IMPACT DE L'UTILISATION DES NOUVELLES TECHNOLOGIES DANS L'EVALUATION DES PRODUITS DE SANTE, SUR LA PROTECTION DES DONNEES PERSONNELLES

Les technologies du numérique ont totalement révolutionné notre façon de vivre. Planifier ses journées, travailler, communiquer, se déplacer, consommer… nos activités quotidiennes tant professionnelles que personnelles ont été radicalement modifiées par l'apparition du numérique. L'organisation et la réalisation des activités des personnes et celles des entreprises et institutions sont entièrement imprégnées de numérique. Cette révolution continue son développement au gré de l'évolution de nos besoins. Un des impacts majeurs de ces nouvelles technologies est la circulation d'un volume colossal de données dans le monde entier, par l'intermédiaire d'internet. Ces données ont une valeur économique qui serait estimée à un trillion par an en 2020, dans l'Union européenne[1]. Parmi ces informations, les données à caractère personnel[2] font l'objet d'une protection spécifique afin de protéger la vie privée de la personne[3]. Les données concernant la santé[4][5] constituent une catégorie particulière de données à caractère personnel. Issues de l'imagerie, de la génomique, des forums patients, des objets connectés… elles constituent un réservoir immense présentant un potentiel d'exploitation particulièrement intéressant pour les industriels du domaine de la santé.

L'évaluation des produits de santé était, il y a peu, réalisée principalement avant la mise sur le marché de ces produits, et les entreprises de santé utilisaient uniquement les données qu'elles produisaient elles-mêmes directement ou indirectement dans le cadre d'expérimentations ou des données relatives aux activités de vigilance, fournies, en majeure partie, par les autorités de santé. Aujourd'hui les obligations de suivi des produits de santé après leur mise sur le marché[6], afin de mieux évaluer leur efficacité, leur sécurité, d'optimiser leur bon usage et de réguler leur impact économique, impliquent l'obtention de données sur l'utilisation de ces produits en situation réelle. Ces données peuvent provenir d'un recueil, organisé ou non, d'informations circulant sur le web. Les réseaux sociaux peuvent être utilisés comme outil en épidémiologie pour suivre une pathologie ou une action de prévention ; en pharmacovigilance[7] pour recueillir des effets indésirables ; dans le cadre d'essais cliniques pour effectuer le recrutement de patients. Les forums de patients fournissent un volume important de données sur la pratique réelle. Des plateformes sont développées pour mettre en relation des patients, des professionnels de santé et des industriels dans l'objectif de réaliser des enquêtes[8]. Les autorités compétentes, les organismes de sécurité sociale peuvent aussi être à l'origine

---

[1] « *According to some estimates, the value of European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020.* » Reding V. dans « *Progress on EU data protection reform now irreversible following European Parliament vote*», http://europa.eu/rapid/press-release_MEMO-14-186_fr.htm, memo de la Commission européenne, Strasbourg, le 12 mars 2014

[2] Selon 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) : « *données à caractère personnel : 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, par exemple un nom,*** *un numéro d'identification****, des données de localisation, ou un identifiant en ligne****, ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.* », Document 9565/15, 11 juin 2015, article 4, 1), p 77. En gras, les modifications apportées par la proposition à la définition en vigueur (directive 95/46/CE) .

[3] La protection des données à caractère personnel a une relation évidente avec le droit à la vie privée : CJUE, 17 oct. 2013, aff. C-291/12, Schwarz, pts 24, 25, 27, 29, 30.

[4] « *Données concernant la santé: toute donnée relative à la santé physique ou mentale d'une personne physique qui révèle des informations sur l'état de santé de ladite personne* », Proposition de règlement du Parlement et du Conseil (op. cit.) article 4, 12), p 79.

[5] « *...l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, paragraphe 1, de la directive 95/46.* » CJCE, 6 novembre 2003 n° C-101/01

[6] Directive 2001/83 du Parlement et du Conseil instituant un code communautaire relatif aux médicaments à usage humain modifiée, article 21bis, b), article 22bis a) et b)

[7] Les titulaires d'autorisation de mise sur le marché (AMM) de médicament, doivent effectuer régulièrement une surveillance des informations relatives à leurs médicaments sur internet : Guideline on good pharmacovigilance practices (GVP), Module VI : « Management and reporting of adverse reactions to medicinal products », EMA/873138/2011, Rev 1, 8 septembre 2014, p10

[8] Ainsi la plateforme Carenity réalise des études pour le compte d'industriels, voir « *Des patients collaborateurs de recherche*», Pharmaceutiques n°228, juin/juillet 2015, p 53

de la collecte de données concernant la santé, tout comme les établissements de santé et les établissements médico-sociaux. Certains établissements de santé se lancent dans une gestion « Data driven » qui permet une analyse en temps réel de différentes données : économiques, commerciales juridiques, financières, … et de santé, notamment de données recueillies au lit du patient dans le but d'anticiper au maximum la prise de décisions pour guérir ou prévenir une pathologie[9]. Ce gigantesque gisement de données de santé, qui deviennent techniquement exploitables, bouleverse totalement le mode de fonctionnement des industriels de la santé ; certains parlent de « *nouveau modèle pharmaceutique* »[10]. Les industriels et les institutions de santé se doivent d'entrer dans une démarche Big Data. Grâce à cette démarche, un volume très important de données issues de sources différentes sont gérées quasiment en temps réel. Les Big Data permettent d'analyser à grande échelle, l'état de santé des populations et les besoins en matière de produits de santé et également, de surveiller l'impact de ces produits, en terme de sécurité, d'efficacité, d'économie et de bon usage, sur les populations et individuellement sur les personnes. Les principales caractéristiques du Big Data sont le volume et l'hétérogénéité des données, mais également la vélocité : la rapidité avec laquelle on peut générer, délivrer, stocker, enlever ou effacer des données. Cette vélocité constitue l'intérêt principal des nouvelles technologies développées dans l'exploitation des données massives. La possibilité d'une analyse quasi-instantanée d'un volume colossal de données est un élément déterminant à prendre en compte dans la protection de la vie privée des personnes.

