La protection des données personnelles en matière de santé. E-santé, droit de l'Union Européenne et protection de la vie privée des personnes : vers l'émergence d'un technodroit spécifique au travers de la proposition de règlement général sur la protection des données personnelles ?

Gauthier Chassang

E-santé, droit de l'Union Européenne et protection de la vie privée des personnes : vers l'émergence d'un « technodroit » spécifique au travers de la proposition de Règlement général sur la protection des données personnelles ?

Gauthier Chassang[1,2]

Introduction

Le terme de « e-santé », ou « cyber-santé », est un néologisme permettant de définir l'utilisation des technologies de l'information et de la communication (TIC) à des fins de santé[3]. Représentant aujourd'hui un domaine d'activité économique prometteur[4] en plein essor[5], la e-santé recouvre l'ensemble des activités utilisant des TIC aux fins de prestations de santé, dans un but de prévention, de diagnostic, de traitement des maladies, de surveillance et de gestion de la santé des personnes. Les TIC peuvent être intégrées à un produit de santé ou faire partie intégrante d'un procédé de prestation de santé.

La e-santé inclut l'usage d'une variété de TIC, de dispositifs techniques et de logiciels qui produisent, stockent, fournissent un accès, copient ou véhiculent des données de santé. Ces TIC faisant généralement usage de l'internet pour traiter les données comprennent des programmes intégrés à des objets commercialisés auprès du grand public et communément utilisées de nos jours mais également des dispositifs médicaux[6] et accessoires[7] dont l'usage est très spécialisé et a priori réservé à un usage professionnel. Ainsi, les téléphones portables, les montres[8], les vêtements dits intelligents qui sont connectés et munis de capteurs[9], tout comme les sites web d'information de santé parmi lesquels figurent les sites de vente en ligne de produits de santé (de médicaments ou de dispositifs médicaux

[1] Inserm, UMR 1027, Equipe 4, Toulouse, F-31062, France.
[2] Université de Toulouse 3, Paul Sabatier, UMR 1027, Toulouse, F-31062, France.
[3] OMS, Connecting for Health : Global Vision, Local Insight. Report for the World Summit on the Information Society, 2002, disponible en ligne en anglais : http://www.who.int/ehealth/en/# accédé le 28 Juillet 2014.
[4] Ex: Research2Guidance Report, Mobile Health market Report 2013-2017 – The commercialisation of mHealth applications (Vol.3), 4 Mars 2013. Cette étude prospective évalue à 500 millions le nombre d'utilisateurs de Smartphones qui utiliseront régulièrement des applications de santé mobile en 2015. Ce nombre devrait tripler et atteindre 1,5 milliard d'utilisateurs à l'horizon 2018.
[5] Ex : « Près de 100 000 #applis de santé mobile sont d'ores et déjà disponibles sur de multiples plateformes telles qu'iTunes, Google play, Windows Marketplace et Backberry World. Les 20 applis de sport, de remise en forme et de santé les plus populaires comptabilisent déjà 231 millions de téléchargements dans le monde entier. » Commission Européenne, Communiqué de presse, La santé en poche : libérer le potentiel de la santé mobile, IP/14/394, Bruxelles, 10 Avril 2014.
[6] Au sens de la Directive 93/42/CEE du Conseil relative aux dispositifs médicaux du 14 Juin 1993, JOCE n° L 169 du 12/07/ç » p. 0001-0043, Article 1 al.2 a), est qualifié de dispositif médical « tout instrument, appareil, équipement, matière ou autre article, utilisé seul ou en association, y compris le logiciel nécessaire pour le bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins de diagnostic, de prévention, de contrôle, de traitement ou d'atténuation d'une maladie, de diagnostic, de contrôle, de traitement, d'atténuation ou de compensation d'une blessure ou d'un handicap ; d'étude ou de remplacement ou modification de l'anatomie ou d'un processus physiologique; de maîtrise de la conception; et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens ».
[7] Au sens de la Directive 93/42/CE, op.cit. Article 1 al.2 b), est qualifié d'accessoire « tout article qui, bien que n'étant pas un dispositif, est destiné spécifiquement par son fabricant à être utilisé avec un dispositif pour permettre l'utilisation dudit dispositif conformément aux intentions du fabricant de ce dispositif ».
[8] Ex: Oxitone, montre conçue comme un dispositif préventif de surveillance et d'alerte des troubles cardiaques, http://oxitone.com/ accédé le 28 Juillet 2014.
[9] Ex : Projet INDIEGOGO, Hexoskin, Wearable Body Metrics, voir https://www.indiegogo.com/projects/hexoskin-the-first-wearable-movement-respiration-and-heart-activity-tracker accédé le 28 Juillet 2014.

par exemple), les sites de téléconsultation[10], les réseaux sociaux de santé et les réseaux utilisés par les professionnels de santé pour gérer les données des patients sont considérés comme des outils de e-santé, au même titre que des technologies de pointes comme les implants actifs ou encore les technologies de tests génétiques ou de séquençage du génome humain, chacun de ces outils devant se conformer à des exigences règlementaires particulières liées à leur qualification juridique, à leurs propriétés et leur destination, la plupart devant répondre aux exigences du droit de l'UE concernant l'obtention d'un marquage CE en tant que dispositifs médicaux.

Par delà sa composante technologique et logicielle, la e-santé recouvre également une variété de pratiques. Cela comprend par exemple le partage de données de santé entre les professionnels de santé, avec le patient, ou entre patients, l'utilisation des dossiers médicaux électroniques, la consultation de bases de données médicales, les prestations de services de télémédecine[11], l'utilisation de dispositifs d'auto-surveillance portables des patients (grâce aux nombreuses applications « m-health » ou dispositifs de santé mobiles[12]), la chirurgie robotisée à distance[13] ou encore la recherche fondamentale sur l'humain physiologique virtuel[14]. Bien que non exhaustif, ce large éventail d'activités considérées comme des pratiques de e-santé illustre néanmoins l'importance croissante de l'utilisation des TIC à des fins de santé, dans la pratique médicale ou dans le cadre de la recherche scientifique, à des fins médico-administratives mais également au-delà, à des fins personnelles d'auto-gestion de la part du patient utilisateurs d'outils de e-santé que ces derniers soient proposés par les professionnels de santé dans le contexte de la prise en charge du patient ou commercialisés comme biens de consommation dans les circuits classiques de distribution (ex : vente en ligne d'applications pour téléphones portables, vente de montres, brassards et accessoires électroniques de fitness dans les magasins de sports etc.).

Les nombreuses innovations de e-santé font émerger de nouveaux modèles organisationnels préfigurant une généralisation programmée de la e-santé dans et en dehors du système de santé traditionnel. Ces évolutions aujourd'hui en cours dans plusieurs pays, y compris dans l'Union Européenne (UE), comme en France[15], ont néanmoins un impact éthique, juridique et social qui ne doit pas être négligé. La plupart de ces TIC s'inscrivent dans une dynamique de réseaux numériques ouverts ou privatifs permettant une circulation quasi-instantanée d'une quantité toujours plus importante d'informations, y compris à l'international, ce qui engendre des questions relatives à la

[10] Ex: e-docteur, site permettant aux usagers de décrire leurs symptômes et d'en obtenir une analyse en ligne amenant à fournir des conseils personnalisés à la personne, sur la signification des symptômes ou la nécessité de consulter un professionnel de santé. Un rapport imprimable peut être obtenus et transmis au médecin qui prendra en charge la personne. Voir http://www.e-sante.fr/e-docteur accédé le 28 Juillet 2014.

[11] Comme la consultation médicale à distance (télé-consultation et le télé-diagnostic); la surveillance à distance d'un patient (télé-surveillance); la fourniture d'un avis donné à distance par un expert ou un médecin (télé-expertise); la formation à distance (téléformation); la réalisation d'une opération chirurgicale à distance (télé-chirurgie).

[12] La santé mobile (m-health) recouvre «les pratiques médicales et de santé publique reposant sur des dispositifs mobiles tels que téléphones portables, systèmes de surveillance des patients, assistants numériques personnels et autres appareils sans fil», OMS, mHealth – New horizons for health through mobile technologies, Global Observatory for eHealth series – Volume 3", page 6.

