TITRE 16
L'impact du Règlement général sur la protection des données dans le secteur de la santé

Jean HERVEG et Jean-Marc VAN GYSEGHEM[1]

CHAPITRE 1. Les changements dans la mise en œuvre de la protection des données qui intéressent le secteur de la santé

SECTION 1. – L'articulation entre protection des données et secret professionnel

1. Un des problèmes qui a surgi, lors de la transposition en droit belge de la directive 95/46/CE 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 (ci-après « directive 95/46/CE »), était celui de savoir si les règles relatives à la protection des données modifiaient ou non les règles relatives au secret médical et, de manière plus large, au secret professionnel. Le principal enjeu de ce débat consistait à savoir si, dans ce nouveau contexte législatif, l'obtention du consentement d'une personne aux fins de légitimer, en tout ou en partie, le traitement de données à caractère personnel relatives à sa santé permettait, en outre, de libérer le praticien professionnel (devenu professionnel de la santé dans le RGPD)[2] de son obligation au secret auquel il était soumis en application de l'article 458 du Code pénal. En effet, dans une vision pénale classique,

[1] Directeurs de recherche, CRIDS, UNamur et avocats au barreau de Bruxelles.

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

il n'était pas admis que le patient puisse libérer le dépositaire de ses secrets sauf dans la mesure (pas nécessairement si limitée en toute hypothèse) de ce qui lui était reconnu dans la littérature et la jurisprudence, sans oublier les situations dans lesquelles la loi elle-même conférait un droit à la personne en ce sens. Cette question était d'autant plus délicate qu'elle s'inscrivait, en outre, dans un contexte de consécration des droits du patient tant au niveau national[3] qu'européen et international, et qui visait à lui donner plus de place dans la relation de soins de santé – ce qui pouvait comprendre la possibilité d'avoir la maîtrise du secret médical.

La réponse était évidente : la protection des données n'a jamais eu pour objectif de modifier les règles relatives au secret médical, que ce soit au niveau belge ou européen. En effet, la protection des données a pour vocation de protéger les individus face au développement des nouvelles technologies de l'information et de la communication ; en particulier, de les protéger contre les fichiers de données à caractère personnel et automatisé et qui les concernent, ainsi que de leur conférer de nouveaux droits à cet égard, et non de s'immiscer dans la règlementation de l'exercice des professions des soins de santé et des obligations qui incombent de ce chef aux professionnels de la santé. Deux arguments principaux soutenaient cette interprétation. D'abord, la directive elle-même faisait référence à l'existence des règles relatives au secret médical[4] sans pour autant prétendre les régir. Il ne pouvait qu'en être déduit que ces dernières existaient indépendamment de la protection des données. Ensuite, l'obligation de traiter licitement les données[5] a été interprétée comme incluant aussi l'obligation de se conformer aux règles particulières qui pouvaient régir le type de données en cause ce qui, dans notre cas, renvoyait au respect des règles relatives au secret médical[6]. Cette interprétation est-elle toujours valide avec l'entrée en vigueur du RGPD ?

---

[3] This work has been done with the financial support from the European Union's Horizon 2020 research and innovation program under Grant Agreements n° 688520 (TeSLA) & 730953 (Inspex) and in part by the Swiss Secretariat for Education, Research and Innovation (SERI) under Grant 16.0136 730953. La publication ne reflète que l'opinion de ses auteurs et la Commission européenne ne peut être tenue responsable de l'usage qui en serait fait.

Loi du 22 août 2002 relative aux droits du patient.

[4] Voy. le considérant n° 33 de la directive ainsi que l'art. 8.3.

[5] Art. 6.1. a), de la directive 95/46/CE.

[6] À ce sujet et en ce sens : J. Herveg, M.-N. Verhaegen et Y. Poullet, « Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique : les conditions d'une alliance entre informatique, vie privée et santé », *Rev. dr. santé*, 2002-2003/2, pp. 56-84 ; C. de Terwangne, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », in *Cabinets d'avocats et technologies de l'information : balises et enjeux*, Cahiers du CRID, n° 26, Bruxelles, Academia-Bruylant, 2005, p. 156.

2. Il faut tout d'abord noter que le RGPD poursuit le même objectif que la directive 95/46/CE, mais, simplement, sous une forme plus développée. De plus, tout comme la directive 95/46/CE, le RGPD se réfère aux règles relatives au secret médical sans donner une quelconque indication qu'il aurait vocation à les régir ou les modifier[7]. Bien au contraire, le RGPD prévoit que l'interdiction de traitement ne s'applique pas aux catégories particulières de données à caractère personnel (dont celles relatives à la santé) quand celles-ci sont traitées à des fins thérapeutiques par un professionnel de la santé soumis à une obligation de secret médical (conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents) ou sous sa responsabilité ou par une autre personne également soumise à une obligation de secret (conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents).

Si cet argument n'était pas suffisant, il faudrait rappeler la possibilité offerte par le RGPD aux États membres de maintenir ou d'introduire des conditions supplémentaires (en ce compris des limitations) en ce qui concerne le traitement des données génétiques, biométriques ou concernant la santé[8], ce qui est susceptible de couvrir la question du maintien ou de l'adoption de nouvelles règles relatives au secret médical.

Enfin, le RGPD prévoit explicitement que les États membres peuvent adopter des règles spécifiques afin de définir les pouvoirs des autorités de contrôle à l'égard des responsables du traitement ou des sous-traitants qui sont soumis, en vertu du droit de l'Union ou du droit d'un État membre ou de règles arrêtées par les organismes nationaux compétents, à une obligation de secret médical ou à d'autres obligations de secret équivalentes, lorsque cela est nécessaire et proportionné pour concilier le droit à la protection des données à caractère personnel et l'obligation de secret[9].

Il paraît donc évident que le RGPD n'a pas pour objectif ni pour effet de modifier les règles relatives au secret médical puisqu'il y fait référence en tant que règles qui lui sont extérieures et dont il reconnaît l'application éventuelle en matière de traitements de données à caractère personnel relatives à la santé dans un contexte thérapeutique.

---

[7] Voy. art. 9.3 du RGPD relatif au traitement portant sur des catégories particulières de données à caractère personnel.

[8] Art. 9.4 du RGPD.

[9] Voy. art. 90 du RGPD. Ces règles ne sont applicables qu'en ce qui concerne les données à caractère personnel que le responsable du traitement ou le sous-traitant a reçues ou a obtenues dans le cadre d'une activité couverte par ladite obligation de secret.

3. Il semble, dès lors, que la réponse à la question de l'articulation entre la protection des données et le secret médical doit demeurer identique : les deux corps de règles doivent cohabiter, ce qui signifie, concrètement, qu'il faut les appliquer de façon complémentaire – l'un ne dérogeant pas à l'autre[10] et ce, tant au niveau européen que national.

SECTION 2. – La notion de données à caractère personnel relatives à la santé

4. Ainsi que cela a déjà été mentionné dans la partie de l'ouvrage consacrée aux données de catégorie particulière ou « sensibles », selon la terminologie de la directive 95/46/CE, le RGPD définit les données à caractère personnel comme étant « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne »[11]. Pour mieux comprendre cette définition, il faut d'abord revenir sur l'évolution de la notion de données relatives à la santé dans le cadre de Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention n° 108) et de la Recommandation (97) 5 relative à la protection des données médicales[12], ainsi que dans le cadre de la directive 95/46/CE.

§ 1. La notion de données relatives à la santé dans la Convention n° 108 et dans la Recommandation (97) 5

5. La Convention n° 108 ne contient pas de définition explicite des données à caractère personnel relatives à la santé[13]. Il s'agit d'une caté-

[10] Ce qui signifie, notamment, que, dans la mesure pré-rappelée, on ne peut pas exciper des règles relatives au secret professionnel pour s'opposer au droit d'accès consacré par la protection des données.

[11] Voy. art. 4.15° du RGPD.

[12] Recommandation n° R (97) 5 relative à la protection des données médicales, adoptée le 13 février 1997 par le Comité des Ministres du Conseil de l'Europe lors de la 584e réunion des Délégués des Ministres.

[13] Son rapport explicatif indique que le Comité d'experts sur la protection des données aurait *soigneusement* étudié cette notion dans le contexte de ses travaux sur les banques de données médicales. Toutefois, formellement, cela ne ressort ni de la Recommandation n° R (81) 1 du Comité des Ministres aux États membres relative à la règlementation applicable aux banques de données médicales automatisées, adoptée le 23 janvier 1981 lors de la 328e réunion des Délégués des Ministres, ni de son annexe.

gorie particulière de données à caractère personnel dont le traitement est interdit sauf à ce que le droit interne prévoie des garanties appropriées. À lire le rapport explicatif joint à la Convention, la notion de *données à caractère personnel relatives à la santé* « (…) couvre les informations concernant la santé passée, actuelle et future, physique ou mentale d'un individu. Il peut s'agir d'informations sur un individu bien portant, malade ou décédé. Il est entendu que cette catégorie de données comprend également les informations relatives à l'abus d'alcool ou à la consommation de drogues »[14]. Mais, ni la Convention, ni son rapport explicatif, ne donnent d'indication sur ce qu'il faut entendre par *information*. Ils ne donnent pas plus d'explication sur ce qu'il faut entendre par la notion de *santé*.

6. De son côté, la Recommandation n° R (97) 5 définit les données médicales comme étant toutes les données à caractère personnel relatives à la santé d'une personne, les données ayant un lien manifeste et étroit avec la santé et les données génétiques[15]. La notion de données à caractère personnel est identique à celle contenue dans la Convention n° 108 ; il s'agit de toute information concernant une personne physique identifiée ou identifiable[16]. La distinction entre données *médicales* et *données relatives à la santé* appelle les observations suivantes.

D'abord, l'exposé des motifs de la Recommandation précise expressément que la notion de données médicales doit recevoir l'interprétation la plus large possible (et elle ne se restreint pas aux données relatives à l'état de santé). Cette précision devait s'entendre comme signifiant que la notion de dossier médical n'était pas suffisante pour délimiter le champ matériel de la Recommandation et que ce dernier ne se limitait pas non plus à la sphère dans laquelle une personne recevait des soins de la part d'un médecin[17]. À l'instar du rapport explicatif joint à la Convention, l'exposé des motifs rappelle que les données médicales concernent tant la santé passée, actuelle ou future de la personne concernée que sa santé

[14] Voy. considérant n° 45 du rapport explicatif de la Convention.

[15] Art. I de l'annexe. Les *données génétiques* sont « toutes les données, quel qu'en soit le type, qui concernent les caractères héréditaires d'un individu ou qui sont en rapport avec de tels caractères formant le patrimoine d'un groupe d'individus apparentés », ainsi que « toute donnée portant sur l'échange de toute information génétique (gènes) concernant un individu ou une lignée génétique, en rapport avec les aspects, quels qu'ils soient, de la santé ou d'une maladie, qu'elle constitue ou non un caractère identifiable ». « La lignée génétique est constituée par des similitudes génétiques résultant d'une procréation et partagées par deux ou plusieurs individus ».

[16] Art. I de l'annexe. Voy. aussi considérant n° 36 de l'exposé des motifs.

[17] Voy. considérant n° 37 et s. de l'exposé des motifs.

physique ou mentale[18]. Sur ce point, il y a convergence entre données médicales et données relatives à la santé.

Ensuite, l'exposé des motifs indique que la notion de *données ayant un lien manifeste et étroit avec la santé* vise les informations (à l'exception des éléments à caractère public) qui permettent de se faire aisément une idée de la situation médicale d'une personne, par exemple à des fins d'assurance, comme notamment le comportement de cette personne, sa vie sexuelle, sa manière de vivre, sa consommation de drogue, l'abus d'alcool et de tabac. Les termes *manifeste et étroit* ont été utilisés afin de viser des éléments qui ont une incidence certaine et directe sur la santé[19]. Il faut en déduire que ces informations ne sont pas des données relatives à la santé mais des données qui vont permettre d'apprendre quelque chose sur la santé d'une personne – elles vont permettre la *déduction* d'une information relative à la santé de la personne concernée (et qui est donc une *autre* information). L'intention manifeste du Conseil des Ministres était d'encadrer l'utilisation d'un certain nombre de données qui, en tant que telles, ne sont pas relatives à la santé, mais dont il peut être déduit des informations relatives à la santé d'une personne.

§ 2. La notion de données relatives à la santé dans la directive 95/46/CE

7. À l'instar de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, la directive 95/46/CE ne contient pas de définition de la notion de données relatives à la santé. Il s'agit aussi d'une catégorie particulière de données à caractère personnel dont le traitement est, en principe, interdit sauf exceptions[20].

8. La Cour de justice a eu l'occasion de se pencher sur la notion de données à caractère personnel relatives à la santé dans son arrêt du 6 novembre 2003[21]. Celui-ci concernait Mme Lindqvist, formatrice de communiants dans la paroisse d'Alseda (Suède), qui avait été poursuivie et condamnée pour avoir traité, de manière illégale, des informations sur certains de ses collègues de la paroisse et, notamment, avoir indiqué

[18] Voy. considérant n° 37 de l'exposé des motifs.

[19] Voy. considérant n° 38 de l'exposé des motifs.

[20] Voy. art. 8 de la directive 95/46/CE et la liste des hypothèses dans lesquelles cette interdiction ne s'applique pas.

[21] C.J.C.E, 6 novembre 2003, arrêt *Bodil Lindqvist*, aff. C-101/01, obs., C. DE TERWANGNE, « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », *R.D.T.I.*, 2004, pp. 67-99.

qu'une de ses collègues s'était blessée au pied et qu'elle était en congé de maladie partiel. La Cour, après avoir indiqué que la notion devait recevoir une interprétation large[22], a retenu que la donnée à caractère personnel relative à la santé était « toute information relative à tout aspect, tant physique que psychique, de la santé d'une personne ». Elle a jugé que l'indication du fait qu'une personne s'était blessée au pied et était en congé de maladie partiel constituait une donnée à caractère personnel relative à la santé[23]. Il n'est pas facile de savoir si la qualification retenue par la Cour à cet égard était le fruit de la présence de ces deux informations (la blessure et l'état de congé de maladie partiel) ou si chacune de ces informations prises séparément était suffisante à cet effet.

9. Dans son document de travail du 15 février 2007 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques[24], le groupe de travail de l'article 29 (Groupe 29 devenu Comité européen de protection des données dans le RGPD) expliquait, après avoir rappelé l'arrêt précité de la Cour de justice du 6 novembre 2003, que la définition des données à caractère personnel relatives à la santé s'appliquait également aux données à caractère personnel lorsqu'elles présentaient *un lien clair et étroit avec la description de l'état de santé d'une personne* et qu'en ce sens, les données sur la consommation de médicaments, d'alcool ou de drogue et les données génétiques sont incontestablement des « données à caractère personnel relatives à la santé », en particulier si elles sont consignées dans un dossier médical[25]. Ce faisant, le Groupe 29 ajoutait à la notion de données à caractère personnel relatives à la santé des données qui n'en sont pas mais qui, en raison *de leur lien clair et étroit avec la description de l'état de santé d'une personne*, devraient être soumises au même régime. Il eut été plus approprié de ne pas déformer la notion de données à caractère personnel relatives à la santé pour y inclure des informations qui n'en sont pas à la seule fin de les soumettre aux mêmes règles. En tout cas, ceci ne signifie pas que les données devraient présenter un lien clair et étroit avec la description de l'état de santé d'une personne pour être des données à caractère personnel relatives à la santé.

---

[22] Contrairement à une crainte qui avait pu naître de l'exposé des motifs de la loi belge procédant à la transposition de la directive 95/46/CE (voy. Th. Leonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution – La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999/20, n° 5928, n° 38).

[23] Considérant n° 51.

[24] Groupe 29, Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques, adopté le 15 février 2007, WP 131.

[25] Le lien avec la définition contenue dans la recommandation n° R (97) 5 relative à la protection des données médicales semble évident.