Au sein de l'Union européenne, de grands principes protègent les personnes au regard de l'utilisation des données à caractère personnel. Une réforme a été engagée afin de mettre en adéquation notre encadrement juridique avec les avancées techniques du numérique et d'harmoniser les législations des états membres pour assurer la libre circulation des données. L'enjeu majeur de cette réforme est de protéger la vie privée des personnes, tout en assurant la compétitivité de l'Union européenne au niveau mondial. La Charte des droits fondamentaux de l'Union européenne consacre le droit fondamental à la vie privée et à la protection des données personnelles[11]. Le droit à la protection des données à caractère personnel est affirmé à l'article 16 du Traité sur le fonctionnement de l'Union européenne[12]. L'Union européenne a adopté une stratégie pour un marché unique numérique[13]. L'objectif est de remplacer les législations des 28 états membres par un seul encadrement. Les textes européens s'appliqueront également aux entreprises des pays tiers qui fournissent des services au sein de l'Union européenne. La directive 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[14] adoptée à une époque où internet était très peu répandu devrait être abrogée par un règlement actuellement en voie de

[9] Par exemple, l'hôpital des enfants malades de Toronto a adopté un système de monitoring permanent des signes vitaux au lit des patients à risque d'infection nosocomiale mortelle, qui permet une détection précoce de signes potentiels d'infection. Ce système anticipe d'au moins 24 heures le diagnostic d'atteinte infectieuse, ce qui permet d'initier le traitement plus tôt et donc d'obtenir un meilleur pronostic pour les patients.

[10] Observation d'Arnaud Laferté (Sté Roland Bergé), dans Badina Juliette « *Pharma/GAFA, la guerre n'est pas (encore) déclarée* », Pharmaceutiques, n°228, juin/juillet 2015, p37

[11] Charte des droits fondamentaux de l'Union européenne, journal officiel des communautés européennes, n° C364 , 18 décembre 2000, p. 1-22 : Article 7 : « *Respect de la vie privée et familiale : Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* » ; Article 8 : « *Protection des données à caractère personnel, 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.* »

[12] Article 16, Traité sur le fonctionnement de l'Union Européenne (ex-art. 286 TCE) : « *1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes* », Journal officiel de l'Union européenne n° C 326 du 26 octobre 2012, p. 47–390

[13] Communiqué de presse de la Commission européenne, « *Un marché unique numérique pour l'Europe : la Commission définit 16 initiatives pour en faire une réalité* », Bruxelles, 6 mai 2015

[14] Directive 95/46/CE du Parlement 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 de communautés européennes, L281, 23 novembre 1995, p. 31

finalisation. L'objectif de ce règlement est de renforcer la protection des individus, tout en facilitant le flux des données au sein du marché du numérique, afin de préserver la compétitivité mondiale de l'Union européenne. Une proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement[15] des données à caractère personnel et à la libre circulation de ces données a été adoptée le 25 janvier 2012 par la Commission européenne[16]. Cette proposition a reçu l'approbation de principe du Conseil en juin 2015. Parlement, Conseil et Commission sont entrés en discussion pour l'ultime étape de finalisation de ce texte. La réforme tant attendue ne devrait plus tarder à voir le jour. Une période transitoire de deux ans durant laquelle les acteurs devront se mettre en conformité, est prévue dans la proposition. Au sein de l'ensemble des dispositions destinées à mieux protéger la personne physique, nous nous pencherons sur deux aspects importants de cette réforme : le consentement (I) et l'information, au sens large, de la personne concernée (II). Ces deux points nous semblent capitaux, puisque le malade, du statut de « patient » est devenu progressivement acteur du système de santé et collaborateur de la recherche, il doit donc être en mesure de veiller lui-même, à sa protection et notamment au respect de sa vie privée. Le nouvel encadrement relatif à la protection des données personnelles aménage-t-il une autonomie de la personne concernée sur la protection des données à caractère personnel ?

I) LE CONSENTEMENT DE LA PERSONNE CONCERNEE, UNE PROTECTION SUBSIDIAIRE :

Le recueil du consentement de la personne concernée pourrait être un principe général du traitement des données à caractère personnel et dans ce cas, par son accord, la personne concernée aurait la maîtrise totale de l'utilisation de toute information relative à sa personne. Le consentement serait alors la première des protections de la personne. Or la réforme de l'Union européenne précise les modalités d'obtention du consentement (2), mais ne lui confère pas pour autant une valeur de principe général (1).

1) Le consentement, une condition de licéité secondaire :

Les données concernant la santé font partie d'une catégorie particulière de données à caractère personnel : les données dites sensibles car leur traitement peut entrainer des risques importants pour les droits et libertés fondamentaux. Cette catégorie comprend, outre les données concernant la santé, les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion, les convictions philosophiques ou l'appartenance syndicale, les données génétiques[17] et les données concernant la vie sexuelle[18]. Le principe est l'interdiction du traitement de cette catégorie de données à caractère personnel.

