Introduction à la protection des données du patient en milieu hospitalier

Introduction

Le droit de la protection des données vise à protéger les droits et libertés des individus face au développement des technologies de l'information et de la communication et, en particulier, à protéger leur droit au respect de la vie privée[1]. Le Règlement général sur la protection des données[2] (RGPD) participe à la protection des données en intervenant à trois niveaux :

1. la détermination (i) des conditions à respecter pour pouvoir traiter des données à caractère personnel ainsi que (ii) des obligations mises à charge des responsables du traitement de données et de leurs sous-traitants éventuels ;
2. la formalisation des droits de la personne à l'égard des données qui la concernent et qui font l'objet d'un traitement ;
3. la mise en place d'autorités de protection des données tant au niveau national qu'au niveau européen (le Comité européen de protection des données), de recours et de sanctions (notamment administratives) en vue de garantir la mise en œuvre effective de la protection des données.

Ce chapitre aborde plusieurs aspects clés liés à la mise en œuvre du RGPD en ce qui concerne les traitements des données du patient en milieu hospitalier.

I. L'articulation entre le RGPD et les règles relatives au secret professionnel

Un des problèmes ayant 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 »), était celui de savoir si les règles relatives à la protection des données modifiaient ou non les règles relatives au secret professionnel[3].

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) de l'obligation au secret auquel il était soumis en application de l'article 458 du Code pénal. En effet, dans une vision pénale classique, 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[4] qu'aux niveaux européen et international, et qui visait à lui donner plus de place dans la relation de soins de santé – ce qui pouvait aussi viser à lui donner plus de maîtrise sur le secret professionnel.

La réponse était pourtant évidente : la protection des données n'a jamais eu pour objectif de modifier les règles relatives au secret professionnel, que ce soit au niveau belge ou au niveau 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 et les traitements automatisés de données, ainsi que de leur conférer de nouveaux droits à leur égard, et non de s'immiscer dans la réglementation de l'exercice des professions des soins de santé ou 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 professionnel[5] 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[6] 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

1 Voy. not. J. Herveg, « La gestion des risques spécifiques aux traitements de données médicales en droit européen », *in* Chr. Herve, B.M. Knoppers, P.A. Molinari et M.-A. Grimaux (dir.), *Systèmes de santé et circulation de l'information. Encadrement éthique et juridique*, Paris, Dalloz, 2007, pp. 79-103 ; R. Gellert, *The Risk-Based Approach to Data Protection*, coll. Oxford Data Protection et Privacy Law, Oxford, Oxford University Press, 2020 ; O. Lynskey, *The Foundations of EU Data Protection Law*, coll. Oxford Studies in European Law, Oxford, Oxford University Press, 2015 ; M. von Grafenstein, « The Principle of Purpose Limitation in Data Protection Law. The Risk-Based Approach, Principles and Private Standards as Elements for Regulating Innovation », *Schriften zur rechtswissenschaftlichen Innovationsforschung*, 2018, p. 12.

2 Règlement (UE) n° 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, *J.O.U.E.*, L 119, 4 mai 2016, p. 1. Le droit à la protection des données s'enracine profondément dans l'article 8 de la Convention européenne des droits de l'homme et est consacré par l'article 8 de la Charte des droits fondamentaux de l'Union européenne (voy. aussi l'article 16 du TFUE et la Convention 108+).

3 Cette section reprend des extraits remaniés et mis à jour d'une publication antérieure : J. Herveg et J.-M. Van Gyseghem, « L'impact du Règlement général sur la protection des données dans le secteur de la santé », *in* K. Rosier et C. de Terwangne (coord.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, coll. du CRIDS, Bruxelles, Larcier, 2018, pp. 703-762. Sur le sujet, voy. aussi : C. Zorn-Macrez, *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, coll. « Santé, qualité de vie et handicap », Nancy, Presses universitaires de Nancy, 2010.

4 Voy. la loi du 22 août 2002 relative aux droits du patient.

5 Voy. le considérant n° 33 de la directive 95/46/CE ainsi que son article 8(3).

6 Voy. l'article 6(1) a) de la directive 95/46/CE.

respect des règles relatives au secret professionnel[7]. Toute la question est de savoir si cette interprétation demeurait valide avec l'entrée en vigueur du RGPD.

Il faut tout d'abord noter que le RGPD poursuit le même objectif que la directive 95/46/CE, mais sous une forme plus développée. De plus, tout comme la directive 95/46/CE, le RGPD se réfère aux règles relatives au secret professionnel sans donner une quelconque indication qu'il aurait vocation à les régir ou les modifier. 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 professionnel (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)[8].

Si ce premier 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[9], ce qui recouvre le maintien ou l'adoption de nouvelles règles en matière de secret professionnel.

En outre, 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 professionnel 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[10].

Il paraît donc évident que le RGPD n'a pas non plus pour objectif ni pour effet de modifier les règles relatives au secret professionnel, 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.

Il semble, dès lors, que la réponse à la question de l'articulation entre la protection des données et le secret professionnel 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[11], et ce, tant au niveau européen qu'au niveau national.

II. L'application du RGPD aux traitements des données du patient en milieu hospitalier

Le RGPD s'applique aux traitements[12] des données du patient en milieu hospitalier pour autant que ces traitements soient automatisés ou que les données du patient figurent ou soient appelées à figurer dans un fichier[13]. Ceci demande de s'attarder sur les notions de « données à caractère personnel » et de « données concernant la santé »[14].

A. La notion de données à caractère personnel

La notion de données à caractère personnel vise « toute information concernant une personne physique identifiée ou identifiable »[15]. C'est un concept large qui vise tout type d'informations dès lors que celles-ci peuvent être rattachées directement ou indirectement à un individu[16].

Sous la directive 95/16/CE, le Groupe de travail de l'article 29[17] avait mis en avant les trois éléments de cette définition[18] : la notion d'information, la relation entre l'information et une personne (physique)[19] et l'identification de cette dernière (la *personne concernée*).

La notion de *données à caractère personnel* vise toutes sortes d'informations et pas seulement celle qui révélerait 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,

7 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*, coll. Cahiers du CRID, Bruxelles, Academia-Bruylant, 2005, n° 26, p. 156.

8 Voy. l'article 9(3) du RGPD relatif au traitement portant sur des catégories particulières de données à caractère personnel.

9 Art. 9(4) RGPD.

10 Voy. l'article 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.

11 Ce qui signifie, notamment, que, dans la mesure prérappelée, on ne peut pas exciper des règles relatives au secret professionnel pour s'opposer au droit d'accès de la personne concernée tel qu'il est consacré en matière de protection des données.

12 La notion de « traitement » est définie à l'article 4.2° du RGPD.

13 En application de l'article 3(1) du RGPD. Pour la notion de « fichier », voy. sa définition à l'article 4.6° du RGPD. La notion de fichier présuppose un support non informatique, donc, le plus souvent, papier.

14 Cette section reprend des extraits remaniés et mis à jour d'une publication antérieure : J. Herveg et J.-M. Van Gyseghem, « L'impact du Règlement général sur la protection des données dans le secteur de la santé », *op. cit.*, pp. 703-762.

15 Voy. l'article 4.1° du RGPD et le considérant n° 26.

16 Voy. à ce sujet : K. Rosier et C. de Terwangne (coord.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 60 et s. ; Chr. Kuner, L.A. Bygrave et Chr. Docksey (éd.), *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2020, pp. 103 et s. (*cf.* aussi la mise à jour de mai 2021 pp. 22-27).

17 À la suite de l'adoption du RGPD, le Groupe de travail de l'article 29 a été remplacé par le Comité européen de protection des données (CEPD) (European Data Protection Board ou EDPB, en anglais).

18 Groupe de travail « Article 29 » sur la protection des données, avis n° 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007, WP 136.

19 Sur la question de la protection des données *post mortem*, voy. not. J. Herveg, « Une vie privée après la mort ? Le cas des données relatives au patient », *J. T.*, 2005, n° 6189, pp. 489-500.

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). Les données biométriques (comme les données ADN) peuvent remplir deux fonctions : soit contenir de l'information, soit servir d'identificateur. 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 doit être assimilée à une collecte (un traitement) de données à caractère personnel.

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 pour 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, de traiter d'une certaine manière ou d'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[20]. 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[21].

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 *identifiée* 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*. 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 croisement de critères significatifs, permettant 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 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[22]. 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) ;
- 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 (p. ex., violations du devoir de confidentialité) ;
- les défaillances techniques, etc.