Le groupe de travail ajoutait que toute autre donnée (comme des données administratives (numéro de sécurité sociale, date d'admission à l'hôpital, etc.)) contenues dans les documents médicaux relatifs au traitement d'un patient devaient être considérées comme sensibles au motif que si elle n'était pas pertinente dans le cadre du traitement du patient, elle n'aurait pas été, et n'aurait pas dû être incluse dans un dossier médical. À son estime, toutes les données contenues dans les documents médicaux, les dossiers médicaux électroniques et les systèmes de DME (dossiers médicaux électroniques) sont à considérer comme des « données à caractère personnel sensibles ». En conséquence, toutes ces données sont soumises aux règles générales sur la protection des données à caractère personnel ainsi qu'aux règles spéciales en matière de protection des données relatives au traitement des informations sensibles. Ce faisant, le Groupe 29 réglait la question épineuse du régime à appliquer à un ensemble de données hétérogènes (données « ordinaires » mélangées avec des données « sensibles ») en choisissant d'appliquer le régime le plus strict à l'ensemble des données hétérogènes[26]. C'est en quelque sorte un effet de *contamination* du régime des données à caractère personnel relatives à la santé à des données qui leur seraient trop proches. Mais, il faut bien voir que strictement rien n'aurait empêché une application distributive des règles en fonction de la qualification à donner à chaque donnée considérée séparément : les règles générales s'appliqueraient aux « simples » données à caractère personnel et les règles « spéciales » aux données « sensibles ». Si cette solution n'est pas nécessairement facile à mettre en œuvre dans le cadre d'un fichier et, en particulier, dans le cas d'un dossier médical en papier, elle ne devrait, par contre, pas rencontrer de problème dans le cadre d'un traitement automatisé bien conçu dès l'origine conformément au principe du *privacy by design*.

Un peu plus tard, le groupe de travail a fait le point sur le concept de données à caractère personnel dans son avis du 20 juin 2007[27]. Il a ainsi mis en avant trois éléments : la notion d'information, la relation entre l'information et une personne (physique) et l'identification de cette dernière (la *personne concernée*). Ces éléments doivent aussi retenir notre attention dans la mesure où leur analyse peut être utile pour définir les données à caractère personnel relatives à la santé.

[26] C'est un problème habituel qui existe aussi, par exemple, en droit international privé lorsque plusieurs lois régissent une même situation mais que l'une d'entre elles est plus stricte que les autres.

[27] Groupe 29, Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007, WP 136.

a) La notion d'information

10. Le groupe de travail rappelle que la notion de *données à caractère personnel* vise toute sorte d'informations et pas seulement celle qui révèlerait la personnalité de la personne concernée ou qui relèverait de la notion plus restreinte d'information secrète, cachée, et sans qu'il soit requis d'opérer une distinction entre des activités publiques ou privées. Il s'agit d'opter pour la définition la plus large du concept de données à caractère personnel. En ce sens, elles englobent n'importe quelle information, sous n'importe quel format, alphabétique, numérique, graphique, photographique ou acoustique. Les sons et les images sont des données à caractère personnel dans la mesure où ils représentent des informations qui concernent une personne physique (identifiée ou identifiable).

11. Le groupe de travail indique que les données biométriques (comme les données ADN) peuvent remplir deux fonctions : soit contenir de l'information soit servir d'identificateur. Il ajoute que les prélèvements de sang (ou tout autre prélèvement de tissus ou cellules humains) ne sont pas des données biométriques mais constituent des sources d'information dont on peut extraire des données biométriques. Il s'ensuit que l'extraction d'informations concernant une personne physique identifiée ou identifiable à partir de ces prélèvements est assimilée à une collecte de données à caractère personnel.

b) La relation entre l'information et une personne physique

12. Pour être une donnée à caractère personnel, l'information doit *concerner* une personne physique. Le groupe de travail a mis en exergue trois éléments qui permettent de savoir si cette exigence est rencontrée : l'information doit présenter soit un élément de **contenu**, soit un élément de **finalité**, soit un élément de **résultat**, étant entendu que la présence d'un seul de ces critères suffit que l'information concerne une personne. Le critère de **contenu** est évident : le contenu de l'information concerne directement une personne ; il a *trait* à cette personne. Ainsi, les résultats d'une analyse médicale ont trait au patient en raison de leur contenu informationnel. C'est le résultat de l'analyse réalisée sur la personne. Le critère de **finalité** élargit le champ de la qualification au-delà du simple contenu informationnel. L'information concerne une personne parce que les données sont utilisées ou susceptibles d'être utilisées, compte tenu de l'ensemble des circonstances du cas d'espèce, afin d'évaluer, traiter d'une certaine manière ou influer sur le statut ou le comportement d'une personne. Ce n'est donc plus une relation informationnelle de contenu mais

une relation informationnelle d'utilisation effective. Le critère de **résultat** signifie que l'information concerne une personne parce que, même en l'absence de tout élément de *contenu* ou de *finalité*, son utilisation est susceptible d'avoir un impact sur certains droits ou intérêts de cette personne, compte tenu de l'ensemble des circonstances du cas d'espèce. Il convient de relever qu'il n'est pas nécessaire que le résultat potentiel ait un impact majeur. Il suffit qu'une personne puisse être traitée différemment par rapport à d'autres personnes à la suite du traitement de ces données[28]. Ce n'est donc ni une relation informationnelle de contenu, ni une relation informationnelle d'utilisation effective mais une relation informationnelle d'impact probable. Par ailleurs, il faut retenir qu'il existe des informations qui, ne fût-ce qu'en raison de leur contenu, sont hautement susceptibles de concerner plusieurs personnes à la fois. C'est le cas des données médicales et des données génétiques[29].

c) L'identification de la personne concernée

13. Pour qu'il y ait *donnée à caractère personnel*, la personne physique concernée par l'information faisant l'objet d'un traitement doit être *identifiée* ou *identifiable*. Le fait d'être ***identifié*** signifie que la personne est distinguée des autres membres du groupe auquel elle appartient. Le fait d'être ***identifiable*** signifie que la personne n'est pas encore identifiée mais qu'il est possible de le faire, que ce soit directement ou indirectement. À cet égard, l'identification s'opère normalement grâce à des ***identifiants*** (dont certains sont énumérés dans la définition de la donnée à caractère personnel retenue par la directive 95/46/CE). Comme le précise le groupe de travail, il peut s'agir de signes extérieurs concernant l'apparence de la personne comme sa taille, la couleur de ses cheveux, ses vêtements, etc., ou d'une caractéristique de la personne qui n'est pas immédiatement perceptible, comme une profession, une fonction, un nom, etc. Il peut aussi s'agir d'un numéro de téléphone, d'un numéro de plaque minéralogique, d'un numéro de sécurité sociale, d'un numéro de passeport, ou d'un un croisement de critères significatifs, qui permettent de reconnaître la personne à l'intérieur d'un petit groupe. Concrètement, c'est le contexte du cas d'espèce qui déterminera si certains identifiants sont suffisants pour permettre cette identification. Ainsi, un nom de famille très courant ne

[28] Voy. l'exemple des RFID : Groupe 29, Document de travail sur les questions de protection des données liées à la technologie RFID, adopté le 19 janvier 2005, WP 105, p. 9.

[29] J.-M. Van Gyseghem, « L'information génétique et le traitement de données à caractère personnel », in A.-M. Duguet, J. Herveg et I. Filippi (éd.), *Dossier Médical et Données Médicales de Santé : Protection de la confidentialité, conditions d'accès, échanges pour les soins et la recherche*, Bordeaux, Les éditions hospitalières, 2007, pp. 243-258.

sera pas suffisant pour identifier une personne (c'est-à-dire pour la distinguer des autres) dans l'ensemble de la population d'un pays, alors qu'il sera probablement suffisant pour identifier un élève dans une classe. La question de savoir si une personne à laquelle se rapportent les informations est identifiée ou pas, dépend dès lors des circonstances de chaque cas d'espèce.

Ceci étant, la possibilité que la personne concernée soit identifiable doit s'envisager de façon raisonnable. Autrement dit, pour déterminer si la personne concernée est identifiable, il faut prendre en considération l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par toute autre personne, pour réaliser cette identification[30]. À cet effet, il faut tenir compte de tous les facteurs à disposition pour réaliser cette identification, ce qui vise notamment :

- les coûts de l'identification ;
- la finalité visée (lorsque la finalité implique l'identification de personnes physiques[31]) ;
- la manière dont le traitement est structuré ;
- l'intérêt escompté par le responsable du traitement ;
- les intérêts en jeu pour les personnes ;
- les risques de dysfonctionnements organisationnels (par exemple violations du devoir de confidentialité) ;
- les défaillances techniques, etc.

Toutefois, le Groupe 29 considère que l'appréciation du caractère raisonnable doit tenir compte de l'état d'avancement technologique au moment du traitement, ce qui est évident, mais aussi des changements technologiques éventuels pendant la période pour laquelle les données seront traitées, ce qui l'est moins. Autrement dit, l'identification peut ne pas être raisonnablement possible aujourd'hui, mais, si les données sont destinées à être conservées pendant une longue durée, le responsable du traitement devrait envisager la possibilité qu'une identification puisse intervenir au cours de cette durée, ce qui en ferait à ce moment-là des données à caractère personnel. Il serait alors souhaitable que le système puisse s'adapter à ces développements et intégrer les mesures techniques et organisationnelles appropriées en temps utile. Cela ne signifie pas pour autant qu'il faille considérer que les données soient à caractère personnel

[30] Considérant n° 26 de la directive 95/46/CE.

[31] Le Groupe 29 considère qu'il s'agit d'un critère très important même s'il n'est pas certain que cette approche soit toujours logique.

dès le début. Le groupe de travail propose ensuite des exemples dont celui des clichés radiographiques et des données de recherche pharmaceutique.

14. Ainsi, le ***cliché radiographique*** d'une patiente a été publié dans un journal scientifique, associé au prénom de celle-ci, un prénom très rare. Le prénom de cette personne associée à la connaissance qu'avaient ses proches de l'affection dont elle souffrait rendaient cette personne identifiable à un certain nombre de personnes ; ce cliché radiographique entre alors dans la catégorie des données à caractère personnel.

15. À propos des ***données de recherche pharmaceutique***, l'hypothèse de travail est celle où les hôpitaux ou les médecins, à titre individuel, transfèrent des informations médicales concernant leurs patients à une société à des fins de recherche médicale. Aucun nom de patient n'est utilisé, mais seulement un numéro de série attribué de manière aléatoire à chacun des cas cliniques, afin d'assurer la cohérence et d'éviter toute confusion avec des informations concernant différents patients. Seuls les médecins, qui sont tenus au secret médical, sont en possession des noms de leurs patients. Les données ne contiennent aucune autre information susceptible de rendre les patients identifiables par recoupement. De plus, toutes les autres mesures ont été prises pour éviter que les personnes concernées puissent être identifiées ou deviennent identifiables, que ce soit sur le plan juridique, technique ou organisationnel. Dans ces circonstances, l'autorité chargée de la protection des données peut considérer qu'il n'existe aucun moyen, dans le cadre du traitement de données réalisé par la société pharmaceutique, susceptible d'être raisonnablement mis en œuvre pour identifier les personnes concernées.

Lorsque l'identification de la personne concernée ne figure pas dans la finalité du traitement, la mise en place des mesures techniques et organisationnelles pour prévenir l'identification peut être déterminante pour considérer que les personnes ne sont pas identifiables, compte tenu de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par toute autre personne, pour réaliser cette identification. L'ennui, c'est que selon la finalité, la donnée sera ou non à caractère personnel, ce qui n'est pas toujours très cohérent. Dans de tels cas, ce n'est plus par nature que la donnée est ou non à caractère personnel mais en fonction de son usage.

Par ailleurs, toute la question est de savoir si, avec les techniques actuelles, l'on peut encore garantir l'impossibilité d'identifier, sans mettre en œuvre des moyens déraisonnables, un individu à partir de données relatives à la santé. La question a toute sa pertinence compte-tenu, d'une part, de la multiplication de bases de données et, d'autre part, de

l'augmentation de la capacité technique d'interconnecter lesdites bases de données pour aboutir à une identification, somme toute, assez aisée de l'individu. Nous sommes donc en droit de mettre en doute la réelle impossibilité d'une telle identification par les sociétés pharmaceutiques.

16. La ***pseudonymisation*** est un traitement de données qui consiste à dissimuler l'identité de la personne concernée. L'objectif de ce traitement est de permettre la collecte de données supplémentaires relatives à cette même personne sans qu'il soit nécessaire de connaître son identité. C'est un aspect particulièrement important dans le contexte de la recherche et des statistiques. Elle peut s'effectuer de manière retraçable en utilisant soit des listes de correspondance des identités et de leurs pseudonymes, soit des algorithmes de cryptage à double sens pour la pseudonymisation. Les données pseudonymisées de manière retraçable sont des données à caractère personnel puisqu'il s'agit d'informations qui concernent des personnes physiques (indirectement) identifiables, les pseudonymes permettant d'établir une correspondance avec la personne concernée. L'efficacité de la procédure de pseudonymisation dépend d'un certain nombre de facteurs :

- le stade auquel on y recourt ;
- son niveau de sécurité en ce qui concerne la possibilité de retracer les informations ;
- l'importance de la population dans laquelle la personne est dissimulée ;
- la possibilité de rattacher des transactions ou des enregistrements individuels à une même personne, etc. ;
- les pseudonymes doivent faire l'objet d'un choix aléatoire et non prévisible ;
- la quantité de pseudonymes possible doit être assez grande pour que le même pseudonyme ne puisse jamais être choisi deux fois au hasard. Pour garantir un niveau de sécurité élevé, il importe que l'ensemble des pseudonymes potentiels soit au moins équivalent à l'éventail des valeurs des fonctions de hachage cryptographique sûres.

Par ailleurs, il est possible de dissimuler l'identité des personnes concernées de manière à rendre toute réidentification impossible, par exemple, grâce à un cryptage à sens unique dont il est actuellement toujours considéré qu'il génère des données anonymisées.

Les ***données codées*** sont un exemple classique de pseudonymisation. Les informations correspondent à des personnes physiques chacune reprise sous un code, la clé permettant d'établir une correspondance entre ce code et des identifiants courants de ces personnes physiques comme

le nom, la date de naissance, l'adresse, ces identifiants étant conservés séparément. Le codage est couramment utilisé dans les essais cliniques de médicaments. En général, l'investigateur collecte des données sur les résultats cliniques des participants qui sont identifiés chacun par un code. Le chercheur ne communique les informations à la société pharmaceutique ou à d'autres parties intéressées (les *promoteurs*) que sous forme codée. L'investigateur conserve séparément la clé permettant d'associer le code aux identifiants qui permettent d'identifier les participants, ce qui permet de mettre à jour ou de compléter les données collectées, de prévenir le participant de la survenance d'effets secondaires, d'un diagnostic ou de la possibilité d'un traitement médical pour améliorer son état de santé. Toute la question est de savoir si les données concernent des personnes identifiables.

Un premier critère à mettre en œuvre est celui de la finalité du traitement des données codées. En effet, à suivre le groupe de travail, si l'une des finalités est de permettre l'identification des participants, notamment pour l'un des motifs énoncés ci-avant, nous sommes en présence de données à caractère personnel. Le Groupe 29 note à cet égard que lorsque le promoteur a analysé les moyens destinés au traitement, qu'il a prévu les mesures organisationnelles et ses relations avec le chercheur qui détient la clé de manière telle que l'identification des personnes concernée *peut* non seulement intervenir, mais *doit* aussi intervenir dans certaines circonstances, il s'ensuit que l'identification des patients figure parmi les finalités et les moyens du traitement. Par voie de conséquence, dans ce cas de figure, les données codées constituent des informations concernant des personnes physiques identifiables par toutes les parties concernées par l'identification éventuelle, et sont soumises aux règles de protection des données. Mais le groupe de travail précise, à juste titre, que cela ne signifie pas pour autant que tout autre responsable du traitement des données qui traite le même ensemble de données codées doive être considéré comme traitant des données à caractère personnel, notamment lorsque le système spécifique dans lequel ces autres responsables du traitement des données codées opèrent, exclut expressément la réidentification et que des mesures techniques ont été prises à cet effet.