[13] Dont l'un des pionniers est le professeur Jacques Marescaux qui à réalisé, en 2001, la première opération chirurgicale à distance d'une patiente hospitalisée à Strasbourg, depuis New-York. Voir à ce sujet, Colette Mainguy, Chirurgie à distance : les exploits d'un médecin français, Le Nouvel Observateur, Dossier, publié le 1er Décembre 2013.

[14] Outils de la nouvelle médecine de précision permettant de modéliser l'ensemble du corps humain en 3D pour tester entre-autres les réactions physiologiques des traitements médicamenteux avant leur administration ou au cours de leur développement en recherche. Voir à ce sujet,

[15] Avec par exemple le Programme de Médicalisation des Systèmes d'Information (PMSI) permettant d'améliorer la saisi et la gestion des données patients dans le système de santé. Voir http://www.atih.sante.fr/mco/presentation

protection des données personnelles et au respect de la vie privée. Le droit doit se saisir des questions nouvelles liés à ces évolutions des systèmes de santé lesquels se transforment rapidement en « systèmes 2.0 » se voulant plus performants et complètement numérisés au bénéfice du patient et de la société.

Or l'encadrement des technologies et des prestations de e-santé en Europe est à ce jour complexe et difficile à identifier, appelant l'application de différents corpus de règles n'étant pas spécifique à la e-santé et impliquant des réflexions d'ordre éthiques allant au-delà des normes juridiques prévues par le droit. Cependant les activités de e-santé doivent respecter les textes applicables ayant une force juridique obligatoire dans les domaines de la protection des droits fondamentaux, du droit commercial, du droit de la consommation et du droit des contrats (dans le e-commerce notamment), du droit de la concurrence, du droit des assurances et, pour certains Etats de l'UE, du droit international médical, tel qu'il est issu de la Convention d'Oviedo du Conseil de l'Europe relative aux applications de la biomédecine et aux droits de l'homme[16] et de ses protocoles additionnels énoncant « les principes fondamentaux applicables à la médecine quotidienne ainsi que ceux applicables aux nouvelles technologies dans le domaine de la biologie humaine et de la médecine[17] ». Pour les Etats n'ayant pas ratifiés ces textes spécifiques du Conseil de l'Europe qui réaffirment l'application des règles relatives à la protection de la vie privée, à la confidentialité des données personnelles dans les activité de santé et à l'autodétermination des patients, il s'agira de considérer les principes éthiques affirmées au travers de la Déclaration d'Helsinki[18] révisée en 2013 par l'Association Médicale Mondiale et les autres règles de bonnes pratiques pertinentes applicable à leur activité de e-santé. Le droit de l'UE, bien que limité par une compétence d'appui des politiques et droits nationaux primant en matière de protection de la santé en vertu des Traités de droit primaire (Traité sur le Fonctionnement de l'Union Européenne et Traité sur l'Union Européenne), à néanmoins un rôle déterminent à jouer pour règlementer plus avant la e-santé, depuis la conception des technologies à leur mise sur le marché, dans leur libre circulation et pour leur bon usage. L'UE à d'ailleurs adoptée une stratégie pour la e-santé[19] et un livre vert sur la santé mobile[20]. Le droit de l'UE doit notamment préserver la qualité et la sécurité de ces dispositifs tout en préservant les libertés et les droits fondamentaux des citoyens dans le respect de la Charte des Droits Fondamentaux de l'UE[21], qu'il s'agisse du droit à une protection sociale (Article 34 de la Charte) ou du droit au respect de la vie privée et familiale (Article 7 de la Charte) et à la protection des données personnelles (Article 8 de la Charte) dans les prestations de e-santé nécessitant un flux transfrontaliers de données personnelles. C'est par exemple dans cette optique que dès 2011 l'Union a adopté une Directive relative aux soins

[16] Conseil de l'Europe, Convention pour la protection des Droits de l'Homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine: Convention sur les Droits de l'Homme et la biomédecine, STCE 164, Oviedo, 4 Avril 1997. La Convention et ses protocoles additionnels sont consultables en ligne http://www.coe.int/t/dg3/healthbioethic/Activities/01_Oviedo%20Convention/default_fr.asp

[17] Site officiel du Conseil de l'Europe : http://www.coe.int/t/dg3/healthbioethic/Activities/01_Oviedo%20Convention/default_fr.asp

[18] Association Médicale Mondiale (AMM), Declaration d'Helsinki de L'AMM - Principes éthiques applicables à la recherche médicale impliquant des êtres humains, adoptée par la 64e Assemblée générale de l'AMM, Fortaleza, Brésil, Octobre 2013. Disponible à l'adresse suivante : http://www.wma.net/fr/30publications/10policies/b3/index.html

[19] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century, COM(2012) 736 final. Disponible en anglais à l'adresse suivante : http://ec.europa.eu/health/ehealth/docs/com_2012_736_en.pdf

[20] Commission Européenne, Livre Vert sur la Santé Mobile, COM(2014) 219 final, Bruxelles le 10 Avril 2014. Disponible à l'adresse suivante : https://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth

[21] UE, Charte des Droits fondamentaux de l'Union Européenne, modifiée, (2010/C 83/02), JOUE C 83/389 du 30 Mars 2010. Disponible à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:FR:PDF

transfrontaliers[22] et à l'échange des données personnelles nécessaires à l'accès aux prestations de santé réalisées pour un ressortissant d'un Etat membre dans un autre Etats membre de l'UE et à leurs remboursements par les organismes d'assurance compétents. En parallèle l'Union est en pleine réforme de son cadre juridique relatif à la protection des données personnelles principalement régit à ce jour par la Directive 95/46/CE[23] qui fixe un cadre général harmonisé pour les opérations de traitement de données personnelles, en cours de révision, à laquelle s'ajoute les Directives et actes composant le « package télécom » dont fait partie la Directive 2002/58/CE relatives à la protection de la vie privée dans les communications électroniques[24]. Cette réforme vise à moderniser les règles existantes et à renforcer le droit de l'UE en matière de protection de la vie privée en tenant compte des évolutions rapides des TIC et appliquant les dispositions de l'Article 16 du TFUE. En Janvier 2012, la Commission proposait au Parlement et au Conseil d'adopter un Règlement Général de l'UE sur la Protection des Données personnelles[25] (RGPD) qui remplacerait l'actuelle Directive 95/46/CE et uniformiserait les règles au sein des 28 Etats Membres en apportant un certain nombre de nouveautés et de modifications du système existant. Cette réforme, très débattue, présente un intérêt majeur pour tous les secteurs d'activités ayant recours au traitement[26] de données à caractère personnel, quelque soit la technologie utilisée pour ce faire, y compris dans le domaine de la e-santé. Quelles sont les principales innovations que l'on peut prévoir pour le futur cadre applicable à la e-santé pour ce qui est de la protection de la vie privée des personnes ? En quoi la nouvelle approche de la proposition de RGPD préfigure-t-elle l'émergence d'un technodroit spécifique pour les utilisateurs des technologies et services de e-santé ? Dans cet article, nous analyserons tout d'abord les potentiels de la e-santé qui expliquent à la fois les développements rapides du secteur que nous constatons aujourd'hui et la nécessité d'établir un cadre juridique européen adapté en ce qui concerne la protection des données personnelles traitées. Nous nous concentrerons sur les dernières avancées dans la réforme encore inachevée du droit de l'UE en la matière telles qu'issues du texte du RGPD adopté en première lecture au Parlement Européen le 12 Mars 2014[27] (1). Nous nous intéresserons ensuite plus spécifiquement à

[22] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers, JOUE L 88, 4 Avril 2011, p. 45–65.

[23] 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, JOCE n° L 281 du 23 Novembre 1995 p. 0031 – 0050.

[24] 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 (directive vie privée et communications électroniques), JOCE L 201 du 31 Juillet 2002, p. 37–47.

[25] Proposition de Règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données), COM(2012) 11 final, 2012/0011 (COD), Bruxelles, le 25 Janvier 2012, ci-dessous référencé par l'abréviation « RGPD », disponible à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF

[26] La notion de « traitement de données » fait référence à toute opération (ou ensemble d'opérations) effectuées ou non à l'aide de procédés automatisés et appliqué(es) à des données à caractère personnel. Cela recouvre la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données personnelles. A l'exclusion des activités exclusivement domestiques la qualification d'une opération de traitement de données personnelles déclenche l'application de la règlementation relative au respect de la vie privée. Cette notion ne change pas dans le cadre de la proposition de RGPD.