Toutefois, le Groupe 29 considérait que l'appréciation du caractère raisonnable devait 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

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

21 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.

22 Considérant n° 26 de la directive 95/46/CE.

techniques et organisationnelles appropriées en temps utile. Cela ne signifie pas pour autant qu'il faille considérer que les données soient à caractère personnel dès le début.

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 plutôt en fonction de son usage.

Toute la question est aujourd'hui de savoir si, avec les techniques actuelles, on peut encore garantir l'impossibilité d'identifier, sans mettre en œuvre des moyens déraisonnables, un individu.

B. La notion de données concernant la santé

Les données à caractère personnel concernant la santé sont des catégories particulières de données à caractère personnel[23]. Ce sont les données « […] 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 »[24].

Les considérants du RGPD précisent que « [l]es 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 « [c]ela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique ; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques ; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic *in vitro* »[25].

Par ailleurs, il ressort des considérants relatifs au traitement des catégories particulières de données pour des motifs d'intérêt public que les données concernant 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[26].

À propos du droit d'accès, les considérants du RGPD précisent que les personnes concernées devraient 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 administré[27].

Autrement dit, dans le RGPD, la notion de données concernant 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 révèlent des informations sur l'état de santé de cette 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.

Cette définition est très large en ce que, à suivre les considérants du RGPD, la notion de données concernant la santé engloberait aussi des données qui, en tant que telles, ne sont pas relatives à la santé, mais dont on pourrait 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 permettraient de retrouver des informations relatives à la santé d'une personne (à l'instar d'un identifiant en matière de santé).

III. L'identification du responsable du traitement des données du patient en milieu hospitalier ainsi que des personnes placées sous son autorité et de ses sous-traitants

Une fois les traitements de données identifiés, il faut déterminer qui en est le responsable, les personnes placées sous l'autorité de ce dernier ainsi que les sous-traitants éventuels[28].

23 Les données génétiques sont définies à l'article 4.13° du RGDP (voy. le considérant n° 34).

24 Voy. l'article 4.15° du RGPD et le considérant n° 35.

25 Considérant n° 35 du RGPD.

26 Voy. le considérant n° 54 du RGPD qui renvoie à la notion de santé publique reprise dans le règlement (CE) n° 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.

27 Voy. le considérant n° 63 du RGPD.

28 Cette section reprend des extraits remaniés et mis à jour de deux publications antérieures : J. Herveg, *La protection des données du patient à l'hôpital*, Waterloo, Kluwer, 2009 ; J. Herveg et J.-M. Van Gyseghem, « Un nouveau métier de la santé : la sous-traitance des données du patient », *in Law, Norms and Freedoms in Cyberspace. Droit, normes et libertés dans le cybermonde. Liber amicorum Yves Poullet*, coll. du CRIDS, Bruxelles, Larcier, 2018, pp. 747-764.

A. Le responsable du traitement des données du patient en milieu hospitalier

Le responsable du traitement est un acteur clé dans la protection des données. C'est *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement*[29]. C'est la personne qui a la maîtrise sur les deux éléments de la définition : elle est la personne qui décide des finalités du traitement des données du patient (dossier informatisé du patient, facturation, recouvrement[30], etc.) et qui décide des moyens financiers, matériels et humains à mettre en œuvre pour atteindre ces finalités. Il faut insister sur le fait qu'il peut y avoir plusieurs responsables de traitement ; ce sont alors des responsables conjoints du traitement[31].

L'identification du responsable du traitement dépend d'une analyse au cas par cas. Toutefois, lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre[32].

À l'hôpital, le nom du responsable du traitement doit être repris dans le règlement de l'hôpital relatif à la protection de la vie privée (qui doit être remis à chaque patient)[33]. Cependant, son identification n'est pas toujours chose aisée[34]. Qui peut ou doit se voir reconnaître la qualité de responsable du traitement de données ? La personne morale qui exploite l'hôpital ? Le gestionnaire de l'hôpital ? Le directeur administratif ? Le directeur médical ? Le médecin-chef ? Le chef du département infirmier ? Chaque chef de service ou de département ? Chaque praticien professionnel en ce qui concerne ses activités ? Faut-il distinguer, en outre, selon le statut de salarié ou d'indépendant du personnel ?

La loi coordonnée sur les hôpitaux[35] ne contient toujours pas de disposition spécifique relative à la détermination du responsable du traitement de données. De manière générale, elle pose que *la responsabilité générale et finale pour l'activité hospitalière, sur le plan de l'organisation et du fonctionnement, ainsi que sur le plan financier, incombe au gestionnaire* de l'hôpital[36]. Ce dernier a aussi la charge de définir *la politique générale de l'hôpital* et de prendre *les décisions de gestion en respectant les dispositions et procédures spécifiques prévues au titre IV* de la loi[37].

La loi coordonnée sur les hôpitaux instaure aussi diverses responsabilités quant à l'organisation de l'activité médicale et infirmière à charge du médecin-chef et du chef du département infirmier, notamment en ce qui concerne l'ouverture et la conservation du dossier du patient[38].

Mais cela n'implique pas nécessairement que ces personnes soient celles qui, dans les faits, déterminent les finalités et les moyens du traitement de données. La notion de responsable est en effet ambiguë : elle désigne tant la personne qui, dans les faits, détermine les finalités et les moyens du traitement de données que la personne ou l'organe qui, selon ses compétences, aurait pu ou dû définir ces finalités et ces moyens[39].

Il semble qu'à ce jour, la meilleure réponse consiste toujours à partir du fait que le responsable du traitement de données devrait être la personne morale qui exploite l'hôpital, et que le gestionnaire assume la responsabilité générale et finale de cette exploitation. Il va de soi que la personne morale exercera ses droits et obligations au travers des différents organes par lesquels elle agit, conformément à la loi ou à ses statuts, sans préjudice des représentations conventionnelles ou ratifications éventuelles.

Mais il faut insister sur le fait que, si une personne détermine les finalités et les moyens d'un traitement de données à caractère personnel au sein de l'hôpital sans respecter les règles de répartition des fonctions et pouvoirs en la matière au sein de l'hôpital, elle aura la qualité de responsable du traitement pour les traitements qu'elle aura initiés.

B. Les personnes placées sous l'autorité du responsable du traitement des données du patient en milieu hospitalier

Le RGPD reprend la notion de personne « agissant sous l'autorité du responsable du traitement (ou du sous-traitant) »[40]. Cette notion d'autorité ne s'entend pas ici au sens classique du droit du travail. C'est un concept de droit européen qui doit recevoir une interprétation autonome.

Sur le sujet, voy. CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, v2.0, adoptées le 7 juillet 2021.

29 Art. 4.7° RGPD.

30 À ce sujet, voy. J. Herveg, « La mise à jour des adresses de patients dans le recouvrement des créances hospitalières », note sous J.P. Wavre (2e cant.), 31 mai 2011, *Revue du droit de la consommation*, 2011.

31 Art. 26 RGPD. Voy. à ce sujet : J.-M. Van Gyseghem, « Les modifications de la relation médecin-patient au contact de la télématique médicale : quelques réflexions à bâtons rompus », *Lex Electronica*, vol. 10, n° 3, 2006.

32 Art. 4.7° RGPD.

33 Arrêté royal du 23 octobre 1964 portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre (annexe, III, Normes d'organisation, 9°*quater*). Cet arrêté est toujours en vigueur.

34 Sur cette question, voy. 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 », *op. cit.*, pp. 56-84, spéc. n° 13.

35 Loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins.

36 Art. 16 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins.

37 *Ibid.*

38 Art. 18, 19, 20, 21, 23, 24, 25 et 26 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins. Voy. aussi les dispositions spécifiques relatives au dossier médical ou infirmier en fonction du service hospitalier considéré, contenues dans l'arrêté royal du 23 octobre 1964, ainsi que les arrêtés royaux du 15 décembre 1987 portant exécution des articles 13 à 17 de la loi relative aux hôpitaux, coordonnée le 7 août 1987, du 3 mai 1999 déterminant les conditions générales minimales auxquelles le dossier médical, visé à l'article 15 de la loi relative aux hôpitaux, coordonnée le 7 août 1987, doit répondre, et du 28 décembre 2006 déterminant les conditions générales minimales auxquelles le dossier infirmier, visé à l'article 17*quater* de la loi relative aux hôpitaux, coordonnée le 7 août 1987, doit répondre.