Le groupe de travail ajoute que, dans d'autres domaines de la recherche ou dans le cadre d'un même projet, il est possible que la réidentification de la personne concernée ait été exclue lors de la conception des protocoles et de la procédure, par exemple lorsqu'aucun aspect thérapeutique n'est concerné. Pour des raisons techniques ou autres, il peut toujours être possible de découvrir à quelles personnes correspondent telles données cliniques, mais cette identification n'est en aucun cas censée se produire ou escomptée, et des mesures techniques appropriées (par exemple cryptographie,

hachage irréversible) ont été mises en place pour prévenir cette éventualité. Dans ce cas, même si l'identification de certaines personnes concernées peut se produire malgré tous les protocoles et mesures (en raison de circonstances imprévisibles telles qu'une correspondance accidentelle des caractéristiques de la personne concernée qui révèle son identité), les informations traitées par le responsable initial peuvent ne pas être considérées comme concernant des personnes physiques identifiées ou identifiables, compte tenu de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par toute autre personne. Leur traitement peut ainsi ne pas être soumis à la réglementation des traitements de données à caractère personnel. Il en va tout autrement pour le nouveau responsable du traitement qui a effectivement eu accès aux données identifiables qui seront elles, sans aucun doute, considérées comme des *données à caractère personnel*.

17. Une ***donnée anonyme*** est toute information qui concerne une personne physique qui ne peut pas être identifiée, ni par le responsable du traitement des données ni par toute autre personne, compte tenu de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par toute autre personne, pour procéder à cette identification. L'arrêté royal (belge) du 21 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel définissait les données anonymes comme « les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable et qui ne sont donc pas des données à caractère personnel »[32] avec une notion de rupture de lien définitive entre, d'une part, la donnée et, d'autre part, la personne concernée.

Une ***donnée anonymisée*** est une donnée anonyme qui concernait auparavant une personne identifiable mais qu'il n'est plus possible d'identifier. De nouveau, il faut tenir compte des circonstances propres à chaque cas d'espèce et un examen au cas par cas s'impose. Il faut vérifier les moyens susceptibles d'être raisonnablement mis en œuvre pour réaliser l'identification de la personne concernée. À cet égard, le Groupe 29 souligne le fait que dans, le cas des informations statistiques, en dépit du fait que les informations peuvent se présenter sous une forme agrégée, l'échantillon initial peut ne pas être suffisamment important, et que d'autres éléments d'information peuvent permettre d'identifier les personnes concernées.

Dans son avis sur les techniques d'anonymisation, le groupe de travail explique que « (…) pour rendre des données anonymes il faut en retirer

[32] Art. 1, 5°, de l'arrêté royal.

suffisamment d'éléments pour que la personne concernée ne puisse plus être identifiée. Plus précisément, les données doivent être traitées de façon à ne plus pouvoir être utilisées pour identifier une personne physique en recourant à « l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre », soit par le responsable du traitement, soit par un tiers. Un facteur important est que le traitement doit être irréversible. (…) ». Le groupe de travail insiste sur le fait que « L'accent est mis sur le résultat : il faut faire en sorte que les données ne permettent pas d'identifier la personne concernée par « l'ensemble » des moyens « susceptibles » d'être « raisonnablement » employés »[33]. Cette approche est ambiguë. En effet, s'il existe des situations dans lesquelles l'information traitée contient en elle-même les éléments qui permettent d'identifier la personne concernée (comme son image ou son nom patronymique ou son prénom), il existe beaucoup d'autres situations dans lesquelles l'information traitée ne contient aucun élément qui permette d'identifier la personne concernée mais il y a des moyens qui peuvent être raisonnablement mobilisés pour établir un lien entre la personne concernée et l'information qui fait l'objet d'un traitement (comme les adresses IP grâce au registre des abonnés tenus par le fournisseur d'accès). Il paraît dès lors inexact de soutenir sans autre précision que l'anonymisation requiert de faire le nécessaire pour que les données (en elle-même) ne permettent pas d'identifier la personne concernée par l'ensemble des moyens susceptibles d'être raisonnablement employés. Il faut, en réalité, mettre en œuvre les mesures (et peu importe leur nature) qui empêcheront (de manière raisonnable) d'établir un lien entre la personne concernée et l'information qui fait l'objet d'un traitement. Et, toujours à l'encontre de ce que semble soutenir ponctuellement cet avis, ce ne sont pas les données qui doivent être rendues non-identifiables ; c'est la personne concernée. Le groupe de travail semble d'ailleurs s'être rendu compte du problème puisqu'il ajoute ensuite que : « D'une manière générale, il ne suffit donc pas de supprimer directement des éléments qui sont, en eux-mêmes, identifiants pour garantir que toute identification de la personne n'est plus possible. Il sera souvent nécessaire de prendre des mesures supplémentaires pour empêcher l'identification, toujours en fonction du contexte et des finalités du traitement auquel sont destinées les données anonymisées », que « l'« identification » ne désigne pas simplement la possibilité de retrouver le nom et/ou l'adresse d'une personne, mais inclut aussi la possibilité de l'identifier par un procédé d'individualisation, de corrélation ou d'inférence » et que « Quand des tiers traitent un ensemble de données auquel une technique d'anony-

[33] Groupe 29, Avis 05/2014 sur les techniques d'anonymisation, adopté le 10 avril 2014, WP 216, p. 6.

misation a été appliquée (données anonymisées et communiquées par le responsable de leur traitement à l'origine), ils ne sont pas tenus d'observer les exigences de protection des données pour autant qu'ils ne puissent pas identifier (directement ou indirectement) les personnes concernées dans l'ensemble de données original. Cependant, les tiers doivent prendre en compte les facteurs contextuels et circonstanciels mentionnés précédemment (y compris les spécificités des techniques d'anonymisation appliquées par le responsable du traitement des données à l'origine) pour décider comment ils comptent exploiter et, en particulier, combiner ces données anonymisées pour leur propre usage – car les conséquences résultantes peuvent entraîner différents types de responsabilités de leur part. Dans le cas où ces facteurs et ces caractéristiques sont de nature à comporter un risque inacceptable d'identification des personnes concernées, le traitement entre de nouveau dans le champ d'application de la législation en matière de protection des données ».

Dans son avis sur les développements récents de l'Internet des choses, le groupe de travail explique que les informations relatives au bien-être des individus ne constituent pas des données relatives à la santé mais que des informations relatives à leur santé peut en être déduites[34]. Dans une interprétation large, les informations relatives au bien-être devraient être constitutives de données relatives à la santé. Ce n'est toutefois pas l'approche retenue ici par le groupe de travail, nonobstant l'enseignement à tirer de l'arrêt *Lindqvist* du 6 novembre 2003 qui souligne le fait que la notion de données à caractère personnel relatives à la santé doit recevoir une interprétation large.

§ 3. La notion de données relatives à la santé dans le RGPD

18. C'est dans ce contexte que le RGPD définit les données relatives à la santé comme étant « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne »[35]. Les considérants du RGPD précisent que « Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. » Ils ajoutent que « Cela comprend des informations sur la personne physique collectées

[34] Groupe 29, Avis 8/2017 sur les développements récents de l'Internet des choses, adopté le 16 septembre 2014, WP 223, p. 17.

[35] Voy. art. 4, 15°, du RGPD.

lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil (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) au bénéfice de cette personne physique ; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques ; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro »[36].

19. Par ailleurs, il ressort des considérants relatifs au traitement des catégories particulières de données pour des motifs d'intérêt public que les données relatives à la santé devraient viser tous les éléments relatifs à la santé, à savoir l'état de santé, morbidité et handicap inclus, les déterminants ayant un effet sur cet état de santé, les besoins en matière de soins de santé, les ressources consacrées aux soins de santé, la fourniture de soins de santé, l'accès universel à ces soins, les dépenses de santé et leur financement, ainsi que les causes de mortalité[37].

À propos du droit d'accès, les considérants du RGPD précisent que la personne concernée devrait avoir accès aux données concernant leur santé, par exemple les données de leurs dossiers médicaux contenant des informations telles que des diagnostics, des résultats d'examens, des avis de médecins traitants et tout traitement ou intervention administrés[38].

Autrement dit, dans le RGPD, la notion de données relatives à la santé tourne autour de deux pôles : d'une part, il y a les données qui sont relatives à la santé physique ou mentale d'une personne physique et, d'autre part, il y a les données qui sont relatives à la prestation de services de soins de santé mais, dans la (seule) mesure où ces deux catégories de données des informations révèlent des informations sur l'état de santé de cette

[36] Considérant n° 35 du RGPD.

[37] Voy. considérant n° 54 du RGPD qui renvoie à la notion de santé publique reprise dans le Règlement (CE) 1338/2008 du Parlement européen et du Conseil du 16 décembre 2008 relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail.

[38] Voy. considérant n° 63 du RGPD.

personne. Il est à noter que la notion de soins de santé doit s'entendre des services de santé fournis par des professionnels de la santé aux patients pour évaluer, maintenir ou rétablir leur état de santé, y compris la prescription, la délivrance et la fourniture de médicaments et de dispositifs médicaux conformément à la 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[39].

Cette définition est très large en ce que, à suivre les considérants du RGPD, la notion de données relatives à la santé englobe aussi des données qui, en tant que telle, ne sont pas relatives à la santé mais dont on peut déduire (extraire) des informations sur la santé d'une personne (comme les informations collectées lors de l'inscription d'une personne à un service de soins de santé) ou qui permettent de retrouver des informations relatives à la santé d'une personne (à l'instar d'un identifiant en matière de santé). Il n'est par contre pas évident de justifier l'inclusion dans cette notion des ressources consacrées aux soins ou les sources de leur financement – sauf en ce que ces informations soient de nature à révéler des données sur l'état de santé de la personne concernée.

§ 4. Le point sur la notion de données relatives à la santé

20. Ainsi que cela a déjà été exposé sous un autre angle dans la partie consacrée aux données particulières, les lignes de tension qui entourent la notion de données à caractère personnel relatives à la santé concernent :

– l'étendue de l'interprétation à lui donner ;
– le caractère objectif ou fonctionnel de sa définition ;
– le lien entre données relatives à la santé et données génétiques.

a) L'étendue de l'interprétation à donner à la notion de données relatives à la santé

21. Le premier souci à résoudre dans la définition des données relatives à la santé est celui qui concerne l'étendue à donner à cette notion. Il y a, d'un côté, les tenants d'une interprétation restrictive et qui considèrent que ne sont des données relatives à la santé que celles qui contiennent matériellement une information sur la santé de la personne concernée. Il y a, de l'autre côté, ceux qui soutiennent une interprétation large et qui pensent opportun, à cet effet, d'inclure dans la notion toutes les

[39] Voy. art. 3.a du RGPD.

informations dont on pourrait déduire une indication sur la santé de la personne concernée. En réalité, ces deux approches ne se contredisent pas dans la mesure où elles ne se situent pas au même niveau de raisonnement. Il n'y a, dès lors, pas à choisir entre interprétation large ou restrictive de la notion de données relatives à la santé mais de savoir si leur définition englobe ou non des données qui ne sont pas relatives à la santé mais dont on peut déduire (extraire) des données relatives à la santé. Pour le surplus, nous renvoyons à la partie consacrée aux données particulières.

b) Le caractère objectif ou fonctionnel de la définition des données relatives à la santé

22. La seconde question à régler concerne la méthode à suivre pour définir les données relatives à la santé. Les définitions balancent à cet égard entre définition *objective* et définition *fonctionnelle* des données relatives à la santé. La définition *objective* des données relatives à la santé s'appuie sur le contenu informationnel de celles-ci : le fait de contenir ou non une information sur l'état de santé de la personne. Dans une définition *fonctionnelle*, la définition ne dépend pas exclusivement du contenu informationnel mais de la volonté d'appliquer le régime de protection des données relatives à la santé à des données qui ne contiennent pas d'information sur l'état de santé mais qui s'y rapportent ou qui permettent d'en déduire. Le meilleur exemple à cet égard a été la tendance de considérer que toutes les données génétiques étaient des données relatives à la santé : puisque la directive 95/46/CE ne leur avait pas réservé de régime spécifique au-delà de la question des traitements de données qui présentaient des risques particuliers pour les droits et libertés des personnes concernées, elles étaient ainsi protégées par le régime propre aux données sensibles. C'est donc bien entre ces deux types de définition des données relatives à la santé qu'il faut choisir.

23. À notre sens, il faut privilégier la *définition objective* qui se fonde sur le contenu informationnel des données relatives à la santé et exclure toute déformation de cette définition dans le but, fût-il légitime, de délimiter ou d'élargir son champ d'application pour y inclure des données qui mériteraient une protection équivalente. Il faut tout autant exclure de la notion de données relatives à la santé les informations dont on peut déduire des indications sur la santé de la personne concernée. En effet, il n'y a rien de pire que de se tromper dans l'objet à protéger ou dans l'identification du traitement en cause. Il n'y a de toute façon aucun intérêt à confondre la source de l'information relative à la santé avec celle-ci. Et procéder de la sorte n'induit aucun affaiblissement de la

protection puisque cela permet de se focaliser correctement sur la donnée relative à la santé que l'on veut réellement protéger (ici, la donnée qui en serait déduite), au lieu de s'attarder à déformer la réalité pour qualifier une donnée anodine en donnée relative à la santé pour ensuite oublier de protéger correctement la donnée relative à la santé qui aurait été déduite (extraite) de la première. Pour le dire autrement, il ne faut pas confondre le récipient et son contenu, et il ne faut pas appliquer au récipient le régime de son contenu. Ainsi, pour prendre un exemple, l'adresse IP peut être une donnée à caractère personnel en ce qu'elle constitue un moyen d'identifier la personne concernée sur le réseau, c'est le reflet de la présence de la personne sur le réseau. Mais, l'adresse IP est aussi un élément dont l'exploitation va permettre de générer d'autres données qui pourraient aussi être à caractère personnel ; et c'est souvent ces données-là qui sont les plus sensibles et qui appellent une réelle protection. L'utilisation de l'adresse IP doit surtout être encadrée au vu de ce qui peut en être fait. Opérer cette distinction est très utile surtout dans le domaine de la santé : cela oblige à se pencher sur la manière de produire des informations relatives à la santé, ce qui paraît essentiel dans un monde dominé par le big data, le datamining et les applications santé de toutes sortes.

c) Le lien entre les données relatives à la santé et les données génétiques

24. Il demeure à aborder la question traditionnelle du lien entre les données génétiques et les données relatives à la santé. Dans son document de travail du 17 mars 2004[40], le Groupe 29 est parti du principe que, dans la majorité des cas, les données génétiques étaient des données à caractère personnel. Il précise que les données génétiques pouvaient, dans une certaine mesure, donner une image détaillée de la condition physique d'un individu et de son état de santé et qu'à ce titre, elles pourraient être considérées comme des données à caractère personnel relatives à la santé. Mais, il ajoute aussitôt qu'elles permettent aussi de décrire des caractéristiques physiques de la personne concernée et que, dans cette mesure, les données génétiques qui, par exemple, déterminent la couleur des cheveux,

[40] Groupe 29, Document de travail sur les données génétiques, adopté le 17 mars 2004, WP 91. L'UNESCO définit les données « génétiques » comme étant les informations relatives aux caractéristiques héréditaires des individus, obtenues par l'analyse d'acides nucléiques ou par d'autres analyses scientifiques. Elle définit aussi les données *protéomiques humaines*. Il s'agit des informations relatives aux protéines d'un individu, y compris leur expression, leur modification et leur interaction (UNESCO, Déclaration internationale sur les données génétiques humaines adoptée à la 20e séance plénière le 16 octobre 2003).

ne devraient pas être considérées comme des données concernant directement la santé.