Toutefois, le Droit de l'Union européenne prévoit des dérogations qui correspondent à des motifs légitimes définis[19,20]. Ces motifs énoncés dans la directive 95/46/CE et dans la proposition de règlement ne peuvent être rendus plus restreints par l'adoption de mesures nationales : « *Dans ces*

[15] Remarque : la définition du traitement de données à caractère personnel (voir article 4, 3) de la proposition 9565/15 op. cit. et article 2 b) de la directive 95/46/CE) a été modifiée de manière à prendre en compte de nouvelles techniques : la structuration et la limitation des données. La structuration est un élément essentiel du Big Data puisque les données proviennent de sources différentes. La limitation est un marquage de données qui permet de limiter leur traitement.

[16] Proposition de règlement de la Commission 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, 2012/00011

[17] La proposition de règlement ajoute dans cette catégorie, les données génétiques.

[18] Article 9 proposition de règlement (op. cit.) et article 8 directive 95/46/CE

[19] Article 8 directive 95/46/CE et article 9 proposition de règlement (op. cit.)

[20] Les états membres ne peuvent pas ajouter d'autres motifs légitimes : « *l'article 7, sous f), de la directive 95/46 doit être interprété en ce sens qu'il s'oppose à une réglementation nationale qui, en l'absence du consentement de la personne concernée et pour autoriser le traitement de ses données à caractère personnel nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable de ce traitement ou par le ou les tiers auxquels ces données sont communiquées, exige, outre le respect des droits et libertés fondamentaux de cette dernière, que lesdites données figurent dans des sources accessibles au public, excluant ainsi de façon catégorique et généralisée tout traitement de données ne figurant pas dans de telles sources* », CJCE 24 novembre 2011, affaires jointes C-468/10 et C-469/10 point 49

conditions s'il est possible aux Etats membres d'apporter lors de la transposition des précisions, il ne leur est pas permis d'imposer des conditions supplémentaires »[21]. En effet, « *Les mesures prises par les Etats membres pour assurer la protection des données à caractère personnel doivent être conformes tant aux dispositions de la directive n° 95-46 qu'à son objectif consistant à maintenir un équilibre entre la libre circulation des données à caractère personnel et la protection de la vie privée* »[22].

La proposition de règlement, vient ajouter comme motifs légitimes de dérogation au principe d'interdiction de traitement des données sensibles, « *l'intérêt public dans le domaine de la santé publique* » ainsi que « *la nécessité, à des fins scientifiques* » d'effectuer le traitement des données concernant la santé. Ces deux motifs légitimes sont conditionnés à l'obligation de prévoir des dispositions qui assurent le respect des droits et libertés de la personne concernée. Les exemples d'intérêt de santé publique cités dans le texte sont : *la protection contre les menaces sanitaires graves transfrontières et le respect de normes élevées de qualité et de sécurité des soins de santé, des médicaments et des dispositifs médicaux*. Ce qui implique que dans ces conditions, le responsable du traitement pourra s'exonérer du recueil du consentement des personnes concernées. Il est évident que les activités de développement des produits de santé réalisées par les entreprises ne rentreront pas dans ce motif légitime, puisque leur but est la mise sur le marché de leurs produits et non le respect des normes ; même si la commercialisation passe par la démonstration d'un rapport bénéfice sur risques favorable. C'est l'intérêt public qui motive la dérogation. Les dérogations à ce principe d'interdiction de traitement ont toutes, en filigrane, une notion d'intérêt supérieur qui impose que les données soient utilisées pour le bien de la nation ou des individus : *sauvegarde d'intérêts vitaux, mission d'intérêt public ou relevant de l'exercice de l'autorité publique, archivage dans l'intérêt public, à des fins historiques, statistiques ou scientifiques* et spécifiquement pour les données concernant la santé : *obligations en matière de droit du travail, de la sécurité et de la protection sociale, constatation , exercice ou défense d'un droit en justice*. En l'absence de motifs légitimes prévus dans la liste limitative du Droit de l'Union européenne, le traitement de données sensibles ne sera possible, que si la personne concernée a donné son consentement explicite[23].

Le texte de la directive comme de la proposition de règlement, n'établit pas un principe général de consentement au traitement des données personnelles assorti de dérogations correspondant à la poursuite d'intérêts supérieurs. L'obligation du consentement est une condition de licéité placée parmi l'ensemble des dérogations au principe d'interdiction de traitement. Bien que ne laissant aucune place à l'autonomie de la personne concernée, le principe général d'interdiction semble plus fortement protéger cette personne, mais il perd de sa force par l'existence de nombreuses dérogations rendant possible le traitement des données sans exigence de consentement. Cette faiblesse de l'obligation de consentement est encore plus accentuée concernant la protection des données personnelles qui ne sont pas des données sensibles par la dérogation : « *les intérêts légitimes poursuivis par le responsable du traitement* »[24]. Qualifiée de « *véritable cheval de Troie* »[25], cette notion, non définie, d' « intérêts légitimes » laisserait porte ouverte à toutes sortes de justifications de la part du responsable du traitement, pour échapper au recueil du consentement de la personne. La proposition de règlement reconnaît même la finalité de marketing direct comme pouvant constituer un intérêt légitime[26].

Nous constatons que les dérogations au principe d'interdiction de traitement des données concernant la santé sont plus nombreuses que les conditions de licéité du traitement des données à caractère personnel. Les données sensibles seraient–elles moins protégées que les données à caractère

---

[21] CJUE 24 nov. 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF),* (C-468/10), *Federación de Comercio Electrónico y Marketing Directo (FECEMD)* (C-469/10) *c/ Administración del Estado, note* Benoît-Rohmer F.*,* RTD Eur. 2012 p. 406

[22] Arrêt CJCE du 6 nov. 2003, *Lindqvist*, C-101/01, point 79, D. 2004, p. 1062 Notons que la proposition de règlement dans son point 5 de l'article 9, affirme la possibilité d'opter pour de nouvelles conditions dans le cadre des données de santé notamment des données génétiques.