[27] Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de Règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Procédure législative ordinaire: première lecture), 12 Mars 2014, Strasbourg. Disponible à l'adresse suivante : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//FR

la nouvelle approche de Privacy by Design (PbD) qui émerge de façon explicite des dernières versions disponibles de la proposition de RGPD. Cette approche relativement nouvelle combinée aux autres innovations juridiques portées par la proposition de RGPD caractérise à la fois l'ambition du droit de l'UE visant à offrir une protection adéquate des personnes au travers d'un cadre juridique unique au niveau mondial et la montée en puissance d'un droit de plus en plus technologique, ou « technodroit », qui encadre un environnement numérique évolutif, internationalisé et immatériel, en s'appuyant sur les nouvelles technologies pour protéger les données personnelles et assurer l'application effective des règles protectrices de la vie privée des personnes concernées qu'il tend par ailleurs à renforcer.

1- D'une analyse des potentiels de la e-santé à la mise en place d'un cadre juridique adapté et protecteur de la vie privée au niveau de l'UE

Pour comprendre les enjeux de la e-santé vis-à-vis de la protection de la vie privée des personnes concernées[28] il est opportun d'en comprendre les avantages attendus et d'en identifier risques connexes (A) avant d'aborder les règles protectrices en cours d'élaboration dans le cadre de la proposition de RGPD qui se veulent adaptées à un tel environnement et auront un impact certain sur les pratiques liées à l'utilisation des technologies de e-santé (B).

A- Les bénéfices et les risques des technologies de e-santé

Des bénéfices importants résultant de l'utilisation des technologies de e-santé sont attendus pour le système de santé. Il s'agit tout d'abord d'améliorer de la coordination des soins par la mise en place de systèmes informatisés interopérables qui sont intégrés au système de santé, dans les hôpitaux, chez les médecins, pharmaciens et spécialistes. Ces systèmes sont souvent couteux et leur mise en place en routine dans la pratique est longue et nécessite une éducation particulière des professionnels de santé afin de pouvoir réellement bénéficier de ses avantages en termes de prise en charge et de suivi des patients. C'est par exemple la mise en place du Dossier Patient Informatisé (DPI) ou encore du Dossier Médical Personnalisé (DMP) grâce auquel le patient peut aisément accéder à ses données personnelles de santé, les consulter et éventuellement les enrichir. C'est également la mise en place de réseaux de communication spécialisé avec l'exemple du PMSI que nous avons précédemment cité ou de dispositifs permettant de faciliter le suivi et le remboursement des consultations et autres prestations de santé effectuées par le patient dans un autre Etats membre de l'Union. La e-santé devrait également améliorer l'accès aux services de santé notamment pour les personnes à mobilités réduites, astreinte à domicile ou résident dans des zones géographiques difficile d'accès ou loin des infrastructures médicales dont elles ont besoins, dans ce que l'on a désormais malheureusement coutume d'appeler les « déserts médicaux ». Les actes de télémédecine présentent également des avantages pour la réalisation d'actes très spécialisés pour lesquels les compétences nécessaires ne sont pas disponible sur le lieu où se trouve le patient pour autant que celui-ci soit équipé de la technologie adéquate à la réalisation de l'acte ou que le patient puisse y accéder par d'autres moyens (ex : transfert dans un autre centre). La e-santé doit également améliorer substantiellement la qualité des prestations en fournissant des outils technologiques performants d'assistance aux professionnels. Les activités de préventions mais aussi de diagnostic et de traitement des patients pourraient alors bénéficier d'outils pratiques connectés facilitant l'accès à des bases de données médicales ou scientifiques de références et aidant à l'interprétation des symptômes en analysant directement les données, ou encore permettant la mise à jour des données d'un patient de manière efficace. Les avantages de la e-santé se décline également du point de vue du patient qui se voit offrir la possibilité de gérer de manière autonome et pro-active sa santé, grâce à l'utilisation du DMP ou des nombreux autres logiciels d'assistance

[28] La personne concernée est la personne à laquelle se rapportent les données qui font l'objet du traitement.

permettant par exemple une auto-surveillance, un auto-diagnostic, une auto-médication adaptée. Les technologies de e-santé permettent par exemple aux patients mais aussi plus largement aux citoyens de surveiller leurs rythme cardiaque ou encore de calculer leur taux de glucose sans avoir à réaliser de prise de sang grâce à des lentilles intelligentes[29], la surveillance de la prise d'un traitement, comme avec des piluliers électroniques de nouvelles génération capables d'alerter la patient par sms en cas d'oubli ou de retard important dans la prise du traitement. Ces dispositifs sont en grande majorité connectés à internet via un ordinateur ou un téléphone portable et permettent d'exporter les données générées ou de les échanger avec d'autres personnes mais ils peuvent également être des dispositifs autonomes et ne pas êtres connectés au web. Ceux bénéficiant d'une connexion peuvent également être interconnectés permettant à leurs utilisateurs d'échanger leurs données, de les comparer et de les discuter. Certains peuvent fonctionner comme des lanceurs d'alertes à destination d'un médecin afin de permettre des interventions rapides, le temps étant souvent un facteur décisif pour certaines pathologies, comme dans le cas des accidents vasculaires cérébraux ou des arrêts cardiaques. Sans remplacer l'acte professionnel les dispositifs de e-health peuvent le compléter. De l'accessoire de convenance au réel dispositif médical, les innovations potentielles dans le domaine de la e-santé sont quasi-infinies. Et c'est là le dernier avantage de la e-santé qui, par le biais de la convergence des technologies de santé et des TIC, constitue un véritable foyer d'innovation et de développement économique. Le développement du marché lié à la e-santé devant stimuler la croissance et l'emploi en favorisant la prévention et l'effectivité des prestations de santé il devrait également permettre d'améliorer la santé de la population et, sur le long terme, diminuer les coûts pour les systèmes de santé. Ainsi, la Commission Européenne prévoit, pour la seule partie santé mobile (m-health) et des applications pour smartphone, un gain de 99 milliards d'euros pour les systèmes de santé dans l'UE si son potentiel est pleinement exploité[30].

Les avantages des TIC en santé sont aussi la source de risques pour la vie privée des personnes puisque une grande partie des informations en cause sont qualifiées de données personnelles de santé, donc de données sensibles au regard du droit de l'UE. Ces données circulent entres différentes personnes et différents lieux et sont souvent stockées dans des bases de données qui peuvent concerner l'individu mais également une population. La masse de données de plus en plus importante, les "big data", tant au niveau individuel, c'est l'exemple du génome complet humain qui pèse aujourd'hui environ 2To (Mille Go ou Mille milliards d'octets) qu'à l'échelle populationnelle, les données personnelles étant souvent rassemblées dans des fichiers concernant un grand nombre d'individus, comme dans les registres de santé ou les biobanques, des fichiers rendus accessibles aux professionnels de santé habilités, aux chercheurs et à d'autres organismes opérant dans le système de santé, pose également nombre de défis quant à la sécurité et à la confidentialité des données. Comme dans d'autres domaines utilisant les TIC, les risques liés à la e-santé sont ceux des accès non-autorisés de la part de pirates informatiques, hackers, mais aussi de la part de compagnies commerciales, d'employeurs ou d'assureurs peu scrupuleux, voire de la part d'autorités étrangères comme l'a récemment montré le scandale de l'affaire PRISM impliquant l'Agence de sécurité Américaine, la NSA, pratiquant une surveillance illégale des communications de plusieurs personnalités européennes. Dans le domaine de la santé le droit vise à prévenir la divulgation illégitime de données médicales en violation de la confidentialité et du secret médical applicable aux données personnelles de santé. Il s'agit d'éviter les usages détournés de ces données sensibles qui peuvent conduire à des discriminations, à une surveillance illégitime ou à des manipulations de la personne. Il s'agit

[29] Article de Armelle Bohineust publié dans Le Figaro du 15 Juillet 2014. Plus d'information sur le site du journal : http://www.lefigaro.fr/societes/2014/07/15/20005-20140715ARTFIG00128-novartis-et-google-preparent-des-lentilles-intelligentes.php

[30] Commission Européenne, Communiqué de presse, La santé en poche : libérer le potentiel de la santé mobile, IP/14/394, Bruxelles, 10 Avril 2014.