25. Trois points méritent d'être soulignés. D'abord, il convient d'insister sur le fait que les données génétiques ne sont pas toujours des données à caractère personnel. Ensuite, toutes les données génétiques ne sont pas des données à caractère personnel relatives à la santé, même si cette confusion des genres permet de résoudre le problème lié au fait que la directive 95/46/CE ne reprenait pas les données génétiques dans la liste des données sensibles, laissant de ce fait accroire qu'elles seraient sans protection particulière, ce qui était inexact. En effet, si les données génétiques ne se subsumaient pas toutes sous la catégorie des données à caractère personnel relatives à la santé, il doit néanmoins être rappelé que leur traitement est fréquemment susceptible de présenter des risques particuliers pour les droits et libertés des personnes concernées, ce qui les soumettait au régime du contrôle préalable prévu à l'article 20 de la directive 95/46/CE, sans préjudice de l'existence de dispositions nationales spécifiques. Enfin, le groupe de protection des données a indiqué que les données génétiques participant à la description de caractéristiques physiques de la personne concernée ne concernaient pas directement la santé. Il ne s'agit donc pas, à ses yeux, de données à caractère personnel relatives à la santé, ce qui est exact.

26. De son côté, le RGPD définit les données génétiques comme étant les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question[41], notamment une analyse des chromosomes, de l'acide désoxyribonucléique (ADN) ou de l'acide ribonucléique (ARN), ou de l'analyse d'un autre élément permettant d'obtenir des informations équivalentes[42]. Il s'en déduit que si les données génétiques ne se confondent pas nécessairement avec des données à caractère personnel relatives à la santé, il n'en demeure pas moins que certaines données génétiques peuvent être en même temps des données à caractère personnel relatives à la santé.

[41] Art. 4 du RGPD.

[42] Voy. considérant n° 34 du RGPD.

d) Les éléments manquants de la définition des données relatives à la santé

27. Ceci étant, deux éléments semblent manquer dans la définition des données relatives à la santé alors qu'ils sont essentiels : il s'agit de la notion *d'information* et celle de *santé*. Usuellement, en l'absence d'une définition explicite, il faut se rabattre sur le sens communément donné à ces deux mots.

- La notion d'information

28. Il ressort de l'analyse du dictionnaire de l'Académie française que la notion d'information est, en quelque sorte, tributaire du contexte dans lequel elle est employée. À notre sens, il faut retenir, dans celui qui nous intéresse, que la notion d'information vise tout élément de connaissance qui concerne, peu ou prou, un individu. En informatique, l'information est un « Élément de connaissance traduit par un ensemble de signaux selon un code déterminé, en vue d'être conservé, traité ou communiqué » et la donnée est une « Représentation d'une information sous une forme conventionnelle adaptée à son exploitation »[43]. Et un élément de connaissance, c'est un élément qui nous apprend quelque chose sur un objet donné ; c'est, plus précisément, un élément de connaissance sous une forme intelligible par un individu. En ce sens, l'information est un élément de connaissance mis en une forme qui permet son appréhension par l'être humain (à travers l'un de ses sens). La donnée relative à la santé serait alors sous cet angle d'approche un élément de connaissance qui nous apprend quelque chose sur la santé d'une personne physique identifiée ou identifiable. Il demeure alors à s'entendre sur ce que veut dire la santé d'une personne.

- La notion de santé

29. En l'absence de précision, la notion de santé s'entend usuellement de la définition qui en est donnée par l'Organisation Mondiale de la Santé et qui se réfère à un état de complet bien-être physique, mental et social,

[43] Voy. la définition de ces termes dans le Dictionnaire de l'Académie française, (9e éd.). En informatique, l'information est un « Élément de connaissance traduit par un ensemble de signaux selon un code déterminé, en vue d'être conservé, traité ou communiqué » et la donnée est une « Représentation d'une information sous une forme conventionnelle adaptée à son exploitation ». En droit, en matière de traitement de données, la notion de *donnée à caractère personnel* est *toute information relative à une personne identifiée ou identifiable* (art. 2.a de la Convention n° 108).

et ne consiste pas seulement en une absence de maladie ou d'infirmité[44]. Il n'est pas possible de savoir si le Conseil de l'Europe ou l'Union européenne a jamais eu l'intention de se référer à cette définition de la santé qui peut sembler appropriée sur certains éléments mais excessives pour les objectifs de la protection des données relatives à la santé – ce qui vise la question des informations relatives à un état de complet bien-être social. Mais, il pourrait être raisonnablement soutenu que les informations relatives à la santé sont celles qui nous apprennent quelque chose sur l'état de la santé, bon ou mauvais, physique ou mental d'un individu.

e) Une proposition de synthèse de la notion de données relatives à la santé

30. À notre sens, il faut retenir une définition stricte et objective de la notion de données relatives à la santé qui se limite aux informations qui contiennent un élément de connaissance sur l'état de santé d'une personne (physique), excluant par-là toute velléité d'étendre la notion à des données qui ne contiennent aucune information sur l'état de santé d'une personne même s'il est possible d'en déduire (en raison notamment de la finalité poursuivie ou du contexte). En effet, les données qui seraient ainsi déduites ou extraites seront automatiquement protégées en raison de leur contenu informationnel et les données dont elles ont été déduites ou extraites ne seront pas régies par un statut qui ne leur est pas approprié et qui n'apporte, en réalité, aucune protection réelle à la personne concernée. Par ailleurs, il n'est (pas) plus sensé d'inclure des données qui ne sont pas relatives à la santé mais dont on peut déduire des informations sur l'état de santé d'une personne et ce, pour une raison bien simple : ainsi que nous l'avons déjà relevé précédemment, il est, aujourd'hui, possible de déduire des informations relatives à l'état de santé d'une personne à partir d'une multitude d'informations tout à fait quelconques et qui, surtout, ne sont (pas) plus discriminables dans les faits. Il vaut donc mieux circonscrire la notion aux seules données qui sont des informations sur l'état de santé de la personne concernée. Il convient de rappeler que les données relatives à la santé ne doivent pas nécessairement émaner d'un professionnel de la santé ou résulter d'un acte réservé aux professionnels de la santé. De plus, une donnée peut être relative à la santé même lorsqu'elle n'est pas traitée à des fins thérapeutiques ; c'est le

[44] Préambule à la Constitution de l'Organisation mondiale de la Santé, tel qu'adopté par la Conférence internationale sur la Santé, New York, 19-22 juin 1946, signé le 22 juillet 1946 par les représentants de 61 États et entré en vigueur le 7 avril 1948 (Actes officiels de l'Organisation mondiale de la Santé, n° 2, p. 100).

cas notamment en matière d'assurance ou de crédit. Par ailleurs, la seule information relative à un aspect physique ou psychique d'un individu ne constitue pas nécessairement en tant que telle une donnée relative à la santé. Pour obtenir cette dernière qualification, l'aspect physique ou psychique doit nous apprendre quelque chose à propos de la santé de la personne concernée. En ce sens, les données relatives à la santé visent toutes les informations relatives à la santé physique ou psychique, passée, présente ou future, d'une personne physique, vivante ou décédée.

SECTION 3. – Les notions de responsable de traitement et de sous-traitant dans le secteur de la santé

§ 1. La sous-traitance de données et les services de *cloud computing* dans le secteur de la santé

31. Le sous-traitant est devenu un acteur important, si pas incontournable dans de nombreux cas, en matière de traitements de données à caractère personnel, surtout depuis le développement des services de *cloud computing*, du Big Data ou encore des applications de téléphonie mobile. Le sous-traitant offre l'expertise technique, les équipements et les ressources matérielles et personnelles, que le responsable de traitement ne peut pas ou ne veut pas prendre en charge pour réaliser ses projets informatiques.

Dans le domaine des soins de santé, la sous-traitance de données est omniprésente, que ce soit au sein des hôpitaux ou des cabinets de médecins généralistes, soit dans le cadre de la gestion des données des patients soit dans le cadre de la communication de données relatives au patient entre professionnels de la santé au travers des réseaux télématiques régionaux et fédéral. Il est, de plus en plus, fait appel à des sous-traitants qui apportent leurs compétences particulières dans la gestion des données de leurs patients[45].

32. Le RGPD a repris la substance des règles relatives à la sous-traitance des données qui étaient contenues dans la directive 95/46/CE, tout en les précisant et en étoffant leur contenu dans une certaine mesure, le but

[45] Ceci n'empêche pas qu'il faut vérifier si, dans certaines hypothèses, le recours à un sous-traitant ne serait pas un procédé incompatible avec les finalités pour lesquelles les données ont été collectées et traitées. Il faut aussi vérifier s'il ne faut pas informer la personne concernée (ici le patient) de l'intervention d'un sous-traitant. Voy. aussi art. 28.4 du RGPD pour la question du recrutement d'un ou plusieurs sous-traitants par le premier sous-traitant.

étant de renforcer l'étanchéité du circuit des traitements de données (sa confidentialité) et par là garantir l'effectivité de la protection de la personne concernée[46].

33. Le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »[47]. Cette définition appelle les observations et explications suivantes.

Tout d'abord, le sous-traitant est une organisation ***extérieure*** à celle du responsable du traitement et qui possède une entité juridique distincte de la sienne[48]. Il s'agit d'un tiers au sens du RGPD.

Ceci étant, le fait d'être une organisation extérieure ne signifie pas qu'il suffise de loger ses activités de traitements de données dans une société dotée d'une personnalité juridique distincte pour qu'il y ait sous-traitance de données. Le sous-traitant ne peut pas, en outre, agir sous l'autorité directe du responsable du traitement (même s'il ne peut traiter les données que sur les instructions (documentées[49] de ce dernier). Pour le dire autrement, il ne peut pas y avoir de relation hiérarchique entre le responsable du traitement et le sous-traitant de données (au sens opérationnel et organisationnel et pas seulement entendu comme une absence de relation de subordination au sens du droit du travail).

Le sous-traitant ne peut donc pas être une personne qui fasse partie de l'organisation du responsable du traitement. L'exemple type est celui du médecin hospitalier qui n'est pas lié par un contrat de travail : il répond bien à la condition de la personnalité juridique distincte mais il ne répond pas à l'exigence de l'organisation extérieure à celle de l'hôpital. Ses activités sont, en effet, totalement intégrées dans celles de l'hôpital. Il n'agit dès lors pas en qualité de sous-traitant de données pour l'hôpital mais bien en qualité de personne agissant sous l'autorité directe de l'hôpital (au sens opérationnel et organisationnel). De même, la secrétaire personnelle d'un médecin généraliste libéral agit sous l'autorité directe de ce dernier ; elle n'intervient donc pas en qualité de sous-traitant lorsqu'elle prend des rendez-vous dans l'agenda électronique ou qu'elle encode des protocoles ou rédige son courrier.

---

[46] Voy. Groupe 29, Avis 1/2010 sur les notions de « responsable de traitement » et de « sous-traitant », adopté le 16 février 2010, WP 169, p. 26.

[47] Art. 4.8 du RGPD.

[48] Voy. Groupe 29, Avis 1/2010 sur les notions de « responsable de traitement » et de « sous-traitant », adopté le 16 février 2010, WP 169, p. 26.

[49] Conformément à l'article 28.3 du RGPD.

La qualification à donner à la société juridiquement distincte qui preste des services de traitements de données dans un contexte de mutualisation de services (entre hôpitaux ou médecins libéraux) s'analyse de la même façon. Si la première condition (personnalité juridique distincte) est souvent remplie, il convient encore de vérifier si ce prestataire de services mutualisés intervient bien en-dehors de l'organisation des activités du responsable du traitement et sans être sous son autorité directe. Si la réponse est positive, nous serons en présence d'un sous-traitant. Sinon, d'une personne agissant sous l'autorité directe du responsable du traitement. Ainsi, le secrétariat extérieur auquel fait appel un médecin généraliste libéral pour la gestion de ses rendez-vous revêt la qualité de sous-traitant dans la mesure des traitements de données qu'il effectue pour le compte de ce médecin.

Une difficulté peut surgir lorsque le prestataire de services est une organisation extérieure dotée d'une personnalité juridique distincte mais qui détache un travailleur au sein de l'organisation du responsable du traitement. Le tout sera de savoir si le travailleur extérieur est ou non soumis à l'autorité directe du responsable du traitement. Un cas fréquent est celui du travailleur d'une société de maintenance informatique qui, dans les faits, est installé à demeure, à durée déterminée ou non, dans les murs de l'hôpital, et qui traite des données pour compte de ce dernier. Par contre, la société extérieure qui réalise une migration de données au sein de l'hôpital sans être sous l'autorité directe du responsable du traitement mais qui, pour ce faire, est bien obligée de dépêcher du personnel sur place pendant plusieurs jours ou semaines, ne perd pas de ce fait sa qualité de sous-traitant de données.

Le tout est, bien sûr, de ne pas autoriser les montages de toutes sortes destinés à faire échapper l'un ou l'autre intervenant dans les traitements de données aux obligations qui lui incombent ou de jouer sur les qualifications pour en tirer profit. Ceci pose la question de la qualification à donner aux services mutualisés au sein d'un grand groupe – question qui, elle-même, renvoie à la question de l'identification des véritables responsables de traitements au sein de ce groupe.

34. La distinction entre les sous-traitants de données et ceux qui agissent sous l'autorité directe du responsable du traitement pose une question qui peut paraître malaisée à trancher : quelle est la différence entre l'obligation faite au sous-traitant d'agir uniquement et exclusivement sur instruction du responsable du traitement et le fait d'agir sous l'autorité directe du responsable du traitement ? Autrement dit, quelle est la différence entre recevoir une instruction et être sous l'autorité directe du responsable du traitement ?

Dans le premier cas, le sous-traitant reçoit une mission à accomplir au profit du responsable du traitement (et il peut la refuser) et il la réalise dans le cadre d'une organisation extérieure et juridiquement distincte de celle du responsable du traitement en choisissant les moyens techniques et d'organisation à mettre en œuvre à cet effet dès lors qu'il est justement fait appel à lui pour ses compétences particulières comme ce sera souvent le cas pour les services de *cloud computing*[50]. Ceci étant, il ne faut pas perdre de vue qu'à partir du franchissement d'un certain seuil, le sous-traitant pourrait devenir un responsable de traitement conjoint en raison de sa participation aux choix des finalités et des moyens du traitement de données par l'hôpital[51].

Dans le second cas, la personne réalise la prestation qui lui est demandée en utilisant les moyens mis à sa disposition par le responsable du traitement sans pouvoir refuser la mission car elle se trouve dans le cadre d'une relation hiérarchique ou subordonnée. Dans cette situation, elle peut apporter son expertise dans le choix des finalités et des moyens sans encourir le risque de devenir un responsable de traitement conjoint.

C'est en tout cela qu'il faut comprendre que le sous-traitant est une entité extérieure et juridiquement distincte de celle de l'hôpital en sa qualité de responsable du traitement. À défaut, il n'y a pas sous-traitance de données mais une intervention sous l'autorité du responsable du traitement. Le tout revient maintenant, à se demander s'il n'est pas artificiel de distinguer entre ces deux catégories qui, *in fine*, doivent répondre aux mêmes obligations…

En tout cas, il faut rappeler que le sous-traitant doit informer « immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du [règlement] ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données »[52].

35. Par ailleurs, le sous-traitant doit traiter des données pour compte du responsable du traitement. À cet effet, il doit, conformément à la définition même de la notion de *traitement*[53], réaliser des opérations ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automati-

[50] Voy. à ce propos, J.-M. Van Gyseghem, « Cloud computing et protection des données à caractère personnel : mise en ménage possible ? », *R.D.T.I.*, vol. 42, 2011, pp. 35-50. Voy. égal. Groupe 29, Avis 05/2012 sur l'informatique en nuage, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf.

[51] Voy. Groupe 29, Avis 1/2010 sur les notions de « responsable de traitement » et de « sous-traitant », adopté le 16 février 2010, WP 169, p. 27.

[52] Art. 28, 3, h), du RGPD.

[53] Voy. art. 4, 2°, du RGPD.

sés et qui sont appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. Changer le câblage, les écrans ou les imprimantes d'un service hospitalier n'est pas constitutif d'un traitement de données, pas plus que l'installation d'un logiciel pour autant que son installation ne requière pas de traitement de données. Par contre, la question est plus ardue en matière de *cloud computing*. Il faut raisonner à cet effet en partant de la classification pédagogique en trois services du *cloud computing*.