[23] Directive 95/46/CE du Parlement 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, considérant n°33

[24] Article 6 point 1, f de la proposition de règlement (op. cit.)

[25] Martial-Braz N., Rochfeld J., Gattone E. « Quel avenir pour la protection des données à caractère personnel en Europe ? », Recueil Dalloz 2013 p. 2788

[26] Considérant 39 in fine de la proposition de règlement

personnel ? Si l'on s'en tient au nombre de dérogations possibles, effectivement une réponse positive s'impose. Mais si ces dérogations sont plus nombreuses pour les données sensibles, elles sont aussi plus restrictives ; ce qui est plus protecteur pour la personne. La dérogation portant sur l'obligation légale du responsable du traitement de données sensibles est réduite à certaines situations, avec comme condition de garantir les droits de la personne concernée. Et l'exception pour sauvegarde des intérêts vitaux ne vaut que si la personne concernée est dans l'incapacité de donner son consentement. Le consentement est une des conditions de licéité parmi d'autres de traitement des données. Ces conditions étant, bien entendu, plus restrictives pour les données sensibles.

Le droit à la protection des données n'est pas une prérogative absolue. Ce droit doit être mis en balance avec d'autres droits. Il n'est donc pas étonnant que le consentement de la personne n'ait pas une valeur de principe. Si cela était le cas, le consentement de la personne pourrait faire obstacle au respect de dispositions de valeur supérieure ou, équivalente alors même que les droits de cette personne seraient respectés. Cependant le droit à la protection des données personnelles a une valeur juridique supérieure à une simple obligation légale du responsable du traitement ou, bien souvent, à un motif d' « *intérêts légitimes pour le responsable du traitement* ». Aussi cette dérogation pour intérêts légitimes est assortie de la condition de ne pas porter atteinte aux intérêts ou aux libertés et droits fondamentaux de la personne. Alors que la finalité de respect d'une obligation légale n'est mise en balance avec aucun de ces droits. Toutefois concernant les données sensibles, cette finalité n'est possible, que dans les domaines du droit du travail, de la sécurité et de la protection sociale, avec comme condition de garantir les droits de la personne concernée. De plus, la proposition de règlement ouvre la possibilité aux États membres et à l'Union européenne, pour les données sensibles, de prévoir des cas d'interdiction absolue de traitement[27]. Dans ces cas, le consentement explicite de la personne concernée ne pourra lever l'interdiction.

Le législateur se doit d'établir un équilibre entre différents droits avant d'accorder une place au consentement de la personne. Dans cet exercice d'équilibriste le respect de la hiérarchie des normes semble délicat. Le Droit de l'Union européenne affirme un principe général d'interdiction du traitement des données sensibles assorti de dérogations légales qui ne sont pas subordonnées à la condition de consentement pour ne pas entraver le respect des droits motivant les dérogations. Le consentement n'est qu'une dérogation supplémentaire à ce principe et ne peut faire obstacle à un traitement des données pour motifs légitimes. La personne peut donc exercer son droit à la protection des données que dans des situations dans lesquelles le législateur n'a pas fait prévaloir un autre droit.

La réforme de l'Union européenne tend à donner plus de valeur au consentement en encadrant ses modalités d'obtention.

2) Des modalités de consentement mieux définies :

Alors que la directive de 95 ne s'attardait pas sur les modalités de recueil du consentement, la proposition de règlement, apporte des précisions, dans l'objectif de faire obstacle aux façons équivoques de recevoir le consentement : après une information peu claire, de manière très expéditive, simplement en cochant une case, voire de manière tacite. Ces modes douteux d'obtention du consentement pourraient entacher sa validité. Pour être valable, le consentement au traitement des données à caractère personnel doit être une manifestation de volonté libre, spécifique, informée[28] et, selon la proposition de règlement de la Commission, « *sans ambiguïté* ».

Le consentement doit être libre, donc exempt de toute contrainte, pression, ruse ou violence. La personne doit pouvoir refuser sans subir de préjudice. Notamment, les liens entre le responsable du traitement des données et la personne concernée, ne doivent pas entacher le libre choix de cette

[27] Article 9 point 2 a) de la proposition de règlement
[28] Directive 95/46/CE article 2, h) et proposition de règlement (op. cit.)article 4, 8)

dernière. Le consentement ne doit pas, non plus, être une condition de l'exécution d'un contrat si le traitement des données n'est pas nécessaire à l'exécution du contrat. Nombreux encore sont les sites qui n'offrent pas leurs services, lorsque la personne a refusé le recueil de données qui seront utilisées pour suivre les habitudes des internautes.

Le consentement doit être spécifique, c'est à dire donné pour une finalité ou plusieurs finalités de traitement déterminées et explicites[29]. La personne doit être clairement informée de cette ou ces finalités. Le consentement donné est valable pour toutes les activités de traitement ayant la même finalité. Tout changement de finalité doit faire l'objet d'une information nouvelle et d'un recueil du consentement spécifique à cette nouvelle finalité.

Il arrive dans le cadre de recherches scientifiques, que les données soient conservées pour faire l'objet de recherches secondaires dans le même domaine que la recherche pour laquelle les données ont été collectées initialement (même pathologie par exemple). Même si, au moment où l'on décide de conserver les données, la ou les finalités des études ultérieures ne sont pas encore totalement précisées, on admet que le consentement initial est valable dès lors que la personne est informée du domaine de la recherche qui s'effectuera dans le respect des principes éthiques reconnus.

