPD, pour la première fois, est posée textuellement une définition des données de santé, celle-ci ne dissipe pas tous les doutes qui entourent la notion notamment dans le cadre de la e-santé. En effet, le développement des objets connectés de santé interroge le juriste sur la nature même de ces objets – appartiennent-il ou non à la catégorie juridique des dispositifs médicaux ou sont-ils simplement des objets de bien-être – ce qui, par ricochet renvoie à une question identique quant à la qualification des données générées par ces objets – sont-elles des données de santé et donc des données sensibles ou simplement des données de bien-être ?

Si progressivement, la catégorie des données de santé semble s'étendre, la frontière entre données de santé et données de bien-être semble toujours aussi poreuse. Le RGPD, dans son préambule, précise qu'est considérée comme une donnée de santé, 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 *indépendamment de leurs sources*[16]. Sans être aussi catégorique que Pierre Desmarais qui considère que le Règlement tord ainsi le « cou à la (pseudo) notion de bien être »[17], il faut admettre toutefois que la distinction entre données de bien être et données de santé ne semble, selon le règlement, *a priori* pas reposer sur le critère de l'origine de la donnée. Ainsi, un individu peut collecter lui-même par le biais d'une application des données de santé. Toutefois, cette précision est contenue uniquement dans le considérant du RGPD qui, de surcroit, ne cite, comme exemple de sources par la suite, que des sources médicales. Il

[15] §35 du Règlement (UE) 2016/679 du 27 avril 2016.
[16] Nous soulignons.
[17] http://www.desmarais-avocats.fr/blog/283/

semble, dès lors, qu'il nous faudra attendre une fois de plus que la Cour de justice de l'Union européenne, ou peut-être en amont les Cours nationales, pour que soit clairement dessiner la frontière entre ces deux notions. Reste, de plus, malgré tout une autre question en suspend : plusieurs données de bien-être, c'est à dire des données qui ne révèlent pas, prises isolément, des informations sur l'état physique ou mentale d'une personne, pourraient-elles constituer une donnée de santé lorsqu'elles sont regroupées ? Le RGPD ne nous semble pas, dès lors, de ce point de vue répondre à l'ensemble des questions de qualification juridique que soulève la santé connectée. Toutefois, une fois le défi de la qualification relevé, le régime juridique applicable au traitement de ces données paraît, quant à lui, davantage défini.

II – La protection des données à caractère personnel issus de la santé connectée : un horizon défini.

La phase préalable de qualification des données issues de la santé connectée ne sera pas bouleversée par la mise en œuvre en mai 2018 du RGPD européen dans la mesure où les fondements de la directive de 95/46/CE demeurent ainsi que ses faiblesses. En revanche, le RGPD est plus ambitieux – et dans le même temps, peut-être moins limpide – en ce qui concerne le cadre juridique du traitement des données à caractère personnel. Il vient sans conteste renforcer les obligations des responsables de traitement ainsi que des sous-traitant aussi bien au stade de l'examen de la licéité du traitement (1) que de celui de son exécution (2).

1. Les conditions de licéité du traitement des données à caractère personnel

L'opération de qualification juridique des données collectées dans le cadre de la santé connectée prend au stade de l'examen de la licéité du traitement de ces données toute son importance. En effet, alors que le traitement des données à caractère personnel est licite s'il répond à l'une des conditions de licéité énumérées à l'article 6 du RGPD, le traitement des données dites sensibles – et donc des données de santé – est dans son principe interdit. L'article 8 de la directive 95/46/CE consacré aux données à caractère personnel dites sensibles posait déjà, en son paragraphe 1, le principe de l'interdiction du traitement de ce type de données. Ces données, de par leur particularité, nécessitent une protection juridique renforcée par rapport au régime juridique général de protection des données à caractère personnel. Le RGPD reprend la même philosophie en son article 9 que celle de l'article 8 en affirmant de nouveau le principe de l'interdiction de traitement des données sensibles. Toutefois, ce principe d'interdiction de traitement des données sensibles n'est pas absolu dans la mesure où il est tempéré par une liste d'exceptions. Le paragraphe 2 de l'article 8 de la directive 95/46/CE prévoyait cinq conditions de licéité du traitement de ce type de données, pour lesquelles le critère de nécessité présidait largement à leur mise en œuvre[18]. L'article 9