également d'éviter les utilisations à des fins de commerciales non consenties ou non sollicitées. Le texte de la proposition de RGPD qualifie ces opérations de « violation de données à caractère personnel[31] ». Il s'agit d'une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel […]. A ces risques s'ajoutent les considérations particulières à porter au traitement des données personnelles relatives aux personnes en situation de vulnérabilité, comme les enfants, pour lesquels il convient de mettre en place des mesures de protection particulières et concevoir des systèmes adaptés. Enfin, il faut aussi considérer les questions liées aux particularités de certaines informations de santé générées et utilisées dans un contexte de e-santé, comme dans le contexte de l'accès aux tests génétiques vendus sur internet qui fournissent aux consommateurs des données génétiques qui peuvent ne pas seulement concerner l'acheteur mais aussi sa famille ou sa descendance, ce qui pose un ensemble de questions éthiques, notamment lors de la découverte de résultats concernant une maladie génétique à caractère familial. Tous ces facteurs augmentant les risques potentiels d'intrusions dans la vie privée des personnes devraient être pris en compte dans la réforme en cours du droit de l'UE sur la protection des données personnelles et les autres travaux d'encadrement, notamment éthiques, de la e-santé.

B- La proposition de Règlement Général de l'UE sur la Protection des Données à caractère personnel au regard des technologies de e-santé et des droits des personnes

Les TIC sont au cœur de la réforme du droit de l'UE sur la protection des données personnelles. En revanche, ni le domaine de la santé ni celui de la recherche scientifique ne semble avoir focalisé les débats, bien qu'ils soient couverts par le champ d'application de la législation Européenne depuis 1995, ce qui peut être regretté mais découle probablement des limites de compétences attribuée à l'Union dans ces secteurs par rapport aux autres domaines comme la consommation. Cependant, le déroulement de la réforme semble faire honneur à la participation démocratique. Depuis 2009 la Commission Européenne prépare le chantier de la réforme en pratiquant de façon régulière des consultations publiques à même de l'éclairer sur la nature et la portée des améliorations à apporter au système mis en place sous l'égide de la Directive 95/46/CE. A titre d'exemple, un sondage Eurobaromètre[32] de 2011 concernant la protection des données personnelles montre clairement que plus des trois quarts des citoyens Européens (78%) sondés ont une totale confiance dans les institutions de santé (hôpitaux, médecins, pharmaciens etc.). En revanche il est intéressant de constater que les acteurs privés et compagnies du secteur des télécommunications (téléphonie et internet inclus) arrivent en dernier du classement, montrant ainsi une méfiance marquée des personnes vis-à-vis de leur capacité à protéger les données personnelles et la vie privée des personnes. Il faudra donc, pour les institutions de santé garantir que l'arrivée massive des TIC ne porte pas atteinte au haut degré de confiance dont elles bénéficient, et, pour les opérateurs commerciaux des TIC il s'agit de développer les garanties nécessaires à recouvrer la confiance qui leur fait défaut, surtout lorsqu'ils envisagent de mettre sur le marché des dispositifs de e-santé utilisant des données personnelles sensibles dont l'utilisation est fortement règlementées, ceci passant par l'offre d'outils à la fois fiable et respectueux des droits et de la vie privée des personnes.

La proposition de RGPD modifiée par le Parlement Européen en Mars 2014 conserve le même champ d'application matériel que celui de la Directive 95/46/CE et son approche dite « technologiquement neutre ». Ses règles visent donc à protéger les personnes physiques dans le

[31] Article 4 al.9 du RGPD, version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.

[32] Eurobaromètre Spécial, EBS 359, Vague EB 74.3, Attitudes à l'égard de la protection des données et de l'identité électronique dans l'Union européenne, p.138, Novembre – Décembre 2010, Publication: Juin 2011. Disponible à l'adresse suivante: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

traitement des données à caractère personnel, ces dernières étant définies dans son Article 4 alinéa 2 comme « Toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tels que le nom, un numéro d'identification, des données de localisation, un identifiant unique ou à un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, ou au genre de cette personne »[33]. Des précisions relatives à l'identité physiologique et génétique ont été apportées. Le Règlement précise également que les règles qu'il fixe s'applique aux traitements utilisant des données pseudonymisées[34] (codées), cryptées[35], y compris ceux utilisant des identifiants fournis par des dispositifs, des applications, outils ou protocoles (ex : adresse IP, cookies, Identification par radiofréquence RFI)[36]. La définition des données sensibles composant une catégorie spéciales de données personnelles impliquant l'application de règles strictes, est complétée. Sont considérées comme sensibles les « données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances, l'appartenance syndicale, ainsi que le traitement des données génétiques ou des données concernant la santé ou relatives à la vie sexuelle ou à des condamnations pénales ou encore à des mesures de sûreté connexes » en référence à l'Article 9 du RGPD. Les données de santé, à l'instar des données génétiques et biométriques, font désormais l'objet d'une définition dans l'Article 4 alinéa 12 de la proposition. Sont considérées de manière large comme des données personnelles de santé « toute information relative à la santé physique ou mentale d'une personne, ou à la fourniture de prestations de santé à cette personne ». Cette définition est complétée par un considérant 26 donnant plus de détails sur cette notion. Le principe d'interdiction de traitement des données personnelles de santé et les exceptions limitatives qui l'accompagnent demeurent[37]. La lecture combinée des Article 9 et 81 du RGPD concernant le traitement des données personnelles de santé fixe la liste des exceptions pouvant légitimer un traitement de ces données à des fins de santé, lesquelles sont principalement liées à l'obtention préalable du consentement informé de la personne concernée, aux nécessités relatives à la prestation d'un service de santé, à la gestion du système de santé et de sécurité sociale, à la réalisation d'un contrat licite ou à la mise en œuvre de recherches scientifiques. La possibilité de traiter des données personnelles de santé à des fins de protection des travailleurs est également prévue à l'Article 82. L'ensemble des personnes impliquées dans le traitement (responsable du traitement des données de santé doivent être soumises à une obligation de confidentialité et de secret professionnel, ici le secret médical. Cependant, sur le fond, le texte du RGPD de Mars 2014 emportent des renforcements notables des principes généraux applicables à tout traitement de données personnelles et des droits des personnes concernées, sans pour autant en modifier fondamentalement la substance. En revanche le texte est porteur d'une refonte organisationnelle importante en introduisant la notion de « guichet unique » dans la gestion des traitements de données transfrontaliers impliquant plusieurs Etats Membres, laquelle confère compétence à l'autorité nationale de protection des données du lieu du principal établissement du

[33] Voir également le considérant 23 du RGPD version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit. Ce considérant donne des précisions sur les éléments à prendre en compte dans la qualification juridique des données.
[34] Article 4 alinéa 2a du RGPD version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.
[35] Article 4 alinéa 2b du RGPD version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.
[36] Voir le considérant 24 du RGPD version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.
[37] Article 9 du RGPD version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.

responsable du traitement[38] pour surveiller les opérations, recevoir les éventuelles demandes d'autorisation du traitement et les plaintes des personnes concernées[39], en coopération avec les autorités compétentes des autres Etats Membre concernée.

Un des renforcements important opéré par la proposition de RGPD prévoit de fournir aux personnes concernées la possibilité d'exercer leurs droits par voie électronique, ce qui préfigure l'émergence de nouveaux systèmes et renforce l'approche technologique du droit sur la protection des données personnelles. Le texte renforce notamment en ce sens le droit à l'information préalable au traitement dont bénéficie la personne concernée en instaurant une nouvelle procédure orientée TIC et internet dans l'Article 14 du RGPD. Cet article fixe une procédure en deux étapes. Dans un premier temps, le responsable du traitement aura l'obligation de fournir une notice d'information standardisée faisant apparaître de manière claire les principaux éléments du traitement des données personnelles impliquant la personne concernée. Chaque rubrique de la notice représente une phase du traitement également représentée par un symbole, pour plus de clarté. A chaque rubrique est associée une indication simple sous la forme d'un symbole signifiant « oui » ou « non ». Une version présentée à l'origine sur du papier millimétré est reproduite et annexé au présent article, en anglais uniquement[40]. Après réception de ces premiers éléments informatifs le responsable du traitement devra fournir des informations détaillées pour chaque opération à réaliser, par tous moyens, dans le respect de la nouvelle liste des éléments à informer fixée à l'Article 14 du RGPD. Outre les éléments classiques pour lesquels une information loyale claire et compréhensible doit être présentée à la personne concernée selon l'actuelle Directive 95/46/CE, le RGPD fait apparaitre de nouveaux items à informer, comme la durée du traitement (y compris donc de conservation), la source des données lorsque celle-ci ne sont pas recueillies auprès de la personne concernée, la transmission des données à des autorités publiques, l'existence d'un droit de recours et les moyens de l'exercer. En complément du droit à l'information préalable au traitement, dans une optique de transparence, les personnes devront être informées en cas de violation de leur données personnelles[41].