En principe, le recours à un service de *cloud computing* « *Infrastructure as a service* » ne consiste pas, dans le chef du responsable du traitement, à demander au fournisseur du service de traiter pour son compte des données ; il consiste « seulement » à lui louer du matériel informatique (du *hardware*) (comme de l'espace disque mais sans système d'exploitation). Pour le dire autrement, le fournisseur de services « *Infrastructure as a service* » loue au responsable du traitement l'équipement dont ce dernier a besoin pour, le cas échéant, traiter des données. Le responsable du traitement ne demande pas au fournisseur de service « *Infrastructure as a service* » de traiter les données à sa place (pour son compte) – même si le responsable du traitement peut utiliser cet équipement pour héberger des données à caractère personnel. D'ailleurs, le fournisseur de ce service va facturer la location du hardware et non des opérations de traitement de données. Le plus souvent, c'est un administrateur réseau qui recourt à ce type de service. En règle, le contrat entre le responsable du traitement et le fournisseur de ce type de services doit inclure des clauses par lesquelles le fournisseur s'engage à ne pas tenter d'accéder aux données qui seraient stockées sur ses serveurs et de protéger ces dernières de tout accès non-autorisé. Il arrive aussi que le responsable du traitement impose au fournisseur de lui garantir que personne d'autre n'utilise le même serveur pour éviter toute tentative d'accès non autorisé par un autre utilisateur du même serveur.

Par contre, il y a nécessairement sous-traitance de données lorsque le responsable du traitement recourt à un service de *cloud computing* de type « *Software as a service* » dont l'exemple le plus fréquent est celui où le responsable du traitement (ici l'hôpital) demande au fournisseur d'héberger des données (comme des dossiers médicaux). L'hôpital demande au fournisseur de ce service d'héberger des données pour son compte. La facturation sera, d'ailleurs, différente de celle qui peut exister pour le service « *Infrastructure as a service* ».

Le troisième type de services de *cloud computing* est celui d'« *Infrastructure as a platform* » dans lequel le fournisseur loue du hardware mais fournit aussi le système d'exploitation. Ce service est habituellement destiné aux développeurs de logiciels. Dans cette hypothèse, il faut analyser de manière encore plus approfondie au cas par cas dans quelle mesure le fournisseur de services intervient dans le traitement de données en tant que tel.

Enfin, si, à une certaine époque, on aurait pu être tenté de soutenir que les médecins n'étaient que les sous-traitants de leurs patients en termes de traitements de données, ce modèle n'a guère prospéré – aussi tentant fût-il au regard du droit fondamental à l'autodétermination informationnelle des individus. À l'heure actuelle, on considère habituellement que les hôpitaux ou les professionnels de la santé exerçant en privé sont les responsables des traitements de données liés à leurs activités professionnelles.

36. La question se pose également en matière de médecine de conseil, c'est-à-dire à la situation du médecin qui interviendra, au côté d'un avocat, dans la défense d'un client qui n'est souvent pas son patient.

Il agira à la demande de l'avocat ou même du client et pour son compte. Si le premier critère de la notion de sous-traitance est rempli, qu'en est-il du second, à savoir d'un travail sous les instructions documentées du responsable du traitement. La question se posera essentiellement au niveau du type de demande qui émane de l'avocat et de la marge de manœuvre dont dispose le médecin.

À l'instar des avocats, le médecin doit travailler de manière objective et ne peut calquer son travail sur des ordres émanant d'un tiers. Il devra travailler de manière libre et le résultat de son travail devra être dénué de toute pression qui le rendrait inutilisable en justice dès lors qu'il serait empreint de partialité ; partialité que ne sied pas à la justice. De plus, des positions partiales ferait perdre toute crédibilité au médecin agissant de la sorte.

Au regard de ces divers éléments, il nous semble que le médecin – conseil technique agira bien à la demande d'un avocat mais disposera de suffisamment de latitude dans l'exercice de sa mission qu'il ne pourra pas être considéré comme travaillant sous les instructions d'un responsable du traitement. Ainsi, il agira comme un responsable du traitement avec sa base de licéité propre même si son intervention sera limitée par un contrat avec l'avocat ou le client de ce dernier ; ce qui n'est pas synonyme de sous-traitance. En d'autres termes, son intervention ne pourra pas dépasser le cadre de la mission qui lui a été assignée mais gardera sa pleine autonomie dans le cadre de cette même mission.

§ 2. Le sous-traitant et la notion de responsable conjoint du traitement de données

37. Le RGPD prévoit, en son article 26, que :

« 1. Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.
2. L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.
3. Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement ».

La coresponsabilité du traitement, qui existait déjà sous la directive 95/46/CE, s'applique quand plusieurs responsables de traitements déterminent ensemble les finalités (le « pourquoi ») et les moyens (le « comment ») de certaines activités de traitements[54]. L'on doit également noter que, « pour qu'une personne puisse être considérée comme un responsable du traitement, au sens de l'article 2, sous d), de la directive 95/46, il n'est pas nécessaire que cette personne dispose d'un pouvoir de contrôle complet sur tous les aspects du traitement. Comme le gouvernement belge l'a indiqué à juste titre lors de l'audience, un tel contrôle existe de moins en moins en pratique. De plus en plus, les traitements ont une nature complexe, en ce sens qu'il s'agit de plusieurs traitements distincts impliquant plusieurs parties exerçant elles-mêmes différents degrés de contrôle. Par conséquent, l'interprétation privilégiant l'existence d'un pouvoir de contrôle complet sur tous les aspects du traitement est suscep-

[54] Sur la détermination des finalités et des moyens, voy., not. : Groupe 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 14.

tible d'entraîner de sérieuses lacunes en matière de protection des données à caractère personnel. »[55] et que « l'interprétation large de la notion de « responsable du traitement », au sens de l'article 2, sous d), de la directive 95/46, qui doit, selon nous, prévaloir dans le cadre de la présente affaire, est de nature à éviter les abus. En effet, il suffirait sinon pour une entreprise de recourir aux services d'un tiers pour se soustraire à ses obligations en matière de protection des données à caractère personnel »[56].

38. En matière de santé, l'on peut se poser la question de savoir si un sous-traitant ne doit pas être considéré le plus souvent comme un responsable conjoint du traitement tant il est impliqué dans les moyens mis en œuvre pour atteindre la finalité du traitement. Prenons l'exemple du service de second avis qui est souvent presté en dehors de l'Union européenne (Inde, Chine) mais offert par des sociétés européennes aux médecins. Pour ce faire, les médecins qui requièrent ce second avis doivent passer par un traducteur chargé de traduire les dossiers médicaux afin de permettre au médecin se trouvant dans un pays tiers de pouvoir rendre un second avis sur base de documents qu'il comprend.

S'il ne fait aucun doute que le médecin est responsable du traitement comme analysé ci-dessus, qu'en est-il exactement de la société offrant un service de de traduction qui, elle-même, fait appel à des traducteurs indépendants ?

Cette société offre un service qui ne met pas l'accent sur le traitement de données mais sur la traduction de dossiers médicaux ou partie de ceux-ci, sur base contractuelle. Le traitement de données est en lien avec la finalité du contrat mais n'est pas son objectif. Par ailleurs, la société travaille sur base d'instructions peu spécifiques ou documentées ne correspondant pas nécessairement au concept de sous-traitant. Par conséquent et si nous considérons que cette société offrant un service de traduction ne remplit pas les critères fixés par le RGPD, elle ne pourra pas être considérée comme étant un sous-traitant du responsable du traitement.

Pourrait-elle être responsable de traitement alors que le médecin l'est déjà ainsi que nous l'avons analysé ci-dessus ? Dans la relation entre parties, la société offre un service de traduction et traite nécessairement des données à caractère personnel même si elle ne met pas l'accent sur

[55] C.J.U.E., arrêt *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, concl. av. gén. du 24 octobre 2017, pt 62. Si l'argumentation porte sur la directive 95/46/CE, cela peut être transposée pour le RGPD.

[56] *Idem*, pt 64 ; si l'argumentation porte sur la directive 95/46/CE, cela peut être transposé pour le RGPD.

un tel traitement pour exécuter le contrat. Au regard de ce service, nous pourrions considérer que la société détermine tant la finalité (traduction) que les moyens (appel à des traducteurs indépendants). Si tel est le cas, nous avons donc affaire à un nouveau responsable du traitement mais qui n'a cependant aucun contact avec les patients qui sont pourtant les personnes concernées. Elle ne pourra donc pas exécuter les obligations en matière d'information ou d'accès au profit de la personne concernée alors que ces obligations sont pourtant à sa charge en sa qualité de responsable de traitement.

Ainsi que le rappelle l'avocat général près la Cour de justice de l'Union européenne, il y a lieu de « préciser que l'existence d'une responsabilité conjointe ne signifie pas une responsabilité sur un pied d'égalité. Au contraire, les différents responsables du traitement peuvent être impliqués dans un traitement de données à caractère personnel à différents stades et à différents degrés »[57]. Par ailleurs, le Groupe 29 a également précisé que « la participation des parties à la détermination des finalités et des moyens de traitement dans le cadre d'une coresponsabilité peut revêtir différentes formes et n'est pas nécessairement partagée de façon égale. (…) De plus, il est tout à fait possible que, dans des systèmes complexes qui font intervenir de multiples acteurs, l'accès aux données à caractère personnel et l'exercice des autres droits des personnes concernées puissent aussi être garantis à différents niveaux par différents acteurs »[58].

Il nous semble que la situation du médecin et du service de traduction pourrait s'inscrire dans cette définition donnée tant par l'avocat général que par le Groupe de l'article 29. Nous aurions dès lors une responsabilité conjointe agissant à divers niveaux mais assurant une protection adéquate des données à caractère personnel des patients qui sont, au surplus, des catégories particulières de données au sens de l'article 9 du RGPD.

Cette situation montre la difficulté de pouvoir déterminer de manière univoque si un acteur est sous-traitant ou responsable du traitement.

---

[57] C.J.U.E., *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, aff. C-210/16, concl. av. gén. du 24 octobre 2017, pt 75, confirmé par la Cour de justice de l'Union européenne dans un arrêt du 5 juin 2018.

[58] Groupe 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP 169, p. 35.

SECTION 4. – Le rôle du consentement en matière de traitements de données à des fins scientifiques

39. Le rôle du consentement de la personne concernée pour légitimer (donner une base de licéité) au traitement de données à caractère personnel à des fins scientifiques a toujours soulevé beaucoup de questions. Malheureusement, il ne peut pas être soutenu que le RGPD ait apporté de réelles réponses au besoin du secteur. Voici quelques points qui ont retenu notre attention.

En premier, nonobstant les commentaires qui lui ont été adressés à ce sujet lors de la consultation publique de son document revisité contenant des lignes directrices en matière de consentement sous le RGPD, le Comité a maintenu l'allégation selon laquelle un responsable de traitement devait choisir une (et une seule) base de licéité pour fonder le traitement de données parmi les six choix offerts par l'article 6 du RGPD et que s'il avait choisi le consentement pour tout ou partie du traitement de données, il devait mettre fin au traitement de données si la personne concernée retirait son consentement ou si le consentement se révélait invalide[59]. Cette prise de position appelle les observations suivantes qui intéressent les traitements de données à des fins scientifiques.

40. Il n'est pas tout à fait exact d'affirmer que la notion de consentement aurait évolué dans le RGPD. Globalement, c'est plutôt la manière de traiter le consentement et la détermination de l'âge pour consentir qui ont retenu l'attention du RGPD.

Par ailleurs, alléguer qu'un responsable de traitement doit nécessairement se cantonner à ne choisir qu'une base de licéité (auparavant, on disait une base de légitimation) parmi les six qui lui sont proposées par l'article 6 du RGPD est inexact et *explicitement* contredit par le RGPD lui-même. En effet, l'article 17 du RGPD expose à propos du droit à l'effacement (« droit à l'oubli ») que le responsable du traitement doit effacer les données dans les meilleurs délais lorsque la personne concernée a retiré son consentement sur lequel était fondé le traitement (que ce soit sur pied de l'article 6.1.a) ou 9.2.a)) et lorsqu'il n'existe pas d'autre fondement juridique au traitement. Ceci démontre de manière incontestable qu'un même traitement peut reposer sur plusieurs bases juridiques différentes.

Ce point est essentiel car, en matière de traitements de données à des fins scientifiques, il est conseillé de se référer au cadre légal et réglementaire

[59] Groupe 29, Lignes directrices sur le consentement sous le Règlement 2016/679, adopté le 28 novembre 2017 et revu et adopté en dernier le 10 avril 2018, WP 259 rev.01, p. 23, pt 6.

spécifiquement adopté par chaque État membre en matière de traitements de données à des fins scientifiques (et qui, le plus souvent, ne prévoit pas d'obtenir le consentement de la personne concernée sous la condition de respect des garanties appropriées comme l'anonymisation ou la pseudonymisation des données – couplé avec l'intervention d'un tiers de confiance dans la réalisation de ce processus), tout en ajoutant le consentement de la personne concernée comme base de (légitimation) licéité afin de *renforcer* la légitimité et la licéité de ce genre de traitements de données qui présente fréquemment des risques particuliers pour les droits et libertés des individus en suite, par exemple, de l'acceptation d'une finalité moins précise ou d'une confidentialité affaiblie notamment en raison de l'exploitation même des données en dehors de la sphère thérapeutique. Il faut bien voir que, dans ce contexte, l'accumulation des fondements de licéité des traitements est un gage de protection renforcée de la personne concernée qui permet, en outre, de l'impliquer plus avant dans le traitement de données qui la concernent et dans la finalité poursuivie.

Il serait, en outre, particulier de refuser l'ajout du consentement de la personne concernée à une autre base de licéité pour renforcer la légitimité d'un traitement de données à des fins scientifiques tout en acceptant, par ailleurs, un allègement des conditions en matière de précision des finalités poursuivies par le traitement de données à des fins scientifiques[60]. Pour le dire autrement, il est difficile de concevoir que le RGPD refuserait de renforcer la légitimité d'un traitement de données par l'ajout du consentement de la personne concernée tout en acceptant d'être moins exigeant sur le degré de précision de la finalité poursuivie en matière scientifique dès lors que cela induit, *de facto*, un consentement plus faible, de moindre qualité puisque moins informé.

41. En résumé – et contrairement à l'opinion du Comité – le responsable du traitement peut et, dans certains cas, doit renforcer la licéité de son traitement de données en ajoutant le consentement de la personne concernée – étant entendu qu'à notre sens, fonder un traitement à des fins scientifiques uniquement sur le consentement de la personne concernée est un choix périlleux et contestable dans de nombreuses situations. Ce consentement pourrait être remplacé par une possibilité d'*opt-out* (d'opposition) pour autant que la personne concernée reçoive une information complète et intelligible, ce qui suppose que le soit dans sa langue, qui lui permettra un exercice effectif de son droit à l'*opt-out*[61].

---

[60] Voy. considérant n° 33 du RGPD à ce sujet.

[61] Voy., entre autres, la Déclaration d'Helsinki de L'AMM – Principes éthiques applicables à la recherche médicale impliquant des êtres humains.

Cette façon de faire permet, en outre, de régler la question, odieuse, du chantage auquel peuvent être soumis des responsables du traitement dans des hypothèses où il existe peu de données susceptibles d'être traitées et que le traitement de données a requis des investissements conséquents dans des secteurs sous-financés en matière de recherche scientifique. En effet, dans ce genre de situations, il est arrivé que des héritiers de la personne concernée, voire la personne concernée elle-même, ait, après l'émission du consentement, sollicité des gratifications indues en échange du maintien du consentement au traitement de données[62]. Ce chantage n'est pas efficace lorsque le traitement de données repose sur plusieurs bases de licéité.

Il faut aussi rappeler que les États membres peuvent ajouter des conditions au traitement de certaines catégories de données sensibles comme les données relatives à la santé[63] voire les alléger en matière de recherche scientifique[64].