[18] Hormis le consentement de la personne concernée, les autres conditions générales de licéité du traitement des données sensibles requièrent que ce traitement soit nécessaire. Ainsi, le traitement des données sensibles peut être licite s'il est « nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates », ou encore s'il est « nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ». De la même manière, le traitement des données sensibles est considéré comme licite s'il est effectué par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, dans le cadre de leurs activités légitimes et avec des garanties appropriées. En d'autres termes, si ce traitement est nécessaire pour la réalisation de leurs activités. Le critère de nécessité vient ainsi limiter le champ d'application de ces exceptions à l'interdiction générale de traitement des données sensibles.

du RGPD élargit la liste de ces exceptions tout en maintenant le critère de nécessité[19]. A quelles conditions, dès lors, un traitement de données à caractère personnel est-il licite ?

Quelles que soient les données à caractère personnel – sensibles ou non – le consentement de la personne concernée, même s'il n'est qu'une des conditions de licéité du traitement des données à caractère personnel, occupe une place particulière dans la mesure où il marque le lien entre la personne concernée et ses données. Le consentement est défini à l'article 4 du RGPD comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Plusieurs remarques peuvent alors être faites.

Tout d'abord, il faut, dès à présent, noter qu'en ce qui concerne les données sensibles, il est précisé dans l'article 9 du RGPD que le consentement de la personne concernée doit, de surcroit, être explicite. Cela signifie-t-il alors qu'en ce qui concerne les autres données à caractère personnel, le consentement de la personne concerné peut-être implicite ? Le Règlement ne semble pas aller dans ce sens pour deux raisons. En premier lieu, le considérant 32 du RGPD précise que « le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale ». La possibilité d'un consentement implicite semble alors écartée d'autant plus que le caractère spécifique du consentement impose que la personne concernée ait consenti à chaque finalité du traitement de ses données, ce qui paraît difficilement réalisable par le biais d'un consentement implicite. En second lieu, l'article 7§1 du RGPD fait peser la charge de la preuve du recueillement d'un consentement libre, informé et spécifique sur le responsable du traitement, comme le préconisait le groupe de travail de « l'article 29 ». Or, la responsabilisation du responsable du traitement devrait conduire ce dernier à recueillir systématiquement un consentement explicite afin de ménager la preuve. Si en théorie, la question du consentement semble claire, en pratique, les difficultés sont multiples d'autant plus dans un environnement dématérialisé où un simple clic peut valoir acceptation. Au fur et à mesure du temps, il semble qu'un guide des bonnes pratiques se dessine notamment sous l'impulsion des autorités de contrôle nationales. La pratique des paramètres par défaut qui nécessite que l'utilisateur décoche une case ou change les paramètres pour que son consentement ne soit pas enregistré n'est, par exemple, pas assimilée à un consentement explicite de la personne concernée. Toutefois, la possibilité pour un utilisateur de donner son consentement en différents lieux – en présentiel dans un magasin, au téléphone ou encore sur internet – et sur différents supports – papier ou numérique – pour une même application complexifie la tâche des responsables de traitement.

Ensuite, il convient bien évidemment de s'interroger sur la place du consentement en pratique. Finalement, le consentement est-il souvent le fondement de la licéité du traitement des données à caractère personnel ? Comme indiqué dès le commencement de ce paragraphe, le consentement n'est qu'une des conditions de licéité du traitement des données à caractère personnel. En matière de santé, le traitement des données à caractère personnel est notamment

[19] Le règlement général de 2016 ajoute que le traitement des données sensibles sera licite s'il est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice et chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ; s'il est nécessaire à des fins d'archivage dans l'intérêt public ou à des fins historiques, statistiques ou scientifiques ; ou encore s'il est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontières graves pesant sur la santé.