Au titre des renforcements importants des droits des personnes pour la e-santé qu'opèreraient le RGDP la notion de consentement libre et éclairé (ou informé) est clarifiée, ses conditions de validité sont renforcées[42]. Ainsi, lorsque le droit national impose le recueil préalable du consentement de la personne au traitement de ses données de santé celui-ci devra être recueilli, éventuellement sous forme électronique, la charge de la preuve reposant sur le responsable du traitement. Selon le RGPD, le consentement doit être informé, donné librement et être explicite, c'est-à-dire donner une indication claire de la volonté de la personne concernée. Le choix de la personne doit s'exercer par une action caractérisant son acceptation du traitement (ex : cocher une case, signer un formulaire papier – modèle opt-in) ou, dans certains cas prévue par la loi, par un comportement significatif. Le considérant 25 du RGPD précise alors qu'il ne saurait y avoir de consentement tacite ou passif. Le consentement dit être limité à la réalisation de certaines finalités spécifiées et respecter le principe de proportionnalité. Lorsque les finalités du traitement sont atteintes ou lorsque les données ne sont plus nécessaires à la

[38] Le responsable du traitement est la personne, l'autorité publique, le service ou l'organisme qui détermine la finalité et les moyens du traitement des données personnelles.

[39] Ce point a été critiqué par le CNIL, autorité de protection des données en France, comme entrainant un éloignement dans la protection des personnes qui devraient alors saisir une autorité étrangère pour faire valoir leur droit au détriment d'une protection nationale mieux à même de traiter ces revendications. CNIL, Article, Projet de règlement européen : la défense de la vie privée s'éloigne du citoyen, epub, 26 janvier 2012, disponible à l'adresse suivante : http://www.cnil.fr/linstitution/actualite/article/article/projet-de-reglement-europeen-la-defense-de-la-vie-privee-seloigne-du-citoyen-1/

[40] Annexe 1 du présent article.

[41] Article 32 du RGPD version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.

[42] Article 7 et considérant 25 du RGPD version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.

réalisation de ces objectifs, le consentement perd sa validité. Sur la forme, lorsqu'un consentement écrit est requis par la loi il doit être distinct de toute autre déclaration. L'Article 81 alinéa 2 érige l'exigence de l'obtention du consentement informé écrit de la personne concernée avant la mise en œuvre du traitement de ses données personnelles de santé à des fins de recherche en tant que principe. Le texte permettrait néanmoins prévoir la possibilité de prévoir une ou plusieurs finalités spécifiques dans ce consentement au traitement des données personnelles de santé en recherche, ce qui semble correspondre aux nécessités de réutilisation des données qui en pratique favorisent les progrès scientifiques. Cette exigence reste néanmoins plus contraignante et peut entrer en conflit avec des dispositions issues des droits nationaux prévoyant une simple non-opposition de la personne afin de pouvoir procéder à ce genre de traitement en recherche. Cela est régulièrement le cas dans le domaine de la santé, y compris en droit français, ces traitements étant souvent secondaire par rapport à une prestation de santé et consistant en une réutilisation légitime d'intérêt public des données. Pour pallier à ces situations contradictoires, le RGPD prévoit que les droits nationaux conservent la possibilité de prévoir des exceptions au consentement requis par l'Article 81 alinéa 2 sous réserve de garanties appropriées et sans que l'application de l'Article 83 du RGPD concernant les traitements de données à des fins de recherche ne soit remis en cause. Quelle que soit le contexte les personnes concernées jouissent d'un droit de retrait de leur consentement au traitement pouvant s'exercer à tout moment.

Les personnes concernées conservent la jouissance de leurs autres droits comme le droit d'accès aux données, complété par un droit à la portabilité des données[43], le droit de rectification[44] et d'effacement[45]. Des modifications importantes concernent le droit à l'effacement des données, lequel est renforcé par un droit à l'oubli numérique consacré à l'Article 17 du RGPD et désormais affirmé dans le droit positif par la récente décision de la Cour de Justice de l'Union Européenne du 13 Mai 2014 ayant imposé à google de se mettre en conformité au regard de ce droit à l'oubli, dans le respect du droit de l'UE, sur le fondement de la Directive 95/46/CE qui, bien que ne reconnaissant pas explicitement ce droit en tant que tels, contient les dispositions nécessaires pour que les juges puisse en affirmer l'existence[46]. Peu de temps après la décision de la CJUE, google mettait en ligne sur ses serveurs européens un formulaire dédié à l'exercice de ce droit. Trois jours plus tard, 41000 demandes avaient déjà été reçues selon un communiqué de la firme, nombre ayant presque doublé selon certains observateurs dès le mois suivant. Les enseignements à en tirer sont nombreux. Les critiques aussi[47]. Pour certains l'application de ce droit est ingérable et demande des ressources humaines et technologiques nouvelles. Il s'agit par exemple de constituer des équipes en charge d'analyser la validité des demandes au regard des conditions juridiques fixées par le droit et des motifs invoqués par le demandeur. De plus, il est selon eux difficile de garantir un effacement total du web lorsque les données ont déjà été disséminées, copiées, modifiées ou déplacées. Cependant, il semble bien légitime de permettre aux personnes d'exercer ce nouveau droit en mettant en œuvre les moyens nécessaires pour y parvenir. Ce nouveau droit également applicable dans le domaine de la e-santé pourrait néanmoins connaitre des limitations lorsque le traitement des données est nécessaire à la protection de

[43] Article 15 du RGPD version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.
[44] Article 16 du RGPD version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.
[45] Article 17 du RGPD version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.
[46] CJUE, Arrêt Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González dans l'affaire C-131/12, 13 Mai 2014. Disponible sur le site de la Cour à l'adresse suivante : http://curia.europa.eu/juris/document/document.jsf?docid=152065 Communiqué de presse officiel n°70-14, disponible à l'adresse suivante : http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070fr.pdf
[47] Article de D. Dq. Google propose un « droit à l'oubli »… La suppression totale d'une info du net ne peut pas être garantie. Science&Vie, n°1163, Rubrique Science et Société, p.36-39, Aout 2014.

la personne concernée ou à la réalisation d'une finalité légitime comme une prestation de santé ou la correcte gestion du système de santé. Dans des cas bien précis, il pourrait être fait exception à l'application de ce droit lorsque cela est justifié par le responsable du traitement, dans le respect du droit de l'UE et du droit national applicable. Ainsi, si le respect du droit à l'oubli numérique ne semble pas poser de problèmes lorsque les données sont référencées sur des réseaux sociaux ou d'autres sites ayant permis à la personne de publier ses informations de santé, il parait impossible qu'une personne accède à une demande de destruction de son dossier médical, celui-ci étant principalement conservé et utilisé dans l'intérêt vital du patient[48]. En revanche le texte du RGPD prévoit la possibilité de limiter le traitement des informations visées ou de reconditionner les données, de les pseudonymiser lorsque celles-ci sont conservées sous une forme directement identifiante, de les crypter ou de les anonymiser totalement lorsque cela est possible. Lorsque celles-ci sont ou ont été traitées de manière illicite ou lorsque les données sont en cours de traitement dans le cadre d'une opération licite mais ne seront plus utile à l'issu de la réalisation des finalités du traitement, il devrait être possible d'en obtenir l'effacement. Bien que ces aménagements spécifiques au domaine de la santé puisse trouver écho dans le domaine de la e-santé leur conception et leur mise en œuvre nécessitera de plus ample études[49].