Avec l'avènement du Big Data, les cas de réutilisation de données collectées se multiplient. La réutilisation des données à caractère personnel est une nouvelle utilisation de ces données, dans une ou des finalités différentes de la finalité du traitement initial. Elle peut être le fait du responsable du traitement initial des données à caractère personnel qui, a posteriori, décide de faire une nouvelle analyse dans un but différent. Mais les données peuvent aussi circuler d'un acteur à un autre qui va les utiliser à ses propres fins. En effet, les données sont source d'acquisition de nouvelles connaissances ; elles ont un intérêt stratégique et économique. Elles ont donc acquis une valeur marchande. Les acteurs peuvent se procurer des données de différentes sources, ils peuvent également céder leurs données. La réutilisation des données se développe de plus en plus, du fait de ces échanges.

La réutilisation des données à caractère personnel est une situation délicate vis à vis de la protection des personnes. Elle présente un risque de détournement des données dont la personne concernée pourrait ne pas être informée et auquel elle pourrait ne pas avoir consenti. Aussi le droit de l'Union européenne prévoit un encadrement spécifique de cette situation. Le traitement ultérieur des données ne doit pas être incompatible avec les finalités initiales[30]. S'il y a « compatibilité » du traitement ultérieur avec les finalités initiales de collecte des données, cette compatibilité exonère le responsable du traitement ultérieur, de l'information sur les nouvelles finalités et du recueil du consentement de la personne concernée. La vérification de compatibilité, doit être réalisée par le responsable du traitement ultérieur. Pour ce faire, la proposition de règlement, énonce de manière non exhaustive, quelques indices à évaluer[31]. Dans son appréciation, le responsable du traitement peut « *tenir compte entre autres, de l'existence d'un lien entre les finalités du traitement initial et celles du traitement ultérieur, du contexte dans lequel les données ont été collectées, y compris les attentes raisonnables de la personne concernée quant à leur utilisation ultérieure, de la nature des données à caractère personnel, des conséquences pour les personnes concernées du traitement ultérieur envisagé et de l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement envisagé* »[32].

En l'absence de compatibilité, il faudra que le traitement ultérieur des données respecte les conditions de licéité, c'est à dire soit le consentement de la personne concernée est obtenu, soit le traitement ultérieur est fondé sur un des motifs légitimes définis à l'article 8 de la directive 95/46/CE (ou article 9 proposition de règlement). Une autre possibilité consiste à procéder avant communication des données à leur anonymisation, dès lors que la personne à laquelle les informations se rapportent ne peut plus être identifiée, les informations ne comportent plus de données à caractère personnel. Le traitement ultérieur des données à caractère personnel à des fins d'archivage dans l'intérêt public, à des fins statistiques, scientifiques ou historiques ou en vue d'un règlement futur des litiges est considéré comme compatible.

[29] Proposition de règlement (op. cit.), article 5 point 1 b) et directive 95/46/CE article 6 point 1 b)
[30] Proposition de règlement (op. cit.), article 5 point 1 b) et directive 95/46/CE article 6 point 1 b)
[31] Proposition de règlement (op. cit.), article 6 point 3 bis
[32] Considérant n°40 de la proposition de règlement (op. cit.)

Actuellement la réutilisation des données issues d'organismes public est souvent évoquée. Dans le domaine de la santé, les données des organismes de protection sociale sont riches en informations sur les soins et produits de santé. La France est dans une démarche d'ouverture de l'accès aux données recueillies par Système national d'information inter-régimes de l'Assurance maladie. Les données rendant l'identification possible pourront être utilisées sur autorisation de l'autorité de contrôle à des fins de recherche ou d'étude pour l'accomplissement de missions poursuivant un motif d'intérêt public uniquement, ce qui exclut une utilisation à des fins commerciales[33]

Le consentement doit être « sans ambiguïté ». La forme du consentement est essentielle pour déterminer si le consentement est donné sans ambiguïté. La personne peut consentir par écrit, oralement ou par un « *acte positif univoque* »[34]. Pour les données sensibles le consentement doit être explicite[35]. Le consentement tacite est prohibé, tout comme le consentement passif . La personne devra exprimer sa volonté par un acte : signer, cocher une case…Le consentement au traitement des données doit être, le cas échéant, bien distingué d'autres consentements délivrés dans le même temps[36]. La charge de la preuve du consentement revient au responsable du traitement des données. Ce dernier a donc tout intérêt à rédiger un formulaire d'attestation de consentement qui devra être signé par la personne concernée.

La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement initialement donné. La personne concernée est informée de son droit de retrait, avant de donner son consentement[37].

Face à des comportements douteux, le consentement de la personne concernée n'est pas toujours garant d'une protection efficace des droits et libertés de la personne. Aussi le principe général d'interdiction de traitement est certainement la solution qui convient le mieux aux pratiques actuelles du numérique. Toutefois, l'encadrement des modalités de consentement vont permettre de renforcer la valeur du consentement et également de développer les pouvoirs de la personne concernée, face à des acteurs qui jouent parfois sur l'opacité induite par les nouvelles techniques. La subjectivation des droits de chacun sur ses données implique une autonomisation qui passe aussi par l'éducation des personnes et par leur information.

II) UNE INFORMATION COMPLETE MAIS TARDIVE :

Une information adéquate sur le traitement des données à caractère personnel, ainsi que sur les droits de la personne concernée est essentielle à la protection subjective des données personnelles. Grâce à ces informations, la personne pourra elle-même prendre les décisions nécessaires pour prévenir ou de faire cesser une atteinte. La proposition de règlement développe les obligations d'information et de communications[38] qui incombent au responsable du traitement des données à caractère personnel et prévoit des sanctions *« effectives, proportionnées et dissuasives »*[39] en cas de non-respect de ces obligations. Ces obligations d'information et de communications sont l'élément principal du principe de transparence.