39 L'exposé des motifs de la loi du 8 décembre 1992 précisait à cet égard que « [l]'important est que le responsable du traitement soit la personne, l'instance administrative, la société, l'association, etc., qui dispose du pouvoir de décision sur le traitement effectué » (*Doc. parl.*, Ch. repr., 1998-1999, n° 49-1566/1, p. 15).

40 Voy. les articles 29 et 32(4) du RGPD.

Au sein de l'hôpital, cette notion vise l'ensemble des personnes dont les fonctions sont intégrées dans l'organisation de l'hôpital. L'hôpital est en effet une entité structurée par la loi et ses statuts et dont tous les travailleurs sont soumis à son autorité au sens du RGPD. Concrètement, il s'agit du personnel médical, salarié ou indépendant, du personnel infirmier, paramédical, administratif et technique (en ce compris le service informatique), etc. En revanche, la société extérieure en charge de la maintenance informatique n'est pas, en principe, sous l'autorité de l'hôpital ; elle n'est pas intégrée dans son organisation. Il faut alors vérifier si elle doit recevoir la qualité de « sous-traitant ».

C. Le sous-traitant du responsable du traitement des données du patient en milieu hospitalier

Le sous-traitant est un autre acteur important ; c'est celui qui offre l'expertise technique, les équipements et les ressources matérielles et personnelles que le responsable du traitement ne peut pas ou ne veut pas prendre en charge pour réaliser ses projets informatiques. La sous-traitance de données est un phénomène qui s'est fortement développé dans le domaine de la santé, et les hôpitaux n'y échappent pas[41].

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 étant de renforcer l'étanchéité du circuit des traitements de données (sa confidentialité) et, par-là, de garantir l'effectivité de la protection de la personne concernée[42].

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 »[43]. 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[44]. 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 du responsable du traitement (même s'il ne peut traiter les données que sur les instructions documentées[45] 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 faisant 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 de l'hôpital (au sens opérationnel et organisationnel). De même, le secrétariat de l'hôpital n'intervient pas en qualité de sous-traitant lors de la prise des rendez-vous dans l'agenda électronique ou lors de l'encodage des protocoles ou de la rédaction du courrier.

La qualification à donner à la société juridiquement distincte qui preste des services de traitements de données dans un contexte de mutualisation de services 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. Si la réponse est positive, nous serons en présence d'un sous-traitant. Sinon, il s'agira d'une personne agissant sous l'autorité du responsable du traitement.

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 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. En revanche, la société extérieure qui réalise une migration de données au sein de l'hôpital sans être sous l'autorité 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.

Le tout, bien sûr, est de ne pas autoriser les montages destinés à faire échapper l'un ou l'autre 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 du traitement de données au sein de ce groupe.

La distinction entre les sous-traitants de données et ceux qui agissent sous l'autorité 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 du responsable du traitement ? Autrement dit, quelle est la différence entre recevoir une instruction et être sous l'autorité du responsable du traitement ?

41 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 l'article 28(4) du RGPD pour la question du recrutement d'un ou plusieurs sous-traitants par le premier sous-traitant.

42 Voy. Groupe de l'article 29, avis n° 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », adopté le 16 février 2010, WP 169, p. 26.

43 Art. 4.8° RGPD.

44 Voy. Groupe de l'article 29, avis n° 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », adopté le 16 février 2010, WP 169, p. 26.

45 Conformément à l'article 28(3) du RGPD.

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*[46]. Cela étant, il ne faut pas perdre de vue qu'à partir du franchissement d'un certain seuil, le sous-traitant pourrait devenir un responsable du traitement conjoint en raison de sa participation aux choix des finalités et des moyens du traitement de données par l'hôpital[47].

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 courir le risque de devenir un responsable du 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 (ici, l'hôpital). Le tout revient maintenant à se demander s'il n'est pas artificiel de distinguer 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 »[48].

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*[49], réaliser des opérations ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés 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.

46 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, pp. 35-50. Voy. également Groupe de travail « Art. 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.

47 Voy. Groupe de travail « Art. 29 » sur la protection des données, avis n° 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », adopté le 16 février 2010, WP 169, p. 27.

48 Art. 28(3), *in fine*, RGPD.

49 Voy. l'article 4.2° du RGPD.

IV. Les conditions à respecter pour traiter des données en milieu hospitalier

Le RGPD impose de nombreuses règles à respecter afin de pouvoir traiter des données à caractère personnel. Ces règles s'appliquent aussi aux traitements des données du patient en milieu hospitalier. Il y a tout d'abord les principes qui régissent tous les traitements de données. Il faut ensuite déterminer la base juridique qui autorise le traitement des données du patient en milieu hospitalier, ce qui vise la question des finalités poursuivies par le traitement de ces données et pose aussi la question du consentement du patient au traitement de ses données dans l'hôpital, avant d'aborder les règles propres aux traitements des données concernant la santé du patient[50].

A. Les principes applicables aux traitements des données du patient

Le traitement des données du patient en milieu hospitalier doit obéir aux sept principes qui régissent tous les traitements de données :

1. les données doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (*ce sont les principes de licéité, de loyauté et de transparence*) ;
2. les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (*c'est le principe de la limitation des finalités*)[51] (le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas incompatible avec les finalités initiales pour autant qu'il soit soumis à des garanties appropriées pour les droits et libertés de la personne concernée. Ces garanties résulteront de la mise en place de mesures techniques et organisationnelles assurant notamment le respect du principe de la minimisation des données[52]. Dans la mesure du possible, le traitement ultérieur ne devrait pas ou plus permettre l'identification de la personne concernée) ;
3. les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (*c'est le principe de minimisation des données*) ;

50 Cette section reprend des extraits remaniés et mis à jour de trois publications antérieures : J. Herveg, *La protection des données du patient à l'hôpital*, *op. cit.* ; J. Herveg et J.-M. Van Gyseghem, « Un nouveau métier de la santé : la sous-traitance des données du patient », *op. cit.*, pp. 747-764 ; J. Herveg, « Réflexions autour de la protection des données et des vulnérabilités », *in* H. Jacquemin et M. Nihoul (coord.), *Vulnérabilités et droits dans l'environnement numérique*, coll. de la Faculté de droit de l'UNamur, Buxelles, Larcier, 2018, pp. 333-392.

51 À ce sujet, voy. not. Art. 29 Data Protection Working Party *Opinion 03/2013 on purpose limitation*, WP 203, 2 avril 2013.

52 Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière. La *pseudonymisation* est le traitement de données à caractère personnel réalisé de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable (art. 4.5° RGPD).

4. les données doivent être exactes et, si nécessaire, tenues à jour, et toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (*c'est le principe d'exactitude*) ;
5. les données ne peuvent être conservées sous une forme qui permette l'identification des personnes concernées pour une durée qui excéderait ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Les données peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, pour autant que leur traitement soit soumis à des garanties appropriées pour les droits et libertés de la personne concernée. Ces garanties résulteront de la mise en place de mesures techniques et organisationnelles assurant notamment le respect du principe de la minimisation des données[53]. Il faut recourir à des traitements ultérieurs qui ne permettent pas ou plus d'identifier les personnes concernées chaque fois que cela se révèle possible ;
6. les données doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (*c'est le principe d'intégrité et de confidentialité*) ;
7. le responsable du traitement est responsable du respect de ces principes. En outre, et c'est nouveau dans la forme, il doit être en mesure de démontrer que ces principes sont effectivement respectés (*c'est le principe de responsabilité*)[54].