Les adaptations apportées aux droits des personnes en fonction des possibilités technologiques[50] actuelles sont complétées par une extension du champ d'application territorial du RGPD visant à faire appliquer les règles qu'il fixe à des opérateurs établis à l'extérieur des frontières de l'Union. En effet l'Article 3 alinéa 2 du RGPD précise que le Règlement « s'applique au traitement des données à caractère personnel appartenant à des personnes concernées dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes concernées ou à l'observation de ces personnes concernées ». Un alinéa 3 précise l'application du RGPD lorsque le responsable du traitement est établi dans un lieu où la législation nationale d'un État membre s'applique en vertu du droit international public. Ainsi un opérateur de e-santé établi aux Etats-Unis pourrait avoir à se conformer aux dispositions du droit de l'UE lorsqu'il offre ses services de e-santé à des personnes résidant sur le territoire de l'UE, sous peine de poursuite et de sanctions[51].

Ces modifications sont complétées par un renforcement des principes généraux applicables à tout traitement de données personnelles[52], au titre desquels figurerait le concept de « Privacy by design » (PbD) que devront respecter les acteurs de la e-santé.

2- L'approche Privacy by design et l'obligation d'évaluation des risques : des rapports resserrés entre le droit et les technologies pour une responsabilisation accrue de l'ensemble des acteurs

[48] A cet égard le groupe de travail des autorités de protection de données européennes (G29 ou Article 29 Working Party) établi par l'Article 29 de la Directive 95/46/CE à adopté une Opinion sur la notion d'intérêt légitime poursuivie par le responsable du traitement, lequel peut être invoqué pour faire exception à certains droits des personnes dans le traitement de leurs données personnelles dans certaines circonstances et sous conditions. Voir, Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopté le 9 avril 2014, uniquement en anglais. Disponible à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

[49] A cet égard le G29 s'est réuni le Les autorités se sont également penchées sur les critères permettant de prendre en compte, dans certains cas spécifiques, l'intérêt du public à accéder à l'information en cause.

[50] Voir le tableau synthétique présenté en Annexe 2 du présent article.

[51] Sur le renforcement des sanctions administratives prévues par la proposition de RGPD voir le tableau présenté en Annexe 2 du présent article.

[52] Article 5 du RGPD version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.

A- L'approche Privacy by design pour la protection des données personnelles et la responsabilisation des professionnels

L'approche « Privacy by Design » (Pbd) ou « Protection de la vie privée dès la conception » est un concept juridique conçue pour les technologies de traitement des données personnelles, y compris de santé. Ce concept n'est pas nouveau mais tend à devenir un véritable principe général au travers de sa possible consécration dans le cadre du futur RGPD de l'UE. Ses origines remontent aux années 1960 où l'idée de ce concept innovant et intégrant faisant de la protection de la vie privée un élément essentiel du développement des nouvelles technologies émerge au sein de la communauté des ingénieurs en informatique[53]. Le concept se développera plus avant dans les années 1990 grâce à Ann Cavoukian, Commissaire à l'information et à la protection de la vie privée de l'Ontario (Canada) qui continue à ce jour[54] à porter ce concept qui sera consacré au niveau international avec la signature d'une Résolution sur la protection de la vie privée dès la conception[55] à Jerusalem, 2010, à l'occasion de la Conférence Internationale des Commissaires à la protection de la vie privée et des données personnelles. L'approche PbD se fonde sur le constat que le droit seul ne permet plus une protection efficace de la vie privée si l'on considère les nouveaux défis posés par les développements technologiques et les évolutions de l'environnement informatique mais nécessite un nouveau standard de développement permettant de mettre la technologie au service du droit et d'assurer une protection de la vie privée par des procédés adaptés, intégrés et innovants. Ces objectifs ne peuvent être atteints sans collaborations interdisciplinaires, sans coopération entre des juristes, des techniciens, des ingénieurs du domaine des TICs et, dans le cadre de la e-health, des spécialistes de l'éthique médicale. L'approche PbD se fonde sur 7 principes[56] qu'il s'agit de prendre en compte dans la conception des TIC, dans l'architecture des systèmes ou réseaux informatiques mais aussi dans les politiques et les bonnes pratiques des industriels et des responsables du traitement. Pour aller à l'essentiel ces principes vise adopter une approche proactive plutôt que réactive sur les questions de respect de la vie privée. Il s'agit d'anticiper les évènements invasifs, volontaires ou accidentels, avant qu'ils ne surviennent afin de les éviter. L'approche PbD cherche également à protéger de manière automatique les données personnelles quelques soit le type de technologie concerné. Aucune action n'est nécessaire de la part de l'individu pour qu'ils bénéficient d'une protection dites « par défaut », c'est inhérent au système et aux pratiques professionnelles. Les principes de PbD incorporés dans la conception et l'architecture des TICs et dans les pratiques professionnelles font des aspects de protection de la vie privée une composante essentielle de la fonctionnalité proposée par un dispositif ou un service. La vie privée est intégrée dans le système sans en diminuer la fonctionnalité. Une approche PbD doit considérer le cycle de vie des données traitées et donc fournir des fonctionnalités protectrices avant-même la première collection de données personnelles mais aussi tout au long du traitement jusqu'à la destruction sécurisée des données. L'approche PbD doit être centrée sur l'utilisateur ou l'usager. Cela demande aux producteurs des TICs (architectes et fournisseurs) et prestataires de service de protéger les intérêts des utilisateurs des dispositifs en leur offrant des notices d'information appropriées et en leur permettant de faire des choix et de prendre des décisions par le biais de "user-friendly options". Les composantes des systèmes ayant trait à la gestion des données personnelles doivent être visibles et transparentes pour les utilisateurs des dispositifs et des services associés. Quelque soit le secteur

[53] Ex: Article de Alan Hedley "Privacy as a factor in residential buildings and site development: an annotated bibliography", in Issue 32 of Bibliography, National Research Council of Canada. Division of Building Research, 1966.

[54] Voir le site internet www.privacybydesign.ca

[55] Résolution sur la protection intégrée de la vie privée, Adoptée lors de la 32e Conférence internationale des commissaires à la protection des données et de la vie privée, 27-29 octobre 2010, Jérusalem, Israël, 2010. Disponible à l'adresse suivante : http://www.ipc.on.ca/site_documents/pbd-resolution-f.pdf

[56] Voir le schéma reproduit à l'Annexe 3 du présent article, en anglais uniquement.

d'activité ou la technologie concernée l'approche PbD cherche à renforcer la confiance de toutes les partie-prenantes, à accommoder tous les intérêts et les objectifs légitimes de manière positive dans un arrangement entre les partie-prenantes qui serait « gagnant-gagnant ».

Le concept de PbD vise à devenir un standard pour la révision des cadres juridiques relatifs à la protection de la vie privée. La proposition de RGPD vise à le consacrer en tant que principe de portée générale dans son Article 23 intitulé « Protection des données personnelles dès la conception et par défaut ». L'Article 23 se compose de deux alinéas représentant de manière claire les deux aspects de l'approche PbD développée outre Atlantique à savoir les aspects de protection « by design », dès la conception, et « by default », par défaut. L'Article 23 alinéa 1 dispose que « Compte étant tenu des techniques les plus récentes, des connaissances techniques actuelles, des meilleures pratiques internationales et des risques représentés par le traitement des données , le responsable du traitement et le sous-traitant éventuel appliquent, tant lors de la définition des objectifs et des moyens de traitement que lors du traitement proprement dit, des mesures et procédures techniques et organisationnelles appropriées et proportionnées, de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et garantisse la protection des droits de la personne concernée, notamment en ce qui concerne les principes établis à l'article 5. La protection des données dès la conception tient compte en particulier de la gestion du cycle de vie complet des données à caractère personnel, depuis la collecte jusqu'à la suppression en passant par le traitement. Elle est systématiquement axée sur l'existence de garanties procédurales globales en ce qui concerne l'exactitude, la confidentialité, l'intégrité, la sécurité physique et la suppression des données à caractère personnel. Une fois que le responsable du traitement a procédé à une analyse d'impact relative à la protection des données, conformément à l'article 33, les résultats sont pris en compte lors de l'élaboration desdites mesures et procédures ». L'alinéa 2 de l'Article 23 dispose quant à lui que « Le responsable du traitement s'assure que, par défaut, seules seront traitées les données à caractère personnel nécessaires à chaque finalité spécifique du traitement, ces données n'étant, en particulier, pas collectées, conservées ou communiquées au-delà du minimum nécessaire à ces finalités, pour ce qui est tant de la quantité de données que de la durée de leur conservation. En particulier, ces mécanismes garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques et que les personnes concernées ont la possibilité de contrôler la diffusion de leurs données à caractère personnel. »