Sur le fond, il est difficile de se défaire de l'idée que, si les contraintes mises par le Comité en matière de consentement sont idéales, il n'en demeure pas moins qu'elles ne correspondent en rien à la réalité ni à quoi que ce soit qui soit praticable dans beaucoup d'hypothèses. Toute la question est donc de savoir s'il n'aurait pas mieux fallu agir sur d'autres points de la règlementation pour contrebalancer des faiblesses dans la légitimation des traitements de données lorsqu'elle est fondée sur le consentement de la personne concernée. Ainsi, par exemple, on pourrait augmenter le bénéfice que la personne concernée serait susceptible d'en retirer comme des retours sur son état de santé, par l'accès aux traitements médicaux disponibles découverts suite à la recherche scientifique, par un droit d'accès plus dynamique (par exemple, une information structurée à intervalles réguliers transmise d'initiative du responsable du traitement vers la personne concernée) ou, enfin, par la mise en place d'une réelle gouvernance de la société de l'information avec de véritables organes démocratiques et judiciaires dédicacés à la régulation des activités humaines dans ce nouveau monde virtuel.

42. D'un autre côté, le RGPD ne règle pas la question de la recherche réalisée par les entités commerciales. En effet, de plus en plus, des entités

[62] Cette situation ne doit pas être confondue avec l'affaire de *Moore v. Regents of the University of California* qui donna lieu au fameux arrêt de la Cour suprême de Californie du 9 juillet 1990 (51 Cal. 3d 120 ; 271 Cal. Rptr. 146 ; 793 P. 2d 479) et qui concernait la revendication par un patient de la propriété de matériel corporel humain et la participation aux bénéfices tirés de la recherche réalisée à partir de celui-ci (« *the man with the golden cells* »).

[63] Art. 9.4 du RGPD.

[64] Art. 89 du RGPD.

commerciales sollicitent (et obtiennent) des données relatives à la santé provenant d'institutions de soins de santé ou de praticiens professionnels de la santé pour créer des algorithmes et des applications dans le secteur de la santé. Un des problèmes réside dans le fait que la communication de ces données par des institutions de soins de santé ou des praticiens professionnels vers des entités commerciales est, en principe, incompatible avec les finalités (normalement de soins, à titre principal) pour lesquelles elles ont été collectées et traitées ainsi que par rapport aux règles qui régissent l'activité de ces institutions de soins de santé et de ces praticiens professionnels, notamment dès lors qu'il n'est pas admis que la recherche réalisée par une entité commerciale soit considérée, sans autre forme de procès, comme relevant de la recherche scientifique. En conséquence, pour parvenir à leurs fins, ces entités commerciales doivent travailler de concert avec une entité qui est, elle, habilitée à traiter des données à des fins scientifiques. Cette situation pose énormément de problèmes en pratique et leur solution réside dans des montages juridiques peu aisés qui ne correspondent pas à la réalité, ce qui est toujours une source de grandes difficultés, sans que l'on sache vraiment déterminer la force à donner au consentement de la personne concernée en la matière.

Par ailleurs, plusieurs questions demeurent grandes ouvertes. Une première question classique est de savoir si le consentement au traitement de données à des fins d'essais cliniques peut faire l'objet du même formulaire que le consentement requis pour la participation à l'essai clinique en tant que tel. Il est difficile de départager les opinions à ce sujet même si l'on sent bien que le Comité pencherait, à juste titre, plutôt pour des formulaires distincts[65]. Un intérêt de procéder de la sorte réside dans le fait que cela permet aussi de conserver et de gérer ces formulaires de consentement de manière distincte, ce qui peut se révéler bien utile quand le traitement de données survit (et de loin) à l'essai clinique.

Tout aussi ouverte est la question de savoir si le consentement au traitement de données dans le cadre d'un essai clinique peut être considéré au même titre qu'un consentement conditionnel à l'accès à un service ? De plus, faut-il concevoir plusieurs consentements dans les essais cliniques en fonction des différents traitements de données comme la collecte et la communication à des tiers, avec toutes les difficultés que cela susciterait en pratique, afin d'accentuer la transparence des traitements et renforcer leur base de licéité ?

[65] Groupe 29, Lignes directrices sur le consentement sous le Règlement 2016/679, adopté le 28 novembre 2017 et revu et adopté en dernier le 10 avril 2018, WP 259 rev.01, p. 23, pp. 27 et s.

En toute hypothèse, il ne faut pas oublier que la représentation d'un enfant mineur d'âge en matière personnelle est encadrée par la Convention de New-York du 20 novembre 1989 relative aux droits de l'enfants[66] et puis par les règles de chaque État membre en matière de capacité d'exercice des enfants mineurs d'âge. À cet égard, la règle généralement admise est que *l'infans* est représenté par ses parents, que l'enfant jusqu'à 15-16 ans est assisté par ses parents dans les décisions personnelles et, qu'à partir de cet âge, il prend seul les décisions importantes en matière personnelle, étant entendu qu'un certain nombre de décisions très personnelles ne sont susceptible d'aucune représentation, quel que soit l'âge de l'enfant (comme le mariage, la vie amoureuse ou sexuelle et le choix de ses relations personnelles – les amis, par exemple).

43. Le RGPD ne règle pas non plus la question du sort à réserver au consentement donné par des parents au nom et pour compte de leur enfant mineur d'âge lorsque ce dernier devient majeur. Le consentement demeure-t-il valide ou faut-il rechercher le consentement de l'enfant devenu majeur ? En matière de recherche clinique, la règle veut qu'il faille rechercher le consentement de ce dernier ou, à tout le moins, lui donner la possibilité de s'opposer à la poursuite de l'essai. Il n'existe aucune raison de ne pas appliquer, *mutatis mutandis*, la même règle en matière de traitement de données. Le consentement ainsi donné par les parents devrait cesser de produire ses effets au jour de la majorité de l'enfant. La règle est impitoyable mais elle est la conséquence logique de l'approche irréaliste adoptée par le Comité (et quelque part par le RGPD et la directive 95/46/CE auparavant) d'un consentement idéalisé qui n'existe pas dans le monde réel.

Ceci étant, si la personne concernée retire son consentement au traitement de données qui la concernent, cela n'invalide pas les traitements passés. Cela s'oppose uniquement à la poursuite des traitements de données. Ce point a été confirmé par le RGPD.

44. Enfin, la question du sort à donner au consentement obtenu sous l'empire de la directive 95/46/CE est incertain. Le considérant n° 171 du RGPD énonce à ce sujet que « [l]es traitements déjà en cours à la date d'application du présent règlement devraient être mis en conformité avec celui-ci dans un délai de deux ans après son entrée en vigueur. Lorsque le traitement est fondé sur un consentement en vertu de la directive 95/46/CE, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la

[66] Voy. déjà art. 12 (droit d'exprimer librement son opinion sur toute question l'intéressant) 13 (liberté d'expression) ou 16 (droit au respect de la vie privée).

manière dont le consentement a été donné est conforme aux conditions énoncées dans le présent règlement, de manière à ce que le responsable du traitement puisse poursuivre le traitement après la date d'application du présent règlement. Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées ». Le Comité ne dit pas autre chose : le consentement est toujours valable à condition d'être conforme aux conditions posées par le RGPD. Autrement dit, il n'est pas possible de soutenir que les consentements obtenus sous le couvert de la directive 95/46/CE seront tous considérés comme demeurant valides au-delà du 25 mai 2018. Pour être plus précis, ce n'est pas que le consentement obtenu antérieurement ne serait plus valide ; en réalité, il ne peut plus produire d'effet juridique s'il n'est pas conforme aux nouvelles règles. Cette solution est conforme aux règles usuelles en matière d'application des lois dans le temps : en règle, la validité d'un acte s'apprécie au jour de la formation de celui-ci. En conséquence, la validité des actes passés avant le 25 mai 2018 devrait s'apprécier au regard de la législation applicable adoptée en transposition de la directive 95/46/CE, au jour de la formation de cet acte. Par contre, l'adoption d'une nouvelle règlementation peut modifier les effets juridiques à produire par cet acte à partir de l'entrée en vigueur de celle-ci.

SECTION 5. – Quelques nouvelles obligations à charge du responsable du traitement et du sous-traitant dans le secteur de la santé

45. Alors que, sous la directive 95/46/CE, le responsable du traitement devait choisir un sous-traitant qui apportait « des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer » et qu'il devait veiller au respect de ces mesures par le sous-traitant, le RGPD exige maintenant que le responsable du traitement choisisse un sous-traitant qui présente « des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du [Règlement] et garantisse la protection des droits de la personne concernée »[67].

[67] Art. 28, 1 du RGPD.

46. Il faut rappeler que l'idée de base est de garantir l'étanchéité du circuit du traitement des données (sa confidentialité) et par là, la protection de la personne concernée. Le sous-traitant ne peut donc pas être un panier percé (dans tous les sens du terme d'ailleurs). À cet effet, il doit prouver au responsable du traitement qu'il est en mesure de réaliser la mission que ce dernier entend lui confier, d'une manière qui soit totalement conforme au RGPD. Ceci peut se faire par la preuve de la conformité de ses activités à un code de conduite (le cas échéant approuvé) ou par la certification de ses activités[68]. Sous la législation précédente, les codes de conduite et les mécanismes de certification n'ont pas vraiment prospéré. Il reste à espérer que les temps changent et que ces nouveaux métiers de la société de l'information prennent enfin leur envol.

De manière générale, la sous-traitance de données doit être régie par un contrat (ou tout acte juridique) qui lie le responsable du traitement et le sous-traitant. Ce contrat (ou cet acte) doit, principalement, définir l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et fixer les obligations et les droits du responsable du traitement[69].

D'ailleurs, il ne serait pas vain d'exiger que les activités du sous-traitant soient couvertes par une assurance qui garantirait la couverture de tout dommage qui affecterait la personne concernée, sans que celle-ci n'ait à rapporter la preuve d'une faute dans le chef du responsable du traitement ou du sous-traitant. Ce serait une véritable garantie de sérieux, d'autant plus si les compagnies d'assurance s'assurent alors elles-mêmes des garanties offertes par le sous-traitant.

Une fois identifié, le sous-traitant doit se conformer à une série d'obligations dont l'intensité est liée aux caractéristiques du traitement de données en cause.

§ 1. Les obligations en matière de sécurité

47. Le RGPD a renforcé les dispositions relatives à la sécurité des traitements en reprenant des dispositifs déjà présents dans d'autres législations européennes comme la directive 2002/58/CE 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). Il met à charge, tant du responsable du traitement que du sous-traitant, la mise en œuvre de « mesures techniques

[68] Voy. art. 40 et s. du RGPD.

[69] Voy. art. 28, 3°, du RGPD pour le surplus.

et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque », « compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques »[70].

L'on voit donc, d'entrée de jeu, que le sous-traitant est un acteur (pro)actif dans la sécurité nécessaire à la confidentialité du traitement de données à caractère personnel. Afin de donner quelques pistes, le RGPD fixe ainsi une série de mesures à prendre, le cas échéant, à savoir :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- la mise en œuvre des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- la mise en œuvre des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- l'existence de procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles destinées à assurer la sécurité du traitement.

L'on constate que nombre de ces mesures sont, techniquement, à charge, partiellement ou totalement, du sous-traitant en fonction de ses compétences spécifiques et de son intervention réelle dans le traitement. Il doit ainsi garantir la sécurité, et corrélativement la confidentialité, du traitement – même s'il est vrai que le responsable de traitement est, en principe, le premier et seul interlocuteur de la personne concernée, ici le patient.

48. Par ailleurs, « le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée [légalement] »[71]. Ces mesures doivent être tant techniques (*access management*, etc.) qu'organisationnelles (formation, règlement d'ordre intérieur, etc.).

D'un *point de vue organisationnel* au niveau du sous-traitant, ce dernier doit s'assurer que les personnes agissant sous son autorité soient

[70] Art. 32 du RGPD.
[71] Art. 32.4 du RGPD.

informées des dispositions du RGPD[72]. Il doit également veiller à mettre en place une structure ou une organisation pour éviter la perte de données, des destructions ou modifications de données non autorisées, des accès non autorisés, etc. En d'autres termes, il doit prendre des dispositions en termes d'organisation qui garantiront la personne concernée contre de tels faits. Par exemple, le sous-traitant – au même titre que le responsable de traitement au demeurant – doit s'assurer que seules les personnes devant effectivement avoir accès à des données à caractère personnel y ait effectivement accès, à l'exclusion des autres. Il lui appartient donc de prévoir une organisation adéquate et efficace.

Ce niveau organisationnel se retrouve également au stade de la formation des personnes à n'accéder qu'aux données à caractère personnel dont elles ont réellement besoin. Par exemple, en matière de données relatives à la santé, le sous-traitant devra s'assurer que son personnel n'accède aux données relatives à des patients que si, et seulement si, sa mission le requiert. Si tel n'est pas le cas, il devra s'en abstenir au risque de se trouver confronté à de très lourdes sanctions….

Au niveau technique, le sous-traitant doit s'assurer qu'il a mis en place des mesures adéquates de protection de ses traitements d'un point de vue technique. Ainsi, il doit s'assurer que son système informatique réunit les conditions nécessaires pour éviter toute intrusion non autorisée via une bonne gestion d'accès, toute perte, destruction ou modification de données, etc. À noter que la notion de sécurité s'entend aussi des accès physiques au réseau informatique du responsable de traitement. Il faudra donc être attentif à ce que l'accès au serveur, par exemple, soit réglementé et ouvert aux seules personnes pour qui cela représente une nécessité. Il serait inutile de prévoir des règles strictes d'accès aux données si le serveur contenant ces données n'était pas suffisamment protégé et si, en conséquence, son contenu venait à être subtilisé…

49. L'ensemble de ces éléments doivent se retrouver dans le contrat de sous-traitance qui sera signé entre le responsable de traitement et son sous-traitant.

§ 2. L'obligation de notifier ou de communiquer les failles de sécurité

50. Si, d'aventure, une faille de sécurité devait intervenir, le responsable du traitement doit procéder à une notification à l'autorité de

[72] Art. 32.4 du RGPD.

contrôle nationale dans tous les cas et à la personne concernée dans certaines situations. Le Comité a, dans des lignes directrices[73], préciser les situations dans lesquelles une telle notification doit intervenir. Ainsi, le Comité précise que l'analyse du risque doit prendre en considération la sévérité du risque d'atteinte aux droits et liberté des personnes concernées[74]. En d'autres termes, toutes les failles de sécurité ne doivent pas être notifiées mais uniquement celles qui présente une certaine sévérité.

51. L'on doit relever que si le sous-traitant a connaissance d'une faille de sécurité, il doit le notifier au responsable du traitement dans les meilleurs délais après cette prise de connaissance[75]. En outre et, afin de permettre au responsable du traitement de remplir son obligation de notification/communication, le sous-traitant a une obligation de documenter complètement l'incident. En conséquence, le contenu de ces notification/communication sera nourri ou documenté par le sous-traitant. Cette documentation produite par le sous-traitant doit être de nature à permettre au responsable du traitement d'évaluer s'il peut bénéficier des exceptions de devoir procéder à la communication à la personne concernée prévues par le RGPD.

52. Le responsable du traitement serait bien avisé de fixer un délai maximum dans lequel son sous-traitant doit lui notifier la faille via une clause su type « … dans les meilleurs délais et au plus tard dans les x heures de la prise de connaissance de la faille de sécurité ».

§ 3. L'obligation de recourir aux services d'un Délégué à la protection des données

53. Le RGPD a repris et renforcé le rôle et la fonction du détaché à la protection des données devenu le Délégué à la protection des données (en abrégé DPO pour *Data protection officer*)[76]. Il s'agit d'une fonction importante au sein de l'organisation du responsable du traitement mais également du sous-traitant dès lors qu'il doit vérifier, entre autres, le respect du RGPD par ce dernier.

[73] Groupe 29, Guidelines on Personal data breach notification under Regulation 2016/679, WP 250 rev.01.

[74] *Ibid.*, p. 23.

[75] Art. 33.2 du RGPD.

[76] Art. 37 et s. du RGPD.

54. Tout responsable du traitement et tout sous-traitant doivent nommer un DPO dans les hypothèses suivantes :

- le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;
- les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou
- les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données sensibles et de données à caractère personnel relatives à des condamnations pénales et à des infractions.