B. La licéité des traitements de données du patient

Le RGPD énumère (de manière exhaustive) les catégories d'hypothèses dans lesquelles il est, *a priori*, licite (c'est-à-dire conforme à ce qu'autorise le droit) de traiter des données à caractère personnel. Il n'est donc permis de traiter des données à caractère personnel « ordinaires » que dans une des hypothèses suivantes à l'article 6(1) du RGPD[55] :

1. la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités *spécifiques* ;
2. le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
3. le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
4. le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
5. le traitement est 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 ;
6. le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel (notamment lorsque la personne concernée est un enfant). Cette hypothèse ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

Il est présumé pour chacune de ces catégories d'hypothèse de licéité qu'il est légitime, en général, de traiter des données. Pour le dire autrement, chacune de ces catégories est censée représenter une situation dans laquelle les intérêts en présence sont dans un équilibre acceptable. Il faut, bien entendu, vérifier, dans chaque cas d'espèce pour chaque traitement pris et considéré séparément et individuellement, si cet équilibre est bien respecté *in concreto*, et non seulement *a priori* et *in abstracto*. À cet égard, la modification dans le temps de l'équilibre des intérêts en présence aura pour effet d'ôter la légitimité du traitement de données pour le futur ; il faudra donc y mettre fin, sauf à trouver une solution pour rééquilibrer de manière satisfaisante les intérêts en présence. Il faut répéter que l'appréciation de la légitimité d'un traitement de données est sensible aux autres aspects de la mise en œuvre de la protection des données, comme le niveau de confidentialité et de sécurité du traitement de données, le niveau de mise en œuvre des droits de la personne concernée, le niveau de contrôle assuré par l'Autorité nationale de contrôle, le degré de nécessité de la finalité poursuivie, la manière d'assurer les droits de la personne concernée, etc.

C. Le consentement du patient au traitement de données qui le concernent

Le consentement du patient au traitement des données qui le concernent induit donc une présomption de licéité du traitement de données qui le concernent – une présomption d'équilibre entre les intérêts en présence[56]. L'hôpital doit être en mesure de prouver que la personne a bien donné son consentement[57] ; il ne peut pas imposer à la personne concernée de prouver qu'elle n'aurait pas consenti au traitement de données.

La demande de consentement doit être présentée sous une forme qui la distingue clairement d'autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. La partie de cette déclaration qui méconnaîtrait ces règles n'est pas contraignante[58], ce qui signifie, aussi, que le patient pourrait renoncer à s'en plaindre et ratifier l'illégalité en cause.

53 Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière.

54 À ce sujet, voy. not. Art. 29 Data Protection Working Party *Opinion 3/2010 on the principle of accountability*, WP 173, 13 juillet 2010.

55 L'article 6(2) du RGPD prévoit la possibilité de régimes particuliers pour les traitements imposés par la loi ou réalisés dans l'intérêt public ou dans l'exercice de l'autorité publique dans le chef du responsable du traitement. Voy. l'article 6(4) à propos des traitements ultérieurs.

56 Au sujet du consentement, voy. CEPD, Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) n° 2016/679, v1.1, adoptées le 4 mai 2020.

57 Art. 7(1) RGPD.

58 Art. 7(2) RGPD.

La personne concernée (ici, le patient) peut toujours retirer son consentement à tout moment et sans avoir à se justifier. Le retrait du consentement n'invalide pas les opérations antérieures. En revanche, il s'oppose à la poursuite du traitement de données. Le patient doit avoir été informé du droit de retirer son consentement avant de le donner. Comme l'énonce le RGPD, il doit être aussi simple de retirer que de donner son consentement[59].

Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat[60].

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 européen de la protection des données a maintenu l'affirmation selon laquelle un responsable du 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[61].

Cette affirmation est inexacte et *explicitement* contredite par le RGPD lui-même. En effet, l'article 6(1) du RGPD énonce déjà que « [l]e traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie […] », ce qui prouve déjà à suffisance que plusieurs bases de licéité peuvent fonder un traitement de données. De plus, 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.

Autrement dit, contrairement à l'opinion du Comité européen de protection des données, l'hôpital peut et, dans certains cas, devrait renforcer la licéité de son traitement de données en ajoutant le consentement de la personne concernée (comme en matière de santé ou de recherche scientifique)[62].

La question du sort à donner au consentement obtenu sous l'empire de la directive 95/46/CE est incertaine. Le considérant n° 171 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 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 européen de la protection des données 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. En revanche, l'adoption d'une nouvelle réglementation peut modifier les effets juridiques à produire par cet acte à partir de l'entrée en vigueur de celle-ci.

Le RGPD ne règle pas 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.

D. Les règles propres aux traitements des données concernant la santé du patient

La règle est bien connue et n'a pas changé : le traitement portant sur des catégories particulières de données à caractère personnel (antérieurement appelées *données sensibles*), en ce compris les données concernant la santé, est interdit[63]. Cette interdiction ne s'applique pas dans les hypothèses suivantes[64], sans préjudice de la nécessité de vérifier *in concreto*

59 Art. 7(3) RGPD.

60 Art. 7(4) RGPD.

61 Groupe de travail « Art. 29 » sur la protection des données, « Lignes directrices sur le consentement sous le Règlement 2016/679 », adoptées le 28 novembre 2017, et revues et adoptées en dernier le 10 avril 2018, WP 259 rev.01, p. 23, point 6.

62 À ce sujet, voy. J. Herveg et J.-M. Van Gyseghem, « L'impact du Règlement général sur la protection des données dans le secteur de la santé », *in Le Règlement général sur la protection des données*, Bruxelles, Larcier, 2018, p. 730, n° 39.

63 Art. 9(1) RGPD.

64 Art. 9(2) RGPD. Toutefois, les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé (art. 9(4) RGPD).

l'existence d'un juste équilibre entre les intérêts en présence pour chaque traitement :

1. la personne concernée a donné son consentement *explicite* au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction ne peut pas être levée par la personne concernée ;
2. le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée ;
3. le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
4. le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées ;
5. le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;
6. le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;
7. le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ;
8. le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées à l'article 9.3 du Règlement ;
9. le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ;
10. le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89.1 du Règlement, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

Les données concernant la santé ne peuvent toutefois faire l'objet d'un traitement à des fins thérapeutiques[65] que si elles sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel 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 ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents[66].

Les États membres peuvent adopter des règles matérielles particulières en matière de traitements de données génétiques, de données biométriques ou de données relatives à la santé, dans la limite de ce que permet la jurisprudence de la Cour européenne des droits de l'homme en matière de protection des données et la Convention 108 et, dans le futur, 108 +, ce qui renvoie, notamment, aux règles relatives au secret professionnel, à la loi relative aux droits du patient, aux règles relatives aux dossiers médicaux et infirmiers et aux dossiers tenus par les pharmaciens et à la loi relative à la qualité des soins de santé.

L'article 33 de la loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé précise le contenu minimal du dossier du patient. L'article 35 de cette loi précise que le professionnel des soins de santé conserve le dossier du patient pendant minimum trente ans et maximum cinquante ans à compter du dernier contact avec le patient.

E. Les traitements de données qui ne nécessitent pas l'identification de la personne concernée

Si les finalités pour lesquelles les données du patient sont traitées n'imposent pas ou n'imposent plus au responsable du traitement d'identifier une personne concernée, celui-ci n'est pas tenu de conserver, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter le RGPD[67]. Le RGPD prévoit que, lorsque le responsable du traitement est à même de démontrer qu'il n'est pas en mesure d'identifier la personne concernée, il en informe la personne concernée, si possible. En pareil cas, la personne concernée doit fournir des infor-

65 Cela vise la finalité reprise à l'article 9(2), h), du RGPD.

66 Art. 9(3) RGPD.

67 Art. 11(1) RGPD.

mations complémentaires qui permettent de l'identifier aux fins d'exercer son droit d'accès, son droit de rectification, son droit à l'effacement, son droit à la limitation du traitement, son droit à la notification de la rectification ou de l'effacement de données ou de la limitation du traitement, ou encore son droit à la portabilité des données[68]. Tout ceci n'empêche pas que le responsable du traitement soit, pour le surplus, soumis à l'ensemble des obligations qui découlent du RGPD et qui s'imposent à lui.

V. Les obligations à charge de l'hôpital et de ses sous-traitants éventuels

A. Les obligations générales à charge de l'hôpital et de son sous-traitant éventuel

Outre le respect des principes applicables au traitement de données et à la licéité de ces derniers, l'hôpital et son sous-traitant éventuel doivent se soumettre à toute une série d'obligations générales qui représentent autant de nouvelles règles matérielles uniformes à respecter[69].

1. Le principe de la responsabilité du responsable du traitement

La *première obligation générale* de l'hôpital est de s'assurer que les traitements de données sont effectués conformément aux règles fixées par le RGPD et il doit être en mesure de le démontrer. À cet effet, il doit mettre en œuvre des mesures techniques et organisationnelles appropriées, en tenant compte 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 peut varier, pour les droits et libertés des personnes physiques. Le responsable du traitement doit aussi mettre en œuvre des politiques appropriées en matière de protection des données qui sont proportionnées au regard des activités de traitement. Il doit réexaminer toutes ces mesures et les actualiser si nécessaire[70], le tout sur une base régulière.