Il est très intéressant de constater que les travaux législatifs e cours au niveau de l'UE dépassent le stade théorique du concept en intégrant dans le corps de la proposition un ensemble d'éléments juridiques et de procédures nouvelles donnant un caractère effectif à cette approche. Ainsi le concepteur de technologies de e-santé, comme l'éventuel prestataire de service associé à l'utilisation de ces technologies, devront prêter une attention particulière au respect des dispositions du Règlement en vertu de l'Article 23. Pour appliquer cette nouvelle approche « technojuridique », la personne responsable du traitement devra se conformer à l'obligation de pratiquer une analyse d'impact préalable au traitement des données personnelles qu'elle prévoit de réaliser. Cette évaluation d'impact du traitement sur la protection des données personnelles caractérise l'approche adoptée par le RGPD fondée sur le risque du traitement et fait l'objet de nouvelles procédures décrites aux Article 32 bis et 33 du RGDP. Cette évaluation d'impact, nommé « Evaluation d'Impact sur la Vie Privée » ou EIVP par la CNIL, concerne certains traitements dont les éléments comportent a priori un risque particulier vis-à-vis des droits et libertés des personnes concernées. Ainsi, cette évaluation est obligatoire lorsque le traitement porte sur des données sensibles comme des données personnelles de santé, les données génétiques ou biométriques, lorsqu'il porte sur des données personnelles relatives à des enfants,

lorsque le traitement envisagé vise à surveiller[57] les personnes, lorsqu'il vise à la fourniture de soins de santé, à des recherches épidémiologiques ou à des études relatives à des maladies mentales ou infectieuses, lorsque les données sont traitées aux fins de l'adoption de mesures ou de décisions à grande échelle visant des personnes précises; ou encore lorsqu'il concerne plus de 5000 personnes identifiable sur une période de 12 mois consécutifs (quelque soit le type de données et la finalité du traitement). Ce dernier exemple démontre la prise en compte des enjeux soulevés par les « big data ». L'analyse devra au moins décrire les éléments listés dans le corps de l'Article 33 et présenter, entre-autres, le(s) traitement(s) envisagé(s), accompagné(s) d'une justification de leur nécessité et de leur proportionnalité par rapport à la finalité poursuivie, les risques prévisibles identifiés vis-à-vis des droits et libertés des personnes et les garanties, mesures et mécanismes envisagées pour prévenir et traiter ces risques, comme les garanties et mesures de sécurité assurant la protection des données et la gestion du cycle de vie des données traitées. L'ensemble des principes généraux fixés à l'Article 5 du RGPD devront être considérés. Le choix des technologies à utiliser devrait être adapté aux risques et permettre de réduire au maximum le volume de données à caractère personnel traitées. L'analyse devra aussi comporter une indication générale des délais impartis pour l'effacement des différentes catégories de données et une liste des destinataires ou des catégories de destinataires des données, y compris lorsque les données feront l'objet d'un transfert vers un pays tiers à l'UE[58]. L'analyse doit être documentée, conservée et mise à disposition des autorités de contrôle. Une seule analyse suffit à examiner un ensemble de traitements similaires présentant des risques similaires. Un calendrier[59] fixant les échéances d'un examen périodique de la conformité de l'analyse d'impact au regard des règles du RGPD devra également être mis en place et en cas de découverte d'une non-conformité il faudra procéder à une mise à jour de l'évaluation et des mesures associées. Un examen périodique de la conformité de l'évaluation d'impact devra dans tous les cas être mis en œuvre par le responsable du traitement ou le sous-traitant agissant pour son compte dans un délai de 2 ans au plus tard après la date de réalisation de l'analyse d'impact d'origine[60].

Ce renforcement des obligations qui incombent au responsable du traitement est associé à une obligation de désigner un Correspondant Informatique et Libertés (connu en droit français depuis 2004 sous l'appellation CIL), ou Data Protection Officer en anglais, qui sera associé à la procédure d'évaluation d'impact, conseillera et administrera le traitement pour le compte du responsable. La désignation d'un CIL devrait être la règle dans le domaine de la e-santé. Ce nouvel acteur de la protection des données personnelles présente plusieurs avantages pour le responsable du traitement et ses sous-traitants qui bénéficieront d'allègements procéduraux, mais également d'un interlocuteur compétent de proximité leur permettant un accès facilité à une information juridique adaptée à leurs activités. Grâce à l'activité des CIL dont les modalités de désignation et les missions sont fixées par le RGPD aux Articles 34, 35 et 36, le responsable du traitement pourra facilement s'inscrire dans la démarche de PbD. Il pourra poser ses questions et trouver des solutions concertées afin de se conformer au droit. Le CIL est également un vecteur de diffusion d'une culture de la protection de la vie privée au sein des entreprises et institutions publiques qui auront dès lors toutes les clés pour

[57] Traitement de données visant à l'évaluation ou à la prédiction de la situation économique de la personne, de sa localisation, de son comportement, de son état de santé, de ses préférences, et sur la base de laquelle sera adopté une décision produisant des effets juridiques pour la personne concernée – ex : profilage.

[58] La liste complète des éléments de base devant faire l'objet d'une évaluation et d'un rapport d'analyse sont énumérés à l'Article 33 alinéa 3 du RGPD, version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.

[59] Article 33 alinéa 3 ter et Article 33 bis alinéa 1 du RGPD, version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.

[60] Article 33 bis alinéa 1 du RGPD, version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.

mettre en place des Codes de bonnes conduites[61]. Tous ces éléments visent à appliquer le principe juridique naissant de PbD dans le droit de l'UE. La proposition de RGPD favorise l'auto-régulation des professionnels et encourage les initiatives allant en ce sens en incitant notamment les Etats Membres à créer des labels et des procédures de certification de qualité[62] au regard de la protection des données personnelles ce qui permet de reconnaitre et de valoriser les efforts accomplies par certaines entités dans le sens d'une protection constante de la vie privée des personnes dont elles utilisent les données personnelles. Un responsable du traitement ou un de ses sous-traitants pourra demander à n'importe quelle Autorité de contrôle dans l'UE de certifier la conformité des traitements entrepris, moyennant le paiement de frais raisonnables. Le texte prévoit également à l'Article 23 alinéa 1 bis que pour encourager la mise en œuvre étendue dans différents secteurs économiques des mesures liées à la protection des données dès la conception le respect de celle-ci sera une « condition préalable aux offres de marchés publics en vertu de la Directive 2004/18/CE du Parlement et du Conseil 48 bis[63] ainsi que de la Directive 2004/17/CE du Parlement européen et du Conseil[64] 48 ter («Directive secteurs spéciaux») ». Mais la responsabilisation accrue des acteurs du traitement par un renforcement des obligations liées à l'approche PbD semble répondre au principe général de responsabilité (« accountability » en anglais) nouvellement distingué par le RGPD dans son Article 5 visant créer un système efficace, à la fois rigoureux et souple. Bien sûr, les acteurs de la e-santé devront (s')investir dans le respect de la vie privée, mais ils devraient pouvoir également en tirer un bénéfice.