Ces critères sont assez flous hormis celui qui se réfère aux catégories particulières de données comme les données relatives à la santé. Le Comité en a précisé les contours[77]. Ainsi, à titre d'exemples :

- le Comité considère comme "**activité de base**" le traitement de données relatives à la santé par un hôpital. Cette analyse doit, à notre sens, être reprise pour tout sous-traitant dont l'activité de base est d'assister le responsable du traitement dans ce type de traitement ;
- il en va de même pour le concept de "**grande échelle**" dès lors que le Comité prend, comme exemple, l'hôpital qui traite des données relatives aux patients dans le cours régulier de ses activités. Cela est transposable pour un sous-traitant dans un tel traitement. Par contre, le médecin lui-même est exclu.

Le DPO peut être soit interne à la structure du responsable du traitement ou du sous-traitant soit externe. Le DPO peut également travailler pour plusieurs responsables du traitement ou sous-traitants mais doit, à notre sens, être transparent à ce sujet.

55. Appliqué au niveau de la sous-traitance dans le domaine médical, on pourrait imaginer le cas d'un responsable du traitement qui ne soit pas soumis à l'obligation de désignation d'un DPO (comme par exemple, les médecins généralistes) mais que le sous-traitant le soit au regard des critères mis en place par le Comité. Cela sera le cas, par exemple, pour un fournisseur de service de *cloud computing* qui traiterait, comme sous-traitant, des données relatives à la santé à grande échelle pour plusieurs médecins, ce qui est de plus en plus fréquent dans les programmes de

[77] Groupe 29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01.

gestion de patientèle qui utilisent le *cloud*. Il en est de même pour les réseaux de santé qui, comme sous-traitants des hôpitaux ou autres professionnels de santé ; doivent nommer un DPO compte tenu du fait qu'il y a un traitement à grande échelle de catégories particulières de données.

56. Le DPO remplit une réelle fonction au sein de l'organisation du responsable du traitement dès lors que[78] :

- il doit être associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel ;
- il doit recevoir les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et les moyens d'entretenir ses connaissances spécialisées ;
- il ne reçoit aucune instruction en ce qui concerne l'exercice des missions. Le DPO doit, en effet, remplir sa fonction en toute indépendance, ce qui explique qu'il « ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions »[79] ;
- il doit être un point de contact pour l'autorité de contrôle et la personne concernée.

57. Par ailleurs, le DPO doit avoir les qualités professionnelles et, en particulier, des connaissances spécialisées du droit et des pratiques en matière de protection des données nécessaires pour exercer sa fonction et remplir les missions qui sont les siennes.

Concernant les qualités professionnelles, doit-on en exiger des particulières dans le cadre de traitement de données relatives à la santé ou peut-on se satisfaire des critères habituels ? Il nous semble que la catégorie à laquelle appartiennent les hôpitaux exigent que le DPO ait une connaissance minimale de la législation relative à cette matière outre le RGPD afin de pouvoir remplir adéquatement sa mission. Pour le dire autrement, il doit connaître les droits du patient, l'organisation des circuits d'information au sein des hôpitaux, les règles relatives aux dossiers de patients, sans parler des règles relatives à la communication de données à des fins de santé publique et de financement des soins de santé.

[78] Art. 38 du RGPD.
[79] Art. 38.3 du RGPD.

§ 4. L'obligation de tenir un registre des activités de traitement

58. Le RGPD a supprimé l'obligation, dans le chef du responsable du traitement, de notifier à l'autorité de contrôle toute une série d'informations à propos des traitements de données qu'il entendait réaliser. Cependant, en contrepartie de cette suppression, le responsable du traitement doit tenir un registre des activités de traitement effectuées sous sa responsabilité reprenant un certain nombre d'informations précisées à l'article 30 du RGPD.

Cette obligation n'est pas applicable à une entreprise ou organisation comptant moins de 250 employés sauf si le traitement effectué « est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 »[80].

59. Une telle obligation, et cela est également nouveau, est aussi mise à charge du sous-traitant qui doit tenir « un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant[81] :

a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données ;

b) les catégories de traitements effectués pour le compte de chaque responsable du traitement ;

c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;

d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1 ».

[80] Art. 30.5 du RGPD.
[81] Art. 30. 2 du RGPD.

L'exception à cette obligation telle qu'elle existe pour le responsable du traitement est également applicable pour le sous-traitant.

L'on doit cependant bien constater que le sous-traitant de traitement de données relatives à la santé ne pourra jamais bénéficier de l'exception dès lors qu'il ne s'agit pas d'un traitement « occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1 »[82].

CHAPITRE 2. Les droits de la personne concernée dans le secteur de la santé

60. Si la directive 95/46/CE ne reconnaissait formellement que trois droits à la personne concernée (le droit d'accès, le droit de s'opposer au traitement de données et le droit de ne pas être soumis à des décisions individuelles automatisées), le RGPD lui en reconnaît huit (le droit à l'information, le droit d'accès, le droit à la rectification, le droit à l'effacement, le droit à la limitation du traitement, le droit à la portabilité des données, le droit de s'opposer au traitement de données et le droit de ne pas être soumis à des décisions individuelles automatisées) sans qu'il ne soit possible de savoir si cette augmentation formelle de leur nombre va induire une augmentation de la protection des données et une plus grande participation des individus à la société de l'information[83]. Le droit à la transparence et à l'information, le droit d'accès, le droit à la portabilité des données et le droit à ne pas être soumis à une décision automatisée retiennent présentement l'attention.

[82] *Ibid.*

[83] Voy. les limitations qui peuvent être apportées à ces droits par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis, par la voie de mesures législatives, conformément à l'article 23 du RGPD. Ces limitations ne sont admissibles que si elles respectent l'essence des libertés et droits fondamentaux et qu'elles constituent des mesures nécessaires et proportionnées dans une société démocratique pour garantir l'un des objectifs énumérés par cette disposition.

SECTION 1. – Le droit à la transparence et à l'information

61. Le principe de la transparence, affirmé dès les débuts de la protection des données[84], se retrouve dans la directive 95/46/CE comme dans la Convention du 28 janvier 1981. Il signifie que la personne concernée a le droit, fondamental, de savoir ce qui est su à son propos, par qui, pour quoi et comment. La directive distinguait à cet égard entre deux hypothèses : celle où les données étaient collectées auprès de la personne concernée et celle où les données n'étaient pas collectées auprès de la personne concernée. Elle tenait compte des objections habituelles des agents de l'activité économique soucieux d'éviter toute sorte de charges économiques ou opérationnelles, en leur offrant la possibilité de se soustraire à cet aspect primordial de la protection des données en leur permettant, dans tous les cas, de jouer sur ce qui était requis pour assurer un traitement loyal des données, et, lorsque les données n'étaient pas collectées auprès de la personne concernée, en invoquant le caractère impossible ou disproportionné de l'obligation (ce qui était bien commode) et sans que la directive ne songe à préciser si le contrôle à opérer sur cette objection devait être renforcé ou, au contraire, marginal[85].

62. Le RGPD a mis en exergue le principe de la transparence et a en souligné l'importance : sans ce principe, il n'est pas possible de mettre en œuvre la protection des données, que ce soit dans le chef de la personne concernée ou des autorités. Le RGPD insiste, à juste titre, sur les conséquences qu'il faut en tirer[86].

D'abord, lorsque le responsable du traitement doit communiquer de l'information à la personne concernée, il doit le faire d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour les informations spécifiquement destinées aux enfants. Ces informations doivent être fournies par écrit ou par d'autres moyens y compris par voie électronique lorsque c'est approprié, mais la personne concernée peut demander que ces informations lui soient fournies oralement. Dans ce cas, le responsable du traitement doit s'assurer de l'identité de la personne concernée autrement que par une déclaration orale de celle-ci (quoique cela puisse bien vouloir dire).

---

[84] Voy. déjà les conclusions de la 7e Conférence des Ministres européens de la justice, Bâle, 15-18 mai 1972, Strasbourg, 5 juin 1972, CMJ/Conc. (72) 1.

[85] Sans compter les exceptions et limites que la directive 95/46/CE permettait d'y apporter par ailleurs dans une certaine mesure (voy. a rt. 13 de la directive 95/46/CE).

[86] Voy. art. 12 du RGPD.

Ensuite, le responsable du traitement doit faciliter l'exercice des droits de la personne concernée. À propos des traitements qui ne requièrent pas l'identification de la personne concernée, le responsable du traitement ne peut pas refuser de donner suite à une demande d'exercice des droits *sauf s'il démontre qu'il n'est pas en mesure d'identifier la personne concernée* qui s'est adressée à lui (sic)[87]. En tout état de cause, le responsable du traitement doit informer la personne concernée des suites réservées à sa demande et ce, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande[88]. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes[89]. Lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies par voie électronique lorsque cela est possible, à moins que la personne concernée ne demande qu'il en soit autrement. Si le responsable du traitement *ne donne pas suite* (?) à la demande formulée par la personne concernée, il doit l'informer sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande, des motifs de son refus et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel. La règle veut que l'information et l'exercice des droits la personne concernée soient *gratuits* dans le chef de celle-ci ; le responsable du traitement ne peut lui exiger aucun paiement à quelque titre que ce soit. Par contre, le responsable du traitement peut refuser de donner suite aux demandes manifestement infondées ou excessives (notamment en raison de leur répétition abusive) ou exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées[90].

63. Les principes de la transparence et du droit à l'information sur le traitement de données rejoignent les droits du patient dans le contexte de la relation thérapeutique, en lui donnant les moyens d'agir. Il faut toutefois bien apercevoir que les informations à fournir à ce titre ne se

[87] La disposition veut sans doute dire s'il n'est pas en mesure d'identifier les données qui concernent la personne qui souhaite exercer ses droits puisque, s'il est approché par la personne concernée, le responsable du traitement connait nécessairement son identité.

[88] Quand le responsable du traitement a des doutes raisonnables sur l'identité de la personne concernée, il peut demander des informations supplémentaires nécessaires pour confirmer son identité (voy. art. 12.6 du RGPD).

[89] Le responsable du traitement doit informer la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.

[90] C'est au responsable du traitement de prouver le caractère infondé ou excessif de la demande formée par la personne concernée.

confondent pas avec les informations dues au patient dans le cadre de l'obtention de son consentement éclairé à l'acte médical ou à la participation à un essai clinique. Ce sont des choses distinctes dans leur objet et dans leur règlementation. À notre sens, la véritable question à traiter est celle de savoir jusqu'où il faut informer le patient en matière de traitement de données. Il ne semble pas excessif d'exiger que le patient soit spontanément informé de l'identité des sous-traitants auxquels il serait fait appel (par exemple, une information sur le laboratoire qui réaliserait les analyses médicales en cette qualité), de l'identité du fournisseur de services qui hébergerait les données du patient, des catégories de personnes qui seraient susceptibles d'avoir accès à ses données, etc. Fournir cette information contribuerait, en outre, à renforcer sa confiance dans le système de santé publique.

Comme la directive 95/46/CE, le RGPD distingue l'information due par le responsable du traitement à la personne concernée selon que les données sont ou non collectées auprès de la personne concernée. Dans les deux hypothèses, les informations à communiquer peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu. Lorsque les icônes sont présentées par voie électronique, elles sont lisibles par machine[91].

Au moment même où les données sont obtenues auprès de la personne concernée, le responsable du traitement doit lui fournir un socle de base d'informations[92] auxquelles il faut ajouter les informations complémentaires qui seront nécessaires pour garantir un traitement équitable et transparent[93], sauf à ce que la personne concernée dispose déjà de ces informations[94].

64. Lorsque les données ne sont pas collectées auprès de la personne concernée, le régime de l'information à fournir par le responsable du traitement à la personne concernée a été substantiellement revu[95].

[91] Art. 12.7 du RGPD. En vertu de l'article 12.8 du Règlement, la Commission est habilitée à adopter des actes délégués aux fins de déterminer les informations à présenter sous la forme d'icônes ainsi que les procédures régissant la fourniture d'icônes normalisées.

[92] Voy. art. 13.1 du RGPD.

[93] Voy. art. 13.2 du RGPD.

[94] Voy. art. 13.4 du RGPD. Lorsqu'il a l'intention d'effectuer un *traitement ultérieur* des données à caractère personnel *pour une finalité autre* que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information complémentaire qui serait nécessaire (art. 13.3 du RGPD).

[95] Art. 14 du RGPD.

Comme dans l'hypothèse précédente, le responsable du traitement doit fournir à la personne concernée un socle de base d'informations[96] auxquelles il faut ajouter les informations complémentaires qui seront nécessaires pour garantir un traitement équitable et transparent[97]. Ces informations doivent être fournies dans un délai raisonnable après avoir obtenu les données à caractère personnel. Ce caractère raisonnable s'apprécie au regard des circonstances particulières dans lesquelles les données à caractère personnel sont traitées mais, en tout état de cause, il ne peut pas dépasser un mois. Dans l'hypothèse où les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, ces informations doivent lui être fournies au plus tard au moment de la première communication. S'il est envisagé de communiquer les informations à un autre destinataire, ces informations doivent lui être fournies au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois[98]. De manière regrettable, selon nous, les possibilités de se soustraire à l'information de la personne concernée ont été maintenues et, dans une certaine mesure, élargies[99].

---

[96] Voy. art. 14.1 du RGPD.

[97] Voy. art. 14.2 du RGPD.

[98] Voy. art. 14.3 du RGPD. Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues, le responsable du traitement doit, au préalable, fournir à la personne concernée des informations au sujet de cette autre finalité et toute autre information supplémentaire pertinente.

[99] Le responsable du traitement peut se soustraire à cette obligation, pourtant fondamentale, dans les hypothèses suivantes (art. 14.5 du RGPD) :

1° lorsque la personne concernée dispose déjà de ces informations ;

2° lorsque la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sous réserve des conditions et garanties visées à l'article 89.1 du RGPD, ou dans la mesure où cette obligation est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles ;

3° lorsque l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée ;

4° ou lorsque les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membre, y compris une obligation légale de secret professionnel.

SECTION 2. – Le droit d'accès aux données relatives à la santé

65. Si le responsable du traitement est obligé de fournir de l'information à la personne concernée, celle-ci est aussi en droit de l'interpeller pour obtenir des informations sur le traitement de données qui la concernent[100] et pour obtenir l'accès aux données qui le concernent et qui font l'objet d'un traitement. La première information que la personne concernée est en droit d'exiger du responsable du traitement est de savoir si des données qui la concernent font ou non l'objet d'un traitement. Dans l'affirmative, la personne concernée a le droit d'accéder aux données qui la concernent, ainsi que le droit d'obtenir des informations[101].

66. Il demeure à s'entendre sur ce que signifie *accéder aux données* ainsi que sur la *manière d'exercer cet accès*, dans le secteur de la santé, ce qui renvoie au sempiternel débat sur l'accès direct ou indirect. En tout cas, la personne concernée a le droit de demander et d'obtenir une copie des données traitées. Lorsque la personne concernée présente sa demande par voie électronique, les informations sont fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement. Le responsable du traitement ne peut pas exiger de paiement à ce titre sauf lorsque la personne concernée demande une copie supplémentaire. Dans ce cas, le responsable du traitement ne peut pas demander plus que le paiement de frais raisonnables tels que ceux-ci sont calculés sur la base des coûts administratifs[102]. Le RGPD précise que le droit d'obtenir une copie des données ne doit pas porter atteinte aux droits et libertés d'autrui[103], ce qui est susceptible de causer des difficultés d'interprétation et de mise en œuvre en matière de données relatives à la santé.

67. Comme auparavant, la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données qui la concernent et qui sont inexactes. Compte tenu des finalités poursuivies par leur traitement, la personne concernée a le droit d'obtenir que les données incomplètes soient complétées, y compris en

[100] Il faut toutefois noter l'asymétrie dans le contenu de l'information selon qu'elle doit être fournie par le responsable du traitement ou qu'elle soit demandée par la personne concernée.

[101] Voy. art. 15.1 et 2 du RGPD.

[102] Art. 15.3 du RGPD.