licite lorsqu'il est « nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement »[20] ; ou « 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 »[21] ; ou encore « s'il est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontières graves pesant sur la santé (…) »[22]. Dans le cadre de la santé, le consentement de la personne concernée ne sera donc que très rarement le seul fondement de la licéité du traitement de ses données notamment de santé. En dehors du cadre du parcours de soin, en revanche, la licéité du traitement des données sensibles reposera souvent sur le consentement ce qui ne sera pas nécessairement le cas pour les autres données à caractère personnel. En effet, dans le contexte notamment des objets connectés de bien être, le consentement de la personne concerné risque d'être écarté au profit d'une autre condition de licéité du traitement des données à caractère personnel non sensibles. L'article 6§1 f) du RGPD indique que le traitement des données à caractère personnel est licite lorsqu'il est « nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant ». Les responsables de traitement risquent ainsi de s'engouffrer dans cette faille sans avoir pleinement conscience qu'ils auront à justifier de la raison pour laquelle leurs intérêts légitimes priment sur les intérêts et libertés de la personne concernée. Dès lors, il semble que si la tentation peut être grande des responsables de traitement de ne pas fonder le traitement des données à caractère personnel sur le consentement de la personne concernée, dans une optique d'éventuels différends avec les utilisateurs ces derniers ont davantage intérêt à ménager la preuve par ce biais.

Dans le cadre de la santé connectée, le traitement des données à caractère personnel est un traitement licite dans la mesure où il est nécessaire à l'amélioration des soins du patient ou encore à la prévention médicale. Toutefois, le traitement de ces données en dehors du cadre du parcours de soin semble, quant à lui, plus délicat à justifier et nécessitera que les responsables de traitement et les sous-traitant soient très attentifs au respect de l'équilibre entre traitement des données et protection de la vie privée et cela…dès la conception des objets connectés de santé ou de bien-être.

2. La protection de la vie privée lors du traitement des données à caractère personnel

Le RGPD de 2016 a voulu renforcer les droits de la personne concernée en lui donnant les outils pour une meilleure maîtrise de ses données et en renforçant les obligations des responsables de traitement des données et des sous traitants. Ainsi, la personne concernée dispose d'un droit d'accès à ses données (article 15) ; d'un droit de rectification de ses données (article 16) ; d'un droit à l'effacement de ses données (article 16) ; d'un droit à la limitation du traitement de ses données (article 17) ; d'un droit à la portabilité de ses données (article 20) et enfin un droit d'opposition (article 21). Bien évidemment aucun de ses droits

[20] Article 6§1 d) et Article 9§2 c) du RGPD.
[21] Article 9§2 h) du RGPD.
[22] Article 9§2 i) du RGPD.

n'est absolu, l'exercice de chacun est strictement encadré dans la disposition du règlement le concernant. Il convient, toutefois, de s'attarder sur deux de ces droits. En ce qui concerne le droit à l'effacement de ses données à caractère personnel, la doctrine juridique a été prolifique sur la question suite à l'arrêt *Google Spain*[23] rendu par la Cour de justice de l'Union européenne[24]. Dans cette affaire, la Cour a certes reconnu un « droit à l'oubli numérique » mais celui-ci non seulement est très encadré juridiquement dans la mesure où le règlement général fait une liste des restrictions à ce droit mais il l'est aussi *de facto* dans la mesure où les moteurs de recherche ne peuvent que déréférencer les données et non les effacer une fois que celles-ci ont été versées dans la toile. Par ailleurs, le règlement général de 2016 offre aux personnes concernées, en son article 20, un droit de portabilité de leurs données ce qui signifie que ces dernières « ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle ». Toutefois, ce droit ne s'applique que lorsque le traitement des données repose sur le consentement de la personne concernée et que celui-ci est automatisé. Si le renforcement des droits de la personne concernée, dans le cadre du RGPD, ne doit pas être négligé, il reste que ces droits avaient pour la plupart étaient largement entérinés par la jurisprudence. Le règlement est davantage ambitieux en ce qui concerne les obligations des responsables de traitement et de leurs sous-traitants en matière de sécurité des données.

Le RGPD consacre son chapitre IV aux obligations qui incombent au responsable du traitement et au sous-traitant. L'article 25 de ce chapitre est particulièrement pertinent dans un contexte de développement prolifique des objets connectés de santé dans la mesure où il affirme que le responsable de traitement doit avoir à la fois une approche de *privacy by design*[25] – protection de la vie privée dès la conception de l'objet ou de l'applictaion – et une approche de *privacy by default* « pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées »[26]. Cette « approche de précaution numérique » fait ainsi peser sur le responsable du traitement une obligation de sécurité des données. Toutefois, il est possible de se demander si le risque zéro d'atteinte à la vie privée existe, si ce risque est mesurable par les spécialistes de l'informatique et donc quelle est la nature de l'obligation qui pèse sur le responsable de traitement ? La lecture des articles 25 et 32 du RGPD indique que le législateur a voulu préconiser une approche par le risque pour conduire les responsables de traitement à prendre toutes les mesures techniques et opérationnelles nécessaires pour assurer la sécurité des données. L'obligation est alors une obligation de moyen dont la mise en œuvre sera accompagnée par des codes de bonnes conduite et qui sera valorisée par des mécanismes de

[23] Cour de justice de l'Union européenne, grande chambre, *Google Spain v Costeja González*, arrêt du 13 mai 2014, affaire C-131/12.