---

[33] L'accès sera restreint, encadré et payant par redevance. Les données agrégées et anonymisées ne contenant ni le nom des patients, ni leur adresse ou leur numéro de sécurité sociale seront accessibles à tous, gratuitement et sans restriction. Auparavant, l'accès à ces données n'était possible que pour des organismes à but non lucratif inscrits sur une liste. L'École polytechnique et la Caisse nationale de l'assurance maladie des travailleurs salariés ont signé fin 2014 une convention de partenariat de recherche et développement pour une durée de 3 ans**.** L'objectif est de favoriser le développement des technologies du big data appliqué au domaine de la santé, la détection de signaux faibles ou anomalies en pharmaco-épidémiologie, l'identification de facteurs utiles à l'analyse des parcours de soins, la lutte contre les abus et la fraude.

[34] Considérant n° 25 de la proposition de règlement (op. cit.)

[35] Article 9 point 2 a)de la proposition de règlement et article 8 point 2 a) de la directive 95/46/CE

[36] Article 7 point 2 de la proposition de règlement

[37] Article 7 point 3 de la proposition de règlement

[38] Nous parlerons d'information au sens large pour l'information et les communications

[39] Article 79ter de la proposition de règlement

La proposition de règlement qualifie l'information à fournir et précise son contenu. Toute information doit être délivrée « *d'une façon compréhensible et facilement accessible, en des termes clairs et simples »*[40]. Le texte insiste sur la nécessité d'une information aisée à comprendre, voire même illustrée, notamment lorsqu'il s'agit d'enfants[41]. Les moyens et la forme de délivrance de l'information importent peu : écrit, oral ; voie électronique ou non. L'information doit être délivrée directement à la personne concernée. Le responsable du traitement doit s'assurer de l'identité de la personne qui demande une information[42]. Sur la délivrance de l'information à fournir, le Droit de l'Union européenne distingue selon que les données sont collectées ou non, auprès de la personne concernée. L'information est obligatoire si les données sont collectées auprès de la personne concernée. Dans le cas contraire, le responsable du traitement peut fournir les informations à cette dernière.

L'information doit être délivrée à la personne concernée, quel que soit le fondement de la licéité du traitement des données à caractère personnel, motif légitime ou consentement.

La proposition de règlement discerne entre les informations à délivrer avant le traitement des données et celles à communiquer au moment du traitement. Ce texte impose une information courte sur les points essentiels, avant l'obtention des données et une information plus complète, notamment sur les droits de la personne, lorsque les données personnelles sont en cours de traitement.

1) Une information préalable succincte :

L'information délivrée au préalable pourrait paraître sans intérêt au regard des droits de la personne qui ne s'exercent qu'une fois le traitement engagé, à l'exception du droit d'opposition. Cependant, lorsque le consentement est une condition de licéité du traitement, l'information devient alors capitale pour l'obtention d'un consentement valable.

Le droit de l'Union européenne[43] prévoit, qu'en cas de collecte des données directement auprès de la personne concernée, cette dernière doit recevoir une information seulement sur l'identité du responsable du traitement, le cas échéant, de son représentant, les coordonnées du délégué à la protection des données, les finalités du traitement et le fondement juridique du traitement. Lorsque les données n'ont pas été collectées auprès de la personne concernée, le contenu de l'information à délivrer est quasiment le même. La principale différence réside dans le fait que la délivrance de l'information n'est pas une obligation pour le responsable du traitement. En plus, cette personne sera informée des catégories de données concernées et de la source de provenance de ces données à caractère personnel, sauf s'il s'agit d'une source accessible au public. Toutefois, concernant la collecte indirecte de données, le législateur ne précise pas le moment de délivrance de l'information à la personne concernée. On peut supposer qu'une information initiale a déjà été délivrée par le responsable de traitement qui est à l'origine de la collecte des données et donc l'information par le responsable du traitement suivant revêt un caractère secondaire.

La personne concernée dispose ainsi des éléments essentiels qui devraient lui permettre, le cas échéant, de consentir au traitement et d'établir un contact avec le responsable du traitement pour avoir plus d'information ou exercer ses droits, si elle le souhaite. La concision de l'information permet une compréhension plus aisée, mais ne va pas dans le sens d'une autonomisation de la personne concernée.

Aucune information n'est délivrée au préalable sur les droits de la personne concernée. Cependant, les droits de la personne, conférés par le texte de la directive et la proposition de règlement, sont des droits qui s'exercent a posteriori : droit d'accès, de rectification, d'effacement, de limitation et de portabilité. Les données doivent être collectées pour que la personne y ait accès ou

[40] Article 12 point 1 de la proposition de règlement
[41] Considérant 52 de la proposition de règlement
[42] Considérant 52 de la proposition de règlement
[43] Article 10 Dir. 95/46/CE et article 14 de la proposition de règlement

demande une rectification… Aussi l'information avant le traitement des données peut sembler peu opérante. Seul, le droit d'opposition au traitement est un droit qui peut être exercé à tout moment. Le texte de la proposition impose que la personne concernée soit informée de ce droit au plus tard au début du traitement des données[44]. Le législateur précise que cette information doit être séparée de toute autre information. Ainsi ce droit revêt une importance particulière. Alors pourquoi ne pas imposer une information préalable de la personne concernée sur ce droit d'opposition. Cette dernière serait alors en mesure de faire obstacle au traitement de ses données et pourrait ainsi prévenir toute atteinte à sa vie privée. Le risque d'entrave à la libre circulation des données est faible compte tenu des conditions restrictives dans lesquelles ce droit peut être exercé[45]. On peut s'interroger sur l'intérêt d'une information a priori, si la personne ne peut agir avant le traitement des données par manque d'informations sur ses droits. On peut supposer qu'intentionnellement le législateur n'a pas voulu obscurcir encore plus la phase préalable au traitement, qui se déroule parfois très rapidement et passe malheureusement trop souvent inaperçue.