2. La protection des données dès la conception

La *seconde obligation générale* de l'hôpital est de mettre en œuvre, *tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même*, des mesures techniques et organisationnelles appropriées[71] destinées à mettre en œuvre les principes relatifs à la protection des données[72] de façon effective, et qui sont destinées à assortir le traitement des garanties nécessaires pour répondre aux exigences fixées par le RGPD et protéger les droits de la personne concernée (ici, le patient)[73].

Ces mesures doivent tenir compte 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 peut varier) que le traitement présente pour les droits et libertés des personnes physiques. Ces mesures sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple, la minimisation des données, de façon effective, et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du RGPD et de protéger les droits de la personne concernée[74].

3. La protection des données par défaut

La *troisième obligation générale* de l'hôpital est de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, *par défaut*, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement soient traitées. Cela s'applique tant à la quantité de données à caractère personnel collectées qu'à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures doivent garantir que, *par défaut*, les données à caractère personnel ne soient pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée[75].

4. Les responsables conjoints du traitement de données

La possibilité d'avoir des responsables conjoints du traitement[76] n'est pas neuve, mais le RGPD précise qu'ils doivent définir de manière transparente leurs obligations respectives pour garantir le respect des règles en matière de protection des données, notamment en ce qui concerne l'exercice des droits de la personne concernée, ainsi que leurs obligations respectives quant à la communication des informations à fournir à la personne concernée. Ils peuvent notamment désigner un point de contact pour les personnes concernées.

Cette répartition des obligations doit se faire par la voie d'un 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[77]. Cet accord doit refléter fidèlement les rôles respectifs des responsables conjoints du traitement ainsi que leurs relations vis-à-vis des personnes concernées. Les

68 Voy. l'article 11(2) du RGPD.

69 Cette section reprend des extraits remaniés et mis à jour de trois publications antérieures : J. Herveg, *La protection des données du patient à l'hôpital*, *op. cit.* ; J. Herveg et J.-M. Van Gyseghem, « Un nouveau métier de la santé : la sous-traitance des données du patient », *op. cit.*, pp. 747-764 ; J. Herveg, « Réflexions autour de la protection des données et des vulnérabilités », *op. cit.*, pp. 333-392.

70 Voy. l'article 24 du RGPD. L'application d'un code de conduite approuvé ou de mécanismes de certification approuvés peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement.

71 Comme la pseudonymisation.

72 Comme la minimisation des données.

73 À ce sujet, voy. CEPD, Lignes directrices 4/2019 relatives à l'article 25, Protection des données dès la conception et protection des données par défaut, v2.0, adoptées le 20 octobre 2020.

74 Sur tout ceci, voy. l'article 25(1) du RGPD. Un mécanisme de certification approuvé peut servir d'élément pour démontrer le respect de ces exigences.

75 Voy. l'article 25(2) du RGPD. De nouveau, un mécanisme de certification approuvé peut servir d'élément pour démontrer le respect de ces exigences. Sur la protection par défaut, voy. CEPD, Lignes directrices 4/2019 relatives à l'article 25, Protection des données dès la conception et protection des données par défaut, v2.0, adoptées le 20 octobre 2020.

76 Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont responsables conjoints du traitement.

77 Voy. l'article 26(1) du RGPD.

grandes lignes de l'accord doivent être mises à la disposition de la personne concernée[78].

En tout état de cause, la personne concernée (ici, le patient) peut exercer les droits qui lui sont reconnus en matière de protection des données à l'égard de et contre chacun des responsables du traitement[79].

5. Le sous-traitant

L'hôpital ne peut choisir qu'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 soit conforme aux règles fixées par le RGPD et que la protection des droits des patients (en leur qualité de personne concernée) soit garantie[80].

Il est maintenant précisé que le sous-traitant ne peut pas faire appel à un autre sous-traitant sans l'autorisation écrite, préalable, spécifique ou générale, du responsable du traitement[81].

Le traitement de données en sous-traitance doit être régi par un contrat ou tout autre acte juridique au titre du droit de l'Union ou d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement. Ce contrat doit définir l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données et les catégories de personnes concernées, ainsi que les obligations et les droits du responsable du traitement[82].

Lorsqu'un sous-traitant recrute *un autre* sous-traitant (un sous-traitant en seconde ligne) pour mener des activités de traitement spécifiques, les mêmes obligations en matière de protection de données que celles imposées au premier sous-traitant doivent être imposées à cet autre sous-traitant[83]. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial *demeure pleinement responsable* devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations[84]. Si, en violation du RGPD, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce traitement[85], avec toutes les conséquences qui s'y attachent en termes de responsabilité et de sanction et sans préjudice du droit de la personne concernée de le poursuivre en réparation de son préjudice.

6. Le principe du traitement sous l'autorité du responsable du traitement ou du sous-traitant

En règle, le sous-traitant et toute personne qui agit sous l'autorité du responsable du traitement ou du sous-traitant et qui a accès à des données, ne peuvent traiter ces données que sur instruction du responsable du traitement, à moins d'y être obligés par le droit de l'Union ou le droit d'un État membre[86].

7. Le registre des activités de traitement

Comme tout responsable du traitement, l'hôpital doit tenir un registre des activités de traitement[87], ce qui participe à la démonstration de la conformité des traitements de données aux règles du RGPD et renvoie au principe de la « responsabilité » du responsable du traitement. Ce registre doit être tenu à jour.

L'obligation de tenir un registre ne s'applique pas lorsque les conditions cumulatives suivantes sont réunies[88] :

- l'entreprise ou l'organisation compte moins de deux cent cinquante travailleurs ;
- le traitement de données est occasionnel ;
- le traitement de données n'est pas susceptible de présenter des risques pour les droits et les libertés des personnes concernées ;
- le traitement de données ne porte pas sur des catégories particulières de données, comme les données concernant la santé ou les données génétiques.

Aucun hôpital ne peut donc raisonnablement se prévaloir de cette exception.

Dans les mêmes conditions, chaque sous-traitant et, le cas échéant, le représentant du sous-traitant doivent aussi tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte de l'hôpital[89].

Le patient ne peut pas exiger d'accéder à ce registre qui ne remplace pas l'information qui lui est due par ailleurs.

8. La coopération avec l'autorité de contrôle

L'hôpital et son sous-traitant ainsi que, le cas échéant, son représentant doivent coopérer avec l'autorité de contrôle, à la demande de celle-ci, dans l'exécution de ses missions[90].

B. La sécurité des données

1. Les mesures techniques et organisationnelles

Au titre de la sécurité des données[91], l'hôpital et son sous-traitant éventuel doivent mettre en œuvre les mesures tech-

78 La loyauté impose, en réalité, que cette information soit communiquée volontairement par les responsables du traitement lors de l'information due aux personnes concernées.

79 Voy. l'article 26(3) du RGPD.

80 Voy. l'article 28(1) du RGPD. Le respect, par le sous-traitant, d'un code de conduite approuvé ou le recours à un mécanisme de certification approuvé peut servir d'élément pour démontrer l'existence de garanties suffisantes (art. 28(5) RGPD).

81 Art. 28(2) RGPD. Dans le cas d'une autorisation écrite générale, le sous-traitant doit informer le responsable du traitement de tout changement concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

82 Sans préjudice du recours à des clauses contractuelles types, l'article 28(3) du RGPD détaille ce que ce contrat (sous forme écrite ou électronique) ou cet acte juridique doit contenir.

83 Ce qui doit se faire par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, en particulier pour ce qui est de présenter 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 présent règlement.

84 Art. 28(4) RGPD.

85 Voy. l'article 28(10) du RGPD.

86 Art. 29 RGPD.

87 Voy. l'article 30(1) du RGPD qui détaille son contenu. Ce registre peut être sous forme écrite ou électronique. Il doit être mis à la disposition de l'autorité de contrôle sur demande.

88 Voy. l'article 30(5) du RGPD.

89 Son contenu est détaillé à l'article 30(2) du RGPD.

90 Art. 31 RGPD. L'application d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir d'élément pour démontrer le respect des exigences en matière de sécurité du traitement.