[24] Voir notamment : D. DECHENAUD (Dir.), Le droit à l'oubli numérique : Données nominatives – Approche comparée, Bruxelles, Larcier, 2015, 452 p. ; M. BOIZARD, « La tentation de nouveaux droits fondamentaux face à internet : vers une souveraineté individuelle ? Illustration à travers le droit à l'oubli numérique », *in* A. BLANDIN-OBERNESSER (Dir.), *Droits et souveraineté numérique en Europe*, Bruxelles, Bruylant, coll. Rencontres européennes, 2016, pp. 31-55. ; C. CASTETS-RENARD, « Google et l'obligation de déréférencer les liens vers les données personnelles ou comment se faire oublier du monde numérique », *RLDI*, dossier spécial, n°106, 2014, pp. 68-75. ; V-L. BENABOU et J. ROCHFELD, « Les moteurs de recherche, maître ou esclaves du droit à l'oubli numérique ? Acte 2 : Le droit à l'oubli numérique, l'éléphant et la vie privée », *Dalloz* 2014, pp. 1481-1485. ; M. CLEMENT-FONTAINE et R. AMARO, « Séance 9 : Le droit à l'oubli numérique », *in* N. MARTIAL-BRAZ (Dir.), La proposition de règlement européen relatif aux données à caractère personnel : propositions du réseau trans Europe experts, Paris, Société de législation comparée, coll. Trans Europe Experts, 2014, pp. 422-453.

[25] La notion de privacy by design a été développée par Ann Cavoukian, préposée à la protection des données de l'Etat d'Ontario au Canada : http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf

[26] Article 25 du RGPD.

certification. Reste que les responsables de traitement ne peuvent pas prévoir toutes les failles de sécurité. Or, « [e]n cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente »[27], ce qui peut alors déclencher une enquête de cette dernière et le prononcé d'une sanction à l'égard du responsable de traitement[28]. Les responsables de traitement ont donc une responsabilité renforcée au sein du règlement qui devrait les obliger avant de mettre sur le marché un objet connecté, notamment de santé, à réfléchir aux atteintes éventuelles à la vie privée qui pourraient être engendrée par le traitement de données à caractère personnel. Cette prise de conscience des responsables de traitement de données sera d'autant plus nécessaire que les sanctions administratives prévues dans le RGPD ne sont pas simplement symboliques, elles sont au contraire dissuasives puisqu'elles peuvent s'élever jusqu'à 4 % du chiffre d'affaires annuel mondial total du responsable du traitement[29].

*****

Conclure sur un tel sujet paraît être une tâche impossible tellement tout semble, dans ce domaine, en être au stade du commencement. En matière de protection des données à caractère personnel, la santé connectée cristallise l'ensemble des enjeux de la matière : problème de qualification juridique, de fondement de la licéité des traitements ou encore de responsabilité des opérateurs économiques. Le cadre juridique européen, tel qu'adopté au printemps 2016, apporte un certain nombre de réponses aux défis posés par les technologies de l'information et de la communication notamment dans le domaine de la santé dans la mesure où il oblige les responsables de traitement et leur sous-traitant à prendre conscience des enjeux des nouvelles technologies pour la protection de la vie privée. Dans le même temps, le RGPD soulève de nouvelles interrogations quant à la mise en œuvre de certaines dispositions. Ainsi, seule la pratique de ce texte permettra d'en faire surgir les forces et les faiblesses qui ne seront d'ailleurs peut-être pas celles que l'analyste aura identifié en amont.

[27] Article 33 du RGPD.
[28] Voir notamment sur cette question : Nathalie MELINOS, « Notification des violations de données à la CNIL : tendre le bâton pour se faire battre ? Observations sous Conseil d'Etat, 18 décembre 2015, n°385019, Société Orange », *Dalloz IP/IT*, 2016, p. 144.
[29] Article 83 du RGPD.