Par ailleurs, il nous semble capital de délivrer une information plus complète dans le cas où la personne doit consentir au traitement des données. On peut regretter que la proposition de règlement ne distingue pas entre l'information à délivrer au préalable, selon que le consentement de la personne est requis ou non. Pour consentir efficacement, la personne devrait pouvoir bénéficier d'une information lui permettant de déterminer si le traitement peut lui nuire ou non. Une information sur les destinataires des données, l'intention de transférer les données dans un pays tiers, l'existence d'une prise de décision automatisée comprenant un profilage, nous semble être déterminante pour cerner l'ampleur du traitement et aboutir à consentement éclairé. Cependant la proposition de règlement affirme que « *les finalités précises du traitement devraient être explicites et légitimes et déterminés lors de la collecte des données. Les données devraient être adéquates et pertinentes au regard des finalités* »[46]. Or ces précisions concernant les finalités et les données collectées s'adressent au responsable du traitement mais ne définissent pas le contenu de l'information à délivrer à la personne. Le principe de libre circulation des données et l'enjeu de compétitivité de l'Union européenne sont des éléments qui ont certainement prévalu dans la proposition de règlement de la Commission, qui écarte tout ce qui pourrait « *inutilement perturber l'utilisation du service* »[47].

L'information préalable est une information trop succincte pour permettre, le cas échéant, un consentement informé[48] et pour assurer un exercice efficace des droits conférés à la personne concernée par la directive. L'information au moment du traitement vient compléter cette dernière, dans un objectif de contrôle en continu, de la personne concernée sur le traitement en cours, des données personnelles.

2) Une information a posteriori impuissante :

Selon la proposition de règlement[49], *au moment de l'obtention des données*, la personne concernée doit recevoir d'autres informations nécessaires pour garantir un traitement équitable et transparent, compte tenu des circonstances spécifiques et du contexte du traitement des données. Ces autres informations doivent être, le cas échéant, les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, la volonté du responsable du traitement d'effectuer un transfert de données à

[44] Article 19 point 1 al. 2 et point 2 al. 2 de la proposition de règlement
[45] Voir article 19 de la proposition de règlement
[46] Considérant 30 de la proposition de règlement
[47] Considérant 25 de la proposition de règlement
[48] Voir référence 26
[49] Article 14 de la proposition de règlement

caractère personnel vers un destinataire d'un pays tiers ou d'une organisation internationale, des informations au sujet de l'autre ou des autres finalités prévues après la finalité initiale, l'existence d'une prise de décision automatisée comprenant un profilage et des informations concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée. A ce stade, la personne est informée de ses droits : droit d'accès, de rectification, d'effacement, de limitation du traitement, d'opposition au traitement, à la portabilité des données et également le droit d'introduire une réclamation auprès d'une autorité de contrôle. La personne concernée devra aussi être informée sur l'existence d'une exigence de fourniture de données, le cas échéant, de la nature de cette exigence : est-elle contractuelle ou règlementaire ; ainsi que sur les conséquences éventuelles de la non-fourniture de ces données.

Le responsable du traitement peut ne pas fournir les informations en cas d'impossibilité ou si cela demande des efforts disproportionnés par rapport aux effets attendus sur la protection de la personne sur lesquelles les données ont été indirectement collectées, ou bien lorsque les données doivent rester confidentielles conformément à la législation.

Le droit de l'Union européenne prévoit la possibilité de déroger à ces obligations du responsable du traitement, lorsque les données sont traitées à des fin scientifiques[50] ou bien dans l'objectif de satisfaire à des intérêts publics d'un Etat membre ou de l'Union européenne. En effet, ces obligations peuvent être limitées par l'adoption de mesures de Droit de l'Union ou de l'État membre nécessaires et proportionnées pour garantir un intérêt supérieur : sécurité nationale, défense nationale, sécurité publique ou bien « *pour sauvegarder d'autres objectifs importants d'intérêt public général…, notamment un intérêt économique ou financier important y compris dans les domaines de… la santé publique et de la sécurité sociale »*[51]. Ainsi, les Etats membres peuvent adopter des dispositions dérogatoires aux obligations des responsables de traitements de données concernant la santé, dans le cadre de la gestion de l'assurance maladie, à condition que la limitation apportée au respect de ces obligations, soit nécessaire et proportionnée à la sauvegarde de l'intérêt économique du système de protection sociale.

Le responsable du traitement doit également informer la personne concernée de toute action intervenue dans le cadre de l'exercice du droit de rectification, d'effacement, ou de limitation du traitement, ou d'opposition au traitement. Cette information doit être délivrée au plus tard dans un délai d'un mois après réception de la demande de rectification, effacement, limitation ou opposition de la part de la personne concernée. Ce délai peut être prolongé de deux mois si les demandes sont complexes ou nombreuses, dans ce cas la personne sera informée dans le délai d'un mois des raisons du report de la réponse[52].

Au-delà de l'obligation d'information, le responsable du traitement des données a l'obligation de communiquer[53], sur demande de la personne concernée, des informations supplémentaires. Le refus de communication d'informations de la part du responsable du traitement est possible, lorsque les demandes de la personne concernée sont manifestement infondées ou excessives. Dans ce cas, il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande[54].