91 À ce sujet, voy. not. Fr. Dumortier et V. Vander Geeten (coord.), *Les obligations légales de cybersécurité et de notifications d'incidents*, Bruxelles, Politeia, 2019.

niques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque lié à leur traitement. Ils doivent tenir compte à cet égard 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 de données ainsi que des risques (dont le degré de probabilité et de gravité varie) pour les droits et libertés des personnes physiques.

Lors de l'évaluation du niveau de sécurité du traitement, il faut tenir compte, en particulier, des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite[92].

Les mesures qui permettent d'assurer le niveau de sécurité approprié peuvent consister, entre autres, en :

1. une pseudonymisation et un chiffrement des données ;
2. des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
3. des moyens permettant de rétablir la disponibilité des données et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
4. une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement de données.

En tout cas, l'hôpital et son sous-traitant éventuel doivent prendre 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, ne les traite pas, excepté sur instruction de l'hôpital et de son sous-traitant éventuel ou à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

La loi du 22 août 2002 précise que le patient a droit, de la part de son praticien professionnel, à un dossier de patient soigneusement tenu à jour et conservé en lieu sûr[93].

2. La notification à l'autorité de contrôle des violations de données

Lorsqu'une violation de la sécurité entraîne, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données[94], l'hôpital doit notifier cet incident (appelé *violation de données*)[95] à l'autorité de contrôle[96], dans les meilleurs délais et, si possible, trois jours au plus tard après en avoir pris connaissance[97].

Il est libéré de cette obligation de notifier l'incident si la violation de données n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Mais, dans tous les cas, l'hôpital et son sous-traitant éventuel doivent documenter toute violation de données, en indiquant les faits concernant la violation des données, ses effets et les mesures prises pour y remédier. Cette documentation doit permettre à l'autorité de contrôle de vérifier le respect des obligations qui s'imposent en cas de violation de données.

De la même façon, le sous-traitant doit notifier à l'hôpital toute violation de la sécurité dans les meilleurs délais après en avoir pris connaissance. Il faut présumer qu'il est aussi tenu de documenter toute violation de données, même si cela n'est pas expressément prévu.

3. La communication à la personne concernée d'une violation de données

De manière asymétrique par rapport à l'obligation de notification à l'autorité de contrôle, l'hôpital ne doit communiquer la violation de données aux patients concernés que dans l'hypothèse où elle est susceptible d'engendrer un risque *élevé* pour leurs droits et libertés.

Cette communication doit alors intervenir dans les meilleurs délais. Elle doit décrire en des termes simples et clairs la nature de la violation des données intervenue, contenir le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues, une description des conséquences probables de la violation de données, une description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données, en ce compris, le cas échéant, les mesures pour en atténuer les conséquences négatives éventuelles.

Toutefois, même en cas de risque élevé pour les droits et libertés, cette communication n'est pas obligatoire lorsque :

1. l'hôpital a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et que ces mesures ont été appliquées aux données affectées par la violation, en particulier les mesures qui rendent les données incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;
2. l'hôpital a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser ;
3. elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

---

92 Voy. l'article 32 du RGPD.

93 Art. 9, § 1er, de la loi du 22 août 2022 relative aux droits du patient.

94 Voy. l'article 4.12° du RGPD.

95 À ce sujet, voy. EDPB, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, adoptées le 14 décembre 2021, v2.

96 La notification doit, à tout le moins :

1. décrire la nature de la violation de données, en ce compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données concernés ;
2. communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
3. décrire les conséquences probables de la violation de données ;
4. décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données, en ce compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

97 Au-delà de ce délai, la notification doit être accompagnée des motifs du retard dans l'accomplissement de cette obligation. Si, et dans la mesure où il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

Si l'hôpital n'a pas déjà communiqué la violation de données aux patients concernés, l'autorité de contrôle peut, après avoir examiné si cette violation de données est susceptible d'engendrer un risque élevé, exiger de l'hôpital qu'il procède à cette communication ou décider que l'hôpital se trouve dans une des hypothèses où il en est exempté[98].

C. L'analyse de l'impact des opérations de traitement envisagées sur la protection des données

1. Les hypothèses dans lesquelles une analyse d'impact doit être réalisée

Le responsable du traitement doit effectuer une analyse de l'impact des opérations de traitement envisagées sur la protection des données lorsque le type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques[99]. L'analyse d'impact est, en tout cas, obligatoire dans les hypothèses suivantes :

1. l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, fondée sur un traitement automatisé, en ce compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
2. le traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions ;
3. la surveillance systématique à grande échelle d'une zone accessible au public.

Les hôpitaux ne peuvent donc que difficilement échapper à l'obligation de réaliser une analyse d'impact.

L'analyse de l'impact des opérations de traitement envisagées doit contenir les éléments suivants au minimum :

1. une description systématique des opérations de traitement envisagées et des finalités du traitement, en ce compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
2. une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
3. une évaluation des risques pour les droits et libertés des personnes concernées ;
4. les mesures envisagées pour faire face aux risques, en ce compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Quand le traitement est nécessaire à l'exécution d'une obligation légale à laquelle le responsable du traitement est soumis ou lorsqu'il est 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, qu'il a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis et que ce droit réglemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, aucune autre analyse d'impact n'est requise à moins que les États membres estiment qu'il soit nécessaire d'effectuer une telle analyse avant les activités de traitement.

Si nécessaire, le responsable du traitement doit procéder à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

2. La consultation préalable et obligatoire de l'autorité de contrôle

Avant de mettre en œuvre le traitement, le responsable du traitement est obligé de consulter l'autorité de contrôle lorsque l'analyse d'impact indique que le traitement pourrait présenter un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer ce risque[100].

98 Art. 34 RGPD.

99 Voy. l'article 35 du RGPD. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires. Le responsable du traitement doit demander conseil au délégué à la protection des données quand il effectue une telle analyse d'impact relative à la protection des données (dans la mesure où un tel délégué a été désigné – ce qui laisse ouverte la question de l'obligation de le faire lorsque le responsable du traitement n'avait pas d'obligation (formelle ou dans le cadre des mesures techniques et organisationnelles) d'en désigner un, mais qu'il l'a quand même fait). L'autorité de contrôle doit établir et publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise. L'autorité de contrôle communique ces listes au *Comité européen de la protection des données*. L'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au *Comité européen de la protection des données*. Avant d'adopter ces deux sortes de listes, l'autorité de contrôle compétente doit appliquer le mécanisme de contrôle de la cohérence lorsque ces listes comprennent des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union. Le respect de codes de conduite approuvés doit être pris en compte lors de l'évaluation de l'impact des opérations de traitement, en particulier aux fins d'une analyse d'impact relative à la protection des données. Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement. Sur le sujet, voy. D. Wright et P. De Hert (éd.), *Privacy Impact Assessment*, coll. Law, Governance and Technology, Dordrecht, Springer, 2012, p. 6, ainsi que CEPD, Recommandation 01/2019 sur le projet de liste établi par le Contrôleur européen de la protection des données concernant les opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise (art. 39, § 4, du règlement (UE) n° 2018/1725), adoptée le 10 juillet 2019.

100 Le responsable du traitement doit communiquer à l'autorité de contrôle les éléments suivants :

1. le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises ;
2. les finalités et les moyens du traitement envisagé ;

L'autorité de contrôle notifie un avis écrit au responsable du traitement lorsqu'elle considère que le traitement est de nature à constituer une violation du RGPD, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque. L'autorité peut aussi user de ses autres pouvoirs comme mener une enquête ou imposer des mesures correctrices notamment[101].

Ce délai peut être prolongé de six semaines, en fonction de la complexité du traitement envisagé. L'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant, de la prolongation du délai ainsi que des motifs du retard, dans un délai d'un mois à compter de la réception de la demande de consultation. Ces délais peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations qu'elle a demandées pour les besoins de la consultation[102].

D. Le délégué à la protection des données

1. L'obligation de désigner un délégué à la protection des données

L'obligation de désigner un délégué à la protection des données est une des mesures qui ont particulièrement retenu l'attention. Au-delà de l'hypothèse où cette désignation est requise au titre des mesures organisationnelles destinées à garantir la sécurité et la confidentialité des traitements de données, le responsable du traitement et le sous-traitant sont, en tout état de cause, obligés de désigner un délégué à la protection des données[103] dans trois hypothèses[104] :

1. 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 ;
2. 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 ;
3. les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données et de données à caractère personnel relatives à des condamnations pénales et à des infractions.