B- L'approche Privacy by design et la responsabilisation des citoyens concernés

Les règles relatives à la protection de la vie privée et des données personnelles dès la conception et par défaut exposées plus haut conduisent à donner plus d'autonomie aux personnes concernées par le traitement de leurs données de santé. Celles-ci devraient donc supporter plus de responsabilités. Se voyant offrir des possibilités de choix plus étendues qu'auparavant celles-ci seront invitées à réfléchir à la portée des traitements de données qui leurs sont proposer et à en délimiter les contours. Si la marge de manœuvre des personnes devra être conçue et limitée par le responsable du traitement il apparait que la distinction entre les rôles de chacun devient ténue. Ainsi faudra-t-il éviter qu'une personne concernée au sens de la définition donnée par la proposition de RGPD puisse être confondu avec le responsable du traitement ou être considérée comme étant co-responsable du traitement, ce qui aurait pour effet de créer une certaine confusion sur la portée des règles applicables. La personne concernée, jusqu'alors considérée comme la partie faible, ne devrait pas avoir à supporter des responsabilités disproportionnées. Si le concept de PbD et le contenu de la proposition de RGPD semble répondre aux préoccupations des citoyens Européens et participer à la démocratie participative il est néanmoins importants de se demander jusqu'à quel point les personnes doivent être impliquées et jusqu'à quel point celles-ci pourront décider de la portée de leur implication. Ceci est particulièrement important dans la conception des outils de e-santé. Si un effort considérable sera demandé au responsable du traitement pour définir le niveau de protection offert par défaut aux données utilisées il faudra également qu'il envisage les options disponibles en fonction des nécessités imposées par la

[61] Article 38 du RGPD, version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.
[62] Article 39 du RGPD, version modifiée adoptée par la Résolution législative du Parlement européen du 12 mars 2014, op.cit.
[63] Directive 2004/18/CE du Parlement européen et du Conseil du 31 Mars 2004 portant coordination des procédures de passation des marchés publics de travaux, de fournitures et de services, JO L 134 du 30 Avril 2004, p. 114.
[64] Directive 2004/17/CE du Parlement européen et du Conseil du 31 Mars 2004 portant coordination des procédures de passation des marchés dans les secteurs de l'eau, de l'énergie, des transports et des services postaux, JO L 134 du 30 Avril 2004, p. 1.

finalité poursuivie. Si le renforcement de la procédure d'information préalable des personnes concernées devrait leur permettre de comprendre les implications d'un traitement de données et d'agir en connaissance de cause, il faudra par ailleurs éduquer les citoyens à comprendre l'utilité des traitements envisagés, y compris annexes, ces derniers étant souvent opérés à d'autres fins que celles prévues au traitement d'origine. En e-santé, il s'agira particulièrement de renseigner la personne sur l'intérêt que peuvent revêtir ces traitements secondaires de l'information notamment dans le cadre de recherche scientifiques. Les données personnelles de santé sont une ressource précieuse pour l'avancée des connaissances dans le domaine de la santé, pour améliorer les technologies et pratiques de santé. S'il ne faut pas être effrayé à l'idée de donner plus de pouvoir à la personne concernée afin que celle-ci exerce ses droits et libertés, il faut être conscient des dépenses connexes pour les professionnels qui peuvent s'avérer coûteuses. Enfin, un aspect de responsabilisation indirectement lié à la protection de la vie privée de la personne vise à réduire le potentiel d'un impact négatif que pourrait avoir une mauvaise utilisation des dispositifs de e-santé. Un usage abusif de ces outils pourrait avoir des effets psychologiques néfastes sur les personnes, lesquelles pourraient développer des obsessions, surtout lorsque l'utilisateur est en bonne santé. Dans de tels cas les avantages procurés par ces dispositifs seraient annulés. De même, les pratiques de e-santé auront certainement un impact sur la pratique des professionnels de santé qui devront parfois composer avec des informations erronées ou exagérées d'un point de vue médical. La relation médecin-patient pourrait pâtir de cette profusion d'informations et l'impact sociétal de l'arrivée massive de ces dispositifs dans une société tentée par la normalisation devrait être surveillée et étudiée afin de pouvoir éviter les dérives. De la même manière, la question de la détermination des responsabilités dans l'utilisation des technologies de e-santé devrait faire l'objet d'une étude approfondie. Cette question, sans nul doute très importante, est également très complexe du fait de la multiplicité des acteurs, des facteurs et des causes de préjudices éventuels, comme le note la Commission Européenne dans son Livre Vert sur la santé mobile[65] de 2014.

Pour conclure nous pouvons constater que la réforme du droit de l'UE sur la protection des données personnelles prend plus que jamais une dimension technologique destinée à garantir l'effectivité des règles de protection des données personnelle dans le monde numérique mouvant dans lequel nous évoluons aujourd'hui. En proposant d'adopter l'approche PbD, la proposition de RGPD adoptée au Parlement Européen veut instaurer un environnement protecteur, cohérent et intégré à même de durer dans un contexte technologique aux évolutions nombreuses et rapide. S'appuyant sur une approche de responsabilisation des acteurs et sur une approche intégrée de la protection des données qui devrait faire corps avec les TIC, le texte de la proposition renforce les droits des personnes concernées et les obligations du responsable du traitement. En parallèle il semble ouvrir à une plus grande autonomie des professionnels pour s'autoréguler en adoptant des Codes de bonne conduite et en prévoyant la création de labels européens sur la protection des données. Si la protection des données apparait alors comme un enjeux économique pour les entreprises et un moteur pour l'innovation, la proposition va au-delà des préoccupations économiques et ouvre également à plus d'autonomie pour les personnes concernées dans les opérations de traitement des données personnelles, y compris de santé, permettant ainsi de créer un environnement participatif et collaboratif plutôt dynamique. L'approche de protection des données personnelles dès la conception et par défaut pourrait constituer le socle d'une vague d'innovations technologiques et juridiques et éthiques plus techniques. Mais elle pourrait se révéler être à double tranchant dans le contexte d'une règlementation assez stricte et complexe à lire pour les non-initiés, surtout si l'on considère le coût potentiel des mesures et l'ampleur des questionnements éthiques et juridiques entourant les activités de e-santé qui ne sont pas traité par le RGPD, nous ne pourrions que redouter un coup de frein ou la

[65] COM(2014) 219 final, 10 Avril 2014, op.cit. p.18.

fuite de quelques entrepreneurs hors de l'UE. Au pire, un délaissement massif du marché Européen. Cependant le potentiel démocratique positif de ces mesures est bien là. Il semble que l'approche de PbD et des dispositions du RGPD permettrait d'incorporer plus précocement les principes de protection de la vie privée et dans le développement des TIC, y compris de e-santé, et en attachant les droits de la personne aux données personnelles, en les faisant circuler avec les données personnelles dont ils seraient l'attribut. Les TIC seraient le vecteur de cet attachement et de cette circulation. Il reste encore beaucoup de questions en suspens sur l'impact de ces règles dans le domaine de la santé et de la recherche. Les questions spécifiques relatives à la e-santé requièrent des développements spécifiques parfois hors du cadre du RGPD. Les réflexions juridiques et éthiques sur la portée des modifications apportées auront leur importance sachant que la Commission Européenne et le nouveau Comité Européen de la Protection des Données qu'instituerait le RGPD auraient compétence pour adopter des actes délégués sectoriels qui pourraient éventuellement préciser l'application des règles au secteur de la e-santé. Le texte est aujourd'hui devant le Conseil qui ne s'est pas encore prononcé sur l'intégralité de la proposition adoptée par le Parlement Européen.

ANNEXES :

Annexe 1 : Notice d'information préalable des personnes concernées par le traitement de leurs données personnelles (y compris de santé), en vertu de l'Article 14 de la proposition de RGPD, version Mars 2014.

ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data are **collected** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **retained** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **processed** for purposes other than the purposes for which they were collected	
	No personal data are **disseminated** to commercial third parties	
	No personal data are **sold or rented out**	
	No personal data are retained in **unencrypted** form	

(a)

(b)

Annexe 2 : Tableau synthétique des principales modifications apportées par la proposition de RGPD, version Mars 2014, vis-à-vis des droits des personnes dans le traitement de leurs données personnelles de santé.

Droits	Renforcements	Ref.
Information préalable au traitement	2 temps / liste	Art.13a ; Art.14 Art.11
Consentement préalable de la personne au traitement des données de santé	Reste un des éléments de la levée de l'interdiction / explicite / distinct / pour une ou plusieurs finalités / droit de retrait / peut être exercé par voie électronique	Art.81; Art. 7; Art.9 al.2(a)
Opposition au traitement	Sans justification / gratuitement / peut être exercé par voie électronique	Art.19
Accès aux données	Droit à la portabilité	Art.15
Rectification, effacement	Droit à l'oubli numérique	Art.16; Art.17
Droit de recours	Vs un responsable / un sous-traitant / une ANPD Recours collectif	Art.73; Art.74; Art.75
Sanctions administratives	Jusqu'à 100 millions d'€ ou 5% CAA mondial	Art.79

Annexe 3 : Schéma représentant les principes fondateurs de l'approche « Privacy by Design ». Source : www.privacybydesign.ca