A tout moment, la personne concernée a le droit de demander communication de ces informations au responsable du traitement. Elle peut également se faire communiquer la durée envisagée de conservation des données. Lorsque les données sont transférées à un pays tiers ou à une organisation internationale, en l'absence de décision de la Commission européenne certifiant un niveau de protection adéquat, la personne peut être informée des garanties apportées par le responsable du traitement ou son sous-traitant[55]. La personne concernée peut également être informée du fait que les données à caractère personnel la concernant sont, ou ne sont, pas traitées. Elle a un droit d'accès à ces données qui peuvent lui être adresser sous forme de copie, sauf si la communication de ces données porte atteinte aux droits de propriété intellectuelle relatifs au traitement des données.

[50] Article 83 de la proposition de règlement
[51] Article 21 de la proposition de règlement
[52] Article 12 point 2 de la proposition de règlement
[53] Nous évoquerons l'information au sens large qui comprend information et communication.
[54] Article 12 point 4 de la proposition de règlement
[55] Article 42 de la proposition de règlement

Toutes les informations sont fournies gratuitement[56] à l'exception de la copie des données qui peut faire l'objet d'un paiement[57]. En cas de non-respect de ses droits la personne concernée pourra introduire une réclamation auprès de l'autorité de contrôle dont elle relève[58]. Le Droit de l'Union européenne prévoit des sanctions, à l'encontre du responsable du traitement des données à caractère personnel qui ne respecte pas ses obligations (non-respect du délai de réponse, pas d'effacement des données, pas de délivrance de l'information, omission de notifier une violation…), notamment des amendes administratives financières qui peuvent aller jusqu'à 1 million d'euros[59] .

Ce texte met en place une véritable obligation de communication à la charge du responsable du traitement. Cette obligation de communication d'informations à tout moment, devrait permettre à la personne concernée de contrôler le traitement de ses données à caractère personnel qu'elle fournit et, le cas échéant, de stopper une atteinte à sa vie privée. Toutefois, l'évolution vers une démarche Big data dans laquelle les traitements de données sont réalisés dans des temps infimes, implique que cette information délivrée a posteriori n'est pas opérante pour prévenir une atteinte aux droits de la personne. Le Big Data est caractérisé par sa vélocité, la capacité d'analyser des données en temps réel. Nous sommes passés d'un système de stockage des données à une logique de flux de données. Le temps de collecte, distribution, stockage, exploitation et effacement d'une donnée peut être de l'ordre de la milliseconde. Ainsi à la seconde même où une donnée a été collectée, elle peut être diffusée et exploitée dans le monde entier, puis effacée. Dans ce contexte, les nouvelles technologies laissent peu de place à la protection de la personne concernée par l'exercice de ses droits a posteriori. Face à l'expansion de la circulation et de l'exploitation des données à caractère personnel et l'enjeu économique qu'elles représentent pour les entreprises, une éducation générale des personnes sur les risques inhérents au traitement des données personnelles et sur leurs droits relatifs à la protection de leur vie privée semble nécessaire. Un bon niveau de culture générale de la population sur le traitement des données personnelles et notamment sur leurs droits, rendrait plus efficace un éventuel exercice de ces droits par son anticipation. Le contenu de l'obligation d'information à la charge du responsable du traitement des données personnelles pourrait ainsi être centré sur les spécificités du traitement en question, ce qui diminuerait la durée de l'étape préalable d'information des personnes. Ainsi cette étape rapide ne constituerait pas un frein à la libre circulation des données. Allier compétitivité et protection des données personnelles est un enjeu de taille dans le contexte actuel.

Les dispositions prévues dans la proposition de règlement relatives au consentement et à l'information de la personne concernée, nous montrent que, le principe de libre circulation des données au sein de l'Union européenne et l'enjeu de compétitivité internationale ont souvent prévalu sur la subjectivation des droits relatifs à la protection des données personnelles. Cependant, face à la complexité des nouvelles technologies, l'autonomie de la personne n'est pas complètement envisageable. Aujourd'hui encore, peu de personnes ont une idée des données personnelles et des données de santé qui peuvent être recueillies sur les plateformes internet ou grâce aux objets connectés. Si l'utilisation des nouvelles technologies se répand rapidement, la compréhension de leurs mécanismes, du fait de leur rapidité d'évolution et de leur complexité, est peu accessible aux non-professionnels. Dans ce contexte, le consentement et l'information de la personne sont peu opérant quant à la protection des données personnelles. Les obligations d'information et de communications relèvent plus de la transparence que de la subjectivisation des droits. Aussi le législateur affirme un principe d'interdiction de traitement des données sensibles et parallèlement, impose de nombreuses obligations au responsable du traitement : analyses d'impact[60], protection par défaut[61], délégué à la

[56] Article 12 point 4 de la proposition de règlement
[57] Article 15 point 1ter de la proposition de règlement : « *À la demande et sans frais excessifs, le responsable du traitement fournit à la personne concernée une copie des données à caractère personnel faisant l'objet d'un traitement* »
[58] Article 73 de la proposition de règlement
[59] Article 79bis de la proposition de règlement
[60] Article 33 de la proposition de règlement
[61] Article 30 de la proposition de règlement

protection des données[62], obligation de communication des violations[63]. Dans un environnement technologique complexe et évolutif, la protection des données personnelles reste sous le contrôle du législateur et des autorités compétentes. Une éducation des personnes sur les techniques de traitement des données et sur leurs droits, serait un premier pas dans l'acquisition d'une autonomie sur la protection des données personnelles.

[62] Section 4 de la proposition de règlement
[63] Article 31 de la proposition de règlement