Les hôpitaux doivent par conséquent désigner un délégué à la protection des données.

2. La fonction du délégué à la protection des données

La fonction du délégué à la protection des données obéit à des règles destinées à lui permettre d'exercer pleinement et effectivement sa mission :

1. la participation au processus décisionnel et opérationnel : le délégué à la protection des données doit être associé tant par le responsable du traitement que par le sous-traitant, et d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel ;
2. la mise à disposition des ressources nécessaires : le responsable du traitement et le sous-traitant doivent aider le délégué à la protection des données à exercer ses missions en lui fournissant les ressources nécessaires pour exercer à cet effet, ainsi que l'accès aux données et aux opérations de traitement, et en lui permettant d'entretenir ses connaissances spécialisées ;
3. l'indépendance et la protection de la fonction : le responsable du traitement et le sous-traitant doivent veiller à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice des missions. Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant ;
4. l'absence de filtrage par rapport aux personnes concernées : les personnes concernées peuvent prendre directement contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données et à l'exercice de leurs droits ;
5. la confidentialité de la fonction : le délégué à la protection des données est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres ;
6. la protection contre le caractère non exclusif de la fonction : le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement

3. les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées ;
4. le cas échéant, les coordonnées du délégué à la protection des données ;
5. l'analyse d'impact relative à la protection des données ; et
6. toute autre information que l'autorité de contrôle pourrait demander.

101 Voy. l'article 58 du RGPD.

102 Art. 36 RGPD. Les États membres sont obligés de consulter l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. De plus, le droit des États membres peut exiger que les responsables du traitement soient obligés de consulter l'autorité de contrôle et d'obtenir son autorisation préalable en ce qui concerne le traitement effectué par un responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci, en ce compris le traitement dans le cadre de la protection sociale et de la santé publique.

103 Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions qui lui incombent. Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service. Le responsable du traitement ou le sous-traitant publie les coordonnées du délégué à la protection des données et les communique à l'autorité de contrôle.

104 Voy. l'article 37 du RGPD. Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'il soit facilement joignable à partir de chaque lieu d'établissement. Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille. Lorsqu'il n'y est pas formellement contraint, le responsable du traitement ou le sous-traitant ou les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peut désigner ou, si le droit de l'Union ou le droit d'un État membre l'exige, est tenu de désigner un délégué à la protection des données. Le délégué à la protection des données peut agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.

ou le sous-traitant veille à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts[105].

3. Les missions du délégué à la protection des données

Les missions qui incombent au délégué à la protection des données sont au moins les suivantes[106] :

1. informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données ;
2. contrôler le respect des règles applicables en matière de protection des données, que ce soient les règles issues du Règlement, d'autres dispositions du droit de l'Union ou du droit des États membres, ainsi que les règles internes du responsable du traitement ou du sous-traitant, en matière de protection des données, en ce compris la question de la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;
3. dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci ;
4. coopérer avec l'autorité de contrôle ;
5. faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, en ce compris à propos de sa consultation préalable, et mener des consultations, le cas échéant, sur tout autre sujet.

Le délégué à la protection des données doit tenir compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

VI. Les droits du patient à l'égard de ses données à caractère personnel en milieu hospitalier

Il faut tout d'abord rappeler que la Charte des droits fondamentaux de l'Union européenne consacre le droit des citoyens européens à la protection des données qui les concernent[107] et qu'il ne serait pas audacieux de soutenir que la protection des données constitue de toute façon une obligation positive qui pèse sur les États cocontractants de la Convention européenne des droits de l'homme au titre de son article 8 qui protège le droit au respect de la vie privée et familiale, le domicile et la correspondance des individus[108]. Le RGPD reconnaît, quant à lui, huit droits à la personne concernée[109] :

1. le droit à la transparence et à l'information ;
2. le droit d'accès ;
3. le droit à la rectification ;
4. le droit à l'effacement ;
5. le droit à la limitation du traitement ;
6. le droit à la portabilité des données ;
7. le droit de s'opposer au traitement de données ;
8. le droit de ne pas être soumis à des décisions individuelles automatisées.

Le patient est en droit de revendiquer et d'exercer ces droits lors des traitements de données qui le concernent en milieu hospitalier[110].

A. Le droit à la transparence et à l'information

1. Le droit à la transparence

La transparence est un principe de base de la protection des données. Sans transparence, 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[111] et qui concernent tout autant les hôpitaux en leur qualité de responsables du traitement des données de leurs patients.

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 quand 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).

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*

105 Voy. l'article 38 du RGPD.

106 Voy. l'article 39 du RGPD.

107 Voy. l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Sur la Charte, voy. not. A. Biad et V. Parisot (dir.), *La Charte des droits fondamentaux de l'Union européenne. Bilan d'application*, coll. « Droit et Justice », Limal, Anthemis, 2018, p. 117 ; N. Cariat, *La Charte des droits fondamentaux et l'équilibre constitutionnel entre l'Union européenne et les États membres*, coll. du Centre des droits de l'homme de l'Université catholique de Louvain, Bruxelles, Bruylant, 2016, p. 14 ; F. Picod et S. Van Drooghenbroeck (dir.), *Charte des droits fondamentaux de l'Union européenne. Commentaire article par article*, coll. Droit de l'Union européenne, Bruxelles, Bruylant, 2018.

108 Voy. G. Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, coll. Law, Governance and Technology, Dordrecht, Springer, 2014, p. 16.

109 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 Règlement. 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.

110 Cette section reprend des extraits remaniés et mis à jour de deux publications antérieures : J. Herveg et J.-M. Van Gyseghem, « Un nouveau métier de la santé : la sous-traitance des données du patient », *op. cit.*, pp. 747-764 ; J. Herveg, « Réflexions autour de la protection des données et des vulnérabilités », *op. cit.*, pp. 333-392.

111 Voy. l'article 12 du RGPD.

s'il démontre qu'il n'est pas en mesure d'identifier la personne concernée qui s'est adressée à lui[112].

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[113].

Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes[114].

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 de 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. En revanche, 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[115].

2. Le droit à l'information

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[116].

B. Le droit d'accès

1. Le droit d'accès reconnu par le RGPD au profit du patient

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[117] et pour obtenir l'accès aux données qui la 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[118].

Il demeure à s'entendre sur ce que signifie *accéder aux données* ainsi que sur la *manière d'exercer cet accès*. Visiblement, il ne s'agit pas seulement du pouvoir d'en demander copie[119]. Par ailleurs, 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[120]. Le RGPD précise que le droit d'obtenir une copie des données ne doit pas porter atteinte aux droits et libertés d'autrui[121].

2. Le droit d'accès du patient à son dossier de patient

Le droit d'accès du patient à son dossier de patient est modalisé par la loi du 22 août 2022 relative aux droits du patient. Cette loi prévoit que le patient a le droit de *consulter* le dossier qui le concerne et il doit être donné suite à sa demande dans les meilleurs délais et au plus tard dans les quinze jours de sa demande. Cette loi restreint toutefois le droit d'accès en ce qu'elle énonce que les annotations personnelles d'un praticien professionnel et les données concernant des tiers n'entrent pas dans le cadre de ce droit de consultation[122]. Cette restriction peut se fonder tant sur l'article 9(4) du

112 La disposition veut sans doute dire qu'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 connaît nécessairement son identité.

113 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. l'article 12(6) du RGPD).

114 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.

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

116 Art. 12(7) RGPD. En vertu de l'article 12(8) du RGPD, 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.

117 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 est demandée par la personne concernée.

118 Sur l'accès du patient à son dossier informatisé, voy. not. J. Herveg, « L'accès du patient aux "logfiles" de son dossier informatisé », *Revue du droit de la consommation*, 2010, vol. 90, pp. 34-55 ; J. Herveg, « Patients'right of access to their electronic health record log files in European Law », Coimbra, Lex Medicinae, *Revista Portuguesa de Direito da Saude*, vol. 14, 2011. Voy. également : EDPB, Guidelines 01/2022 on data subject rights – Right of access, v1.0, adoptees le 18 janvier 2022.

119 En effet, l'article 15(4) du RGPD énonce que « [l]e droit d'obtenir une copie visé au paragraphe 3 ne porte pas atteinte aux droits et libertés d'autrui », ce qui signifie que le droit à la copie ne se confond pas avec le droit visé à l'article 15(1) du RGPD.

120 Art. 15(3) RGPD.

121 Art. 15(4) RGPD.

122 Art. 9, § 2, de la loi du 22 août 2022 relative aux droits du patient.

RGPD[123] que sur son article 23[124], et elle ne paraît pas déraisonnable.

Pour rappel, le patient peut se faire assister par une personne de confiance désignée par lui ou exercer son droit de consultation par l'entremise de celle-ci. Si cette personne est un praticien professionnel, elle consulte également les annotations personnelles du praticien.

Si, après avoir consulté un autre praticien professionnel, le praticien professionnel en charge du patient a inséré une motivation écrite dans le dossier du patient selon laquelle la divulgation d'informations qui le concernent risquerait de causer manifestement un préjudice grave à la santé du patient et que cette motivation est toujours pertinente, le patient exerce son droit de consulter son dossier par l'intermédiaire d'un praticien professionnel désigné par lui et qui pourra consulter les annotations personnelles du praticien[125]. La loi du 22 août 2002 précise elle-même que cette restriction est conforme à l'article 23 du RGPD.

Pour rappel encore, le patient a le droit d'obtenir, aux mêmes conditions que pour sa consultation, une copie de son dossier ou d'une partie de celui-ci[126]. Chaque copie précise que celle-ci est strictement personnelle et confidentielle. Le praticien professionnel peut refuser de donner cette copie s'il dispose d'indications claires selon lesquelles le patient subit des pressions afin de communiquer une copie de son dossier à des tiers[127].

Après le décès du patient, l'époux, le partenaire cohabitant légal, le partenaire et les parents jusqu'au deuxième degré inclus ont, par l'intermédiaire du praticien professionnel désigné par le demandeur, le droit de consulter le dossier du patient, pour autant que leur demande soit suffisamment motivée et spécifiée et que le patient ne s'y soit pas opposé expressément. Le praticien professionnel désigné consulte également les annotations personnelles du praticien professionnel[128].

3. Le droit d'accès par un professionnel de la santé aux données du patient détenues par un autre professionnel de la santé

Un professionnel de la santé peut accéder aux données de santé de son patient qui sont détenues par d'autres professionnels de la santé à condition d'avoir obtenu au préalable le consentement éclairé de son patient à cet accès[129].

Cet accès est restreint aux données à caractère personnel relatives à la santé du patient avec lequel le professionnel de la santé entretient une relation thérapeutique[130].

Le professionnel des soins de santé qui entretient une relation thérapeutique avec le patient a uniquement accès aux données à caractère personnel relatives à la santé de ce patient dans le respect des conditions suivantes[131] :

- la finalité de l'accès consiste à dispenser des soins de santé ;
- l'accès est nécessaire à la continuité et à la qualité des soins de santé dispensés ;
- l'accès se limite aux données utiles et pertinentes dans le cadre de la prestation de soins de santé.

Lorsque, dans un cas d'urgence, il y a une incertitude quant au consentement du patient concernant l'accès d'un professionnel des soins de santé aux données à caractère personnel relatives à sa santé, ce professionnel a accès aux données visées dans le respect des conditions précitées en vue de dispenser les soins de santé nécessaires dans l'intérêt du patient[132].

Le professionnel des soins de santé qui tient à jour et conserve les données personnelles relatives à la santé du patient prend les mesures nécessaires afin que le patient puisse contrôler quelles personnes ont ou ont eu accès à ses données personnelles relatives à la santé[133]. Autrement dit, il doit tenir un fichier des accès aux données du patient et le lui remettre à première demande.

C. Le droit de rectification

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 fournissant une déclaration complémentaire[134]. Toute la question est de savoir ce qu'est une donnée inexacte en matière de santé.

D. Le droit à l'effacement ou à l'oubli

1. Le principe du droit à l'effacement ou à l'oubli

Présenté comme une avancée significative apportée par le Règlement à la protection des données, le *droit à l'effacement*

123 Pour mémoire, l'article 9(4) du RGPD énonce : « Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé. »

124 L'article 23 du RGPD énonce les hypothèses dans lesquelles des restrictions peuvent être apportées aux droits reconnus par le RGPD aux personnes concernées.

125 Art. 9, § 2, de la loi du 22 août 2022 relative aux droits du patient.

126 Voy. l'arrêté royal du 2 février 2007 fixant le montant maximal par page copiée pouvant être demandé au patient dans le cadre de l'exercice du droit d'obtenir une copie du dossier de patient le concernant.

127 Art. 9, § 3, de la loi du 22 août 2022 relative aux droits du patient.

128 Art. 9, § 4, de la loi du 22 août 2022 relative aux droits du patient.

129 Art. 36 de la loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé. Le patient peut exclure certains professionnels des soins de santé.

130 Art. 37 de la loi du 22 avril 2019. Par relation thérapeutique, la loi vise toute relation entre un patient et un professionnel des soins de santé dans le cadre de laquelle des soins de santé sont dispensés. Par ailleurs, cette disposition prévoit que le Roi peut, en indiquant les cas spécifiques d'échange de données à caractère personnel relatives à la santé du patient, désigner les catégories de professionnels des soins de santé qui, malgré le fait qu'ils entretiennent une relation thérapeutique avec le patient, n'ont pas accès à l'échange des données visées.

131 Art. 38 de la loi du 22 avril 2019.

132 Art. 39 de la loi du 22 avril 2019.

133 Art. 40 de la loi du 22 avril 2019.

134 Art. 16 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 RGPD).

ou à l'oubli[135] préexistait toutefois dans la directive 95/46/CE en tant que conséquence logique et, en principe, implacable, de la limite imposée au responsable du traitement dans la durée de conservation des données sous une forme permettant l'identification de la personne concernée au terme de la réalisation des finalités poursuivies. Maintenant, la personne concernée se voit reconnaître expressément le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, des données qui la concernent, dans l'une des hypothèses suivantes, étant entendu que lorsqu'elle exerce ce droit, le responsable du traitement a l'obligation d'effacer ces données dans les meilleurs délais[136] :

1. les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
2. la personne concernée a retiré son consentement et il n'existe pas d'autre fondement juridique au traitement ;
3. la personne concernée s'oppose au traitement pour des raisons tenant à sa situation particulière et il n'existe pas de motif légitime impérieux pour poursuivre le traitement, ou la personne concernée s'oppose au traitement à des fins de prospection ;
4. les données à caractère personnel ont fait l'objet d'un traitement illicite ;
5. les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;
6. les données à caractère personnel ont été collectées dans le cadre de l'offre directe de services de la société de l'information aux enfants.

2. Les effacements subséquents et par ricochet

Lorsqu'il a rendu publiques les données et qu'il est tenu de les effacer, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, doit prendre des mesures raisonnables, y compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci[137].

3. Les exceptions au droit à l'effacement ou à l'oubli

Même lorsque le traitement des données est inutile, dépourvu de fondement juridique, dépourvu de nécessité impérieuse, illicite, et même lorsque la loi impose l'effacement des données, la personne concernée se voit dénier, de manière surprenante et paradoxale, le droit à l'effacement ou à l'oubli des données qui la concernent lorsque le traitement est nécessaire[138] :

1. à l'exercice du droit à la liberté d'expression et d'information ;
2. pour respecter une obligation légale qui impose le traitement et qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
3. pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, § 2, h) et i), ainsi qu'à l'article 9, § 3, du RGPD ;
4. à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89(1) du RGPD, dans la mesure où le droit à l'effacement ou à l'oubli est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs de ce traitement ; ou
5. à la constatation, à l'exercice ou à la défense de droits en justice.

E. Le droit à la limitation du traitement

La personne concernée a le droit d'exiger et d'obtenir du responsable du traitement qu'il limite le traitement des données qui la concernent dans les hypothèses suivantes[139] :

1. lorsque l'exactitude des données est contestée par la personne concernée, et ce, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ;
2. lorsque le traitement est illicite et que la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ;
3. lorsque le responsable du traitement n'a plus besoin des données mais que celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;

135 À ce sujet, voy. C. de Terwangne, « Droit à l'oubli numérique, élément du droit à l'autodétermination informationnelle ? », *in Le droit à l'oubli numérique : données normatives – Approche comparée*, Bruxelles, Larcier, 2015, p. 23 ; « Droit à l'oubli, droit à l'effacement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », *in Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 245, ainsi que : J. Ausloos, *The Right to Erasure in EU Data Protection Law. From Individuals Rights to Effective Protection