[103] Art. 15.4 du RGPD.

fournissant une déclaration complémentaire[104]. Toute la question est de savoir ce qu'est une donnée inexacte en matière de santé…

68. Le droit d'accès est aussi utile pour permettre à la personne concernée d'exercer son droit à l'oubli. Celui-ci peut toutefois entrer en conflit avec les obligations de conservation des données imposées aux praticiens professionnels et autres institutions intervenant dans le système de santé publique.

La personne concernée dispose du droit, *spécial*, de s'opposer au traitement de ses données pour des raisons tenant à sa situation particulière, et elle dispose du droit, *général*, de s'opposer au traitement de ses données à des fins de prospection. L'existence de ce double droit doit être explicitement portée à l'attention de la personne concernée, au plus tard au moment de la première communication avec la personne concernée. Il doit lui être présenté clairement et séparément de toute autre information[105].

Comme auparavant sous la directive 95/46/CE, la personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données ou un profilage réalisé dans le cadre de l'exécution d'une mission d'intérêt public ou qui relève de l'exercice de l'autorité publique dont est investi le responsable du traitement[106]. La personne concernée peut aussi s'opposer au traitement de données ou au profilage réalisé dans la poursuite des intérêts légitimes du responsable du traitement ou d'un tiers. Suite à l'opposition de la personne concernée, le responsable du traitement ne peut plus traiter les données, à moins qu'il ne démontre l'existence de motifs légitimes et impérieux qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou que le traitement est nécessaire pour la constatation, l'exercice ou la défense de droits en justice.

---

[104] Art. 16 du RGPD. Autrement dit, la personne concernée est associée à la réalisation des finalités poursuivies par le responsable du traitement, ce qui induit, quelque part, un renversement des rôles. Le responsable du traitement doit notifier à chaque destinataire auquel les données ont été communiquées toute rectification effectuée, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement doit fournir à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande (art. 19 du RGPD).

[105] Voy. art. 21 du RGPD. Dans le cadre de l'utilisation de services de la société de l'information, et nonobstant la directive 2002/58/CE, la personne concernée peut exercer son droit d'opposition à l'aide de procédés automatisés utilisant des spécifications techniques.

[106] Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques, la personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, au traitement de données à caractère personnel la concernant, à moins que le traitement ne soit nécessaire à l'exécution d'une mission d'intérêt public (art. 21.6 du RGPD).

Le droit de droit de s'opposer au traitement de ses données pour des raisons tenant à sa situation particulière peut se révéler difficile à mettre en œuvre en droit de la santé surtout en ce qui concerne la composition et la gestion du dossier tenu au nom du patient.

SECTION 3. – Le droit à la portabilité appliqué aux données relatives à la santé

69. Le RGPD prévoit expressément, et c'est nouveau, que lorsque les données sont traitées sur base de son consentement ou d'un contrat, et à l'aide de procédés automatisés, la personne concernée a le droit de demander et de recevoir du responsable du traitement, dans un format structuré, couramment utilité et lisible par machine, les données qu'elle lui a fournies. La personne concernée peut, ensuite, les transmettre à un autre responsable du traitement. Elle peut aussi demander au premier responsable du traitement de les transmettre directement à un autre responsable du traitement si la technique le permet[107].

En dehors de ces deux hypothèses, consentement et contrat, le droit à la portabilité n'existe pas, pas plus qu'en ce qui concerne les dossiers papier[108]. Il ne s'applique donc pas au dossier tenu au nom du patient sur base d'une obligation légale ou déontologique ou à des fins thérapeutiques. S'il est considéré que la tenue du dossier s'inscrit dans une relation contractuelle ou est rendue possible grâce au consentement du patient, le droit à la portabilité trouvera à s'appliquer.

70. Une autre difficulté en matière d'exercice de droit à la portabilité consiste à déterminer les données qui sont portables. Ce droit recouvre, incontestablement, les données effectivement fournies par la personne concernée au responsable du traitement. Mais couvre-t-il les observations enregistrées par le praticien professionnel ou le résultat des examens auxquels le patient aurait été soumis ? De manière générale, le Comité considère que les données fournies par la personne incluent celles qui découlent de l'observation de ses activités. Par contre, il rejette les données générées

[107] Voy. art. 20 du RGPD. Ce droit est sans préjudice du droit à l'effacement ou à l'oubli. Ce droit ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Il ne peut pas non plus porter atteinte aux droits et libertés de tiers.

[108] Groupe 29, Lignes directrices relatives au droit à la portabilité des données, adoptées le 13 décembre 2016, révisées et adoptées le 5 avril 2017, WP 242 rev.01, pp. 10 et s.

par le responsable du traitement fut-ce à partir des données observées ou fournies directement par la personne concernée[109]. Il donne, d'ailleurs, expressément le cas d'une appréciation relative à la santé d'un utilisateur. Le Comité exclut les données déduites ou dérivées, ce qui comprend les données créées par un prestataire de service. Toutefois, souvent, le droit de la santé va prévoir des obligations en termes de communication de ces données entre praticiens professionnels qui interviennent dans la prise en charge d'un même patient, dans le respect des règles en matière de secret professionnel partagé. Pour le dire autrement, le droit à la portabilité des données du patient existait déjà, *mutatis mutandis*, en droit de la santé, et le RGPD n'y porte pas atteinte.

SECTION 4. – Le droit de ne pas être soumis à des décisions automatisées

71. La directive 95/46/CE reconnaissait le droit à toute personne de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité[110], sauf lorsque la décision était autorisée par une loi qui précisait les mesures visant à garantir la sauvegarde de l'intérêt légitime de la personne concernée et lorsque la décision était prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées (telles que la possibilité de faire valoir son point de vue) garantissent la sauvegarde de son intérêt légitime. Concrètement, ces décisions individuelles automatisées visaient, par exemple, les logiciels de vérification de la couverture d'un assuré social.

72. Sous l'empire du RGPD, la personne concernée a toujours le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, en ce compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire[111].

[109] Groupe 29, Lignes directrices relatives au droit à la portabilité des données, adoptées le 13 décembre 2016, révisées et adoptées le 5 avril 2017, WP 242 rev.01, p. 12.

[110] Art. 15 de la directive 95/46/CE. La directive fournit comme exemples d'aspects de la personnalité, le rendement professionnel, le crédit, la fiabilité ou le comportement de la personne concernée.

[111] Voy. art. 22 du RGPD.

Comme auparavant, ce droit ne peut pas être invoqué lorsque la décision automatisée est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, ou qu'il est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, ou qu'il est fondée sur le consentement explicite de la personne concernée.

Toutefois, les décisions automatisées ne peuvent pas se fonder sur des catégories particulières de données, à moins que la personne concernée n'ait donné son consentement explicite ou que le traitement ne soit nécessaire pour des motifs d'intérêt public important et que, dans les deux hypothèses, des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée soient mise en œuvre. Il semble donc que les logiciels de vérification de la couverture d'un assuré social soient dès lors toujours autorisés.

Lorsque la *décision* est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ou lorsque la *décision* est fondée sur le consentement explicite de la personne concernée, le responsable du traitement doit mettre en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins le droit d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.

CHAPITRE 3. L'effectivité de la protection des données dans le secteur de la santé

SECTION 1. – La multiplication des autorités de contrôle

73. Les activités dans le secteur de la santé sont très règlementées et, souvent, les règlementations applicables prévoient la création et l'intervention d'une autorité de contrôle spécifique pour assurer son effectivité. L'ennui est que les autorités s'accumulent. Toute la question est de savoir s'il ne faudrait pas songer, un jour, à rationaliser le nombre d'autorités de contrôle susceptibles d'intervenir dans le secteur de la santé. L'exemple le plus marquant est celui du nombre d'autorités ou d'organes susceptibles de se prononcer, peu ou prou, sur la question de la protection des données

dans un projet de recherche en matière biomédicale : le conseiller en sécurité, le délégué à la protection des données, l'organisation professionnelle dont dépendent les praticiens impliqués, l'autorité nationale de contrôle en matière de protection des données et le comité éthique ou le ministère qui doivent autoriser la rechercher biomédicale. Il existe, bien entendu, d'excellentes raisons à l'intervention de toutes ces autorités et organes mais, dans la réalité, leur multiplicité alourdit de manière inutile la réalisation de toute une série d'activités qui sont pourtant très importantes et qui gagneraient à pouvoir être gérées plus efficacement.

SECTION 2. – La mise en œuvre des pénalités

74. L'imposition d'amendes administratives conséquentes est un des points régulièrement mis en avant dans la mise en œuvre du RGPD. Il faut toutefois distinguer entre le « simple » responsable de traitement et celui qui est en même temps une « entreprise » au sens du RGPD, et rappeler qu'il appartient à chaque État membre d'établir les règles qui déterminent si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire[112]. Ceci signifie, en bref, que le « simple » responsable de traitement encourt jusqu'à 100 ou 200.000 euros d'amendes tandis que l'entreprise risque une amende jusqu'à 2 à 4 % de son chiffre d'affaire annuel mondial, alors que les acteurs du secteur public sont exonérés de toute amende si celle-ci n'est pas prévue par le droit de l'État membre concerné. Dans le secteur de la santé, un grief de discrimination pourrait être utilement articulé par les hôpitaux privés qui seraient susceptibles d'encourir pareilles amendes alors que leurs homologues du secteur public y échapperaient en l'absence de disposition spéciale adoptée en ce sens par l'État membre concerné.

75. Par ailleurs, l'imposition d'amendes administratives dans le secteur de la santé est de nature à poser un réel problème quant à son opportunité. En effet, il arrive souvent que les hôpitaux fonctionnent sur base d'enveloppes budgétaires fermées et qu'il n'existe pas d'article budgétaire dans le cadre de leur financement couvrant les hypothèses d'amende administrative pour violation de la protection des données. La question qui se pose alors est de savoir d'où va provenir l'argent nécessaire pour payer ces amendes. Il n'existe, dans ce cas, *mutatis mutandis* comme pour le

[112] Voy. art. 83.7 du RGPD.

paiement de la fonction de délégué à la protection des données et la mise en conformité avec le RGPD, qu'une seule réponse : l'hôpital va devoir divertir des fonds de son budget ordinaire ou extraordinaire pour payer les amendes éventuelles. L'imposition d'amendes administratives à un hôpital va donc se faire au détriment de la qualité des soins et des infrastructures. Autrement dit, c'est le patient qui va payer les amendes administratives par une diminution des soins susceptibles de lui être offerts par l'hôpital. Assurément, c'est la même chose pour les consommateurs mais l'impact est plus sensible dans le secteur de la santé.

Conclusions

76. La mise en œuvre du RGPD est un véritable défi pour les acteurs des soins de santé dont toutes les conséquences sont loin d'avoir été identifiées par les auteurs du RGPD.

Il faut en tout cas retenir que les règles relatives au secret professionnel ne sont pas modifiées par le RGPD et le consentement de la personne concernée au traitement de données qui la concernent ne libère pas, à ce titre, le praticien professionnel de son obligation au secret.

Si le RGPD fournit une définition des données relatives à la santé, il aurait mieux fallu, à notre sens, retenir une définition stricte et objective de la notion de données relatives à la santé qui se limite aux informations qui contiennent un élément de connaissance sur l'état de santé d'une personne (physique), excluant par là toute velléité d'étendre la notion à des données qui ne contiennent aucune information sur l'état de santé d'une personne même s'il est possible d'en déduire (en raison notamment de la finalité poursuivie ou du contexte). Il faut rappeler que les données relatives à la santé ne doivent pas nécessairement émaner d'un professionnel de la santé ou résulter d'un acte réservé aux professionnels de la santé. De plus, une donnée peut être relative à la santé même lorsqu'elle n'est pas traitée à des fins thérapeutiques. Par ailleurs, la seule information relative à un aspect physique ou psychique d'un individu ne constitue pas nécessairement en tant que telle une donnée relative à la santé. Pour obtenir cette dernière qualification, l'aspect physique ou psychique doit nous apprendre quelque chose à propos de la santé de la personne concernée. En ce sens, les données relatives à la santé devraient être définies comme visant toutes les informations relatives à la santé physique ou psychique, passée, présente ou future, d'une personne physique, vivante ou décédée.

77. Par ailleurs, la sous-traitance des données relatives aux patients est un phénomène incontestable qui prend de plus en plus d'ampleur. Elle présente souvent la difficulté d'être internationale sinon à tout le moins intra-européenne. Si le RGPD fournit un cadre juridique plus étoffé pour la réalisation des missions qui peuvent être confiées au sous-traitant, sous réserve néanmoins du fait que les États membres peuvent prendre des mesures au niveau national en ce qui concerne les données relatives à la santé, il n'en demeure pas moins que nous sommes en présence d'un tronc commun qui ne tient pas compte du contexte spécifique des soins de santé. À nos yeux, il manque des règles relatives aux qualifications professionnelles à remplir pour traiter des données relatives à la santé. Il est difficile, sinon périlleux, de vouloir répondre à cette question par les règles actuelles relatives à l'exercice des professions des soins de santé. Pour le dire autrement, celles-ci peuvent intervenir dans une certaine mesure pour les actes qui relèvent indubitablement de leur exercice, comme l'établissement d'un protocole en imagerie médicale. Mais, cela ne couvre absolument pas les nouveaux métiers qui sont apparus depuis plusieurs années dans le secteur de la santé et qui sont en lien avec les technologies de l'information et de la communication. Il existe bien de ci de là quelques formations éparses qui tentent de répondre à ce nouvel environnement mais il faut bien constater que le cadre législatif et réglementaire est très en retard, ce qui est de nature à retarder le développement de technologies utiles ce qui est préjudiciable tant pour les patients que pour l'économie de la santé. Il est donc grand temps que les pouvoirs publics se saisissent de la question du cadre juridique des nouveaux métiers de la santé qui doit venir compléter la protection des données du patient au-delà de la règlementation des infrastructures télématiques dans le domaine de la santé. Aussi, après avoir règlementé les traitements de données et les infrastructures télématiques, il est maintenant urgent de réglementer les nouveaux métiers et les nouvelles fonctions dans le domaine de la santé.

78. Contrairement à ce que semble défendre le Comité, il est, selon nous, toujours permis voire conseillé d'appuyer la licéité des traitements de données sur plusieurs bases de légitimation et il est particulièrement conseillé d'agir en ce sens en matière de traitements de données relatives à la santé (et de catégories particulières de données en général) à des fins scientifiques. Il faut toutefois éviter d'avoir une approche trop irréaliste de la notion de consentement. Ainsi, le consentement du participant au traitement de ses données dans le cadre d'un essai clinique de médicaments est tout à fait valide même si sa participation est conditionnée par la possibilité de traiter ses données. Par ailleurs, la multiplicité des bases de licéité dans ce domaine empêche aussi les

personnes indélicates de soumettre les responsables de traitement à des chantages éhontés.

79. Les responsables de traitement du secteur de la santé seront attentifs à leurs obligations répétées et parfois renforcées en termes de sécurité, de notification des failles de sécurité, de tenue d'un registre des activités de traitement et de désignation d'un délégué à la protection des données.

La mise en œuvre du RGPD leur impose des obligations renforcées de transparence et d'information. Le droit d'accès est maintenu et précisé en plusieurs aspects. Le droit à la portabilité des données est affirmé même s'il n'existe que dans la mesure où le traitement de données est fondé sur le consentement de la personne concernée ou s'il s'inscrit dans un cadre contractuel. Heureusement, le droit de la santé prévoit le plus souvent la transmission du dossier du patient entre les différents praticiens de la santé susceptibles d'intervenir dans sa prise en charge.

Ceci étant, le RGPD présente l'inconvénient d'alourdir encore plus le cadre juridique du secteur de la santé sans que les budgets requis ne soient nécessairement adoptés. Il n'y a, ceci étant, pas beaucoup de justification acceptable pour que les hôpitaux publics échappent aux amendes administratives.

Enfin, il va sans dire qu'il manque toujours une sensibilisation suffisante des acteurs de terrain et des formations appropriées pour garantir effectivement la protection des données sur le terrain, en ce compris dans le chef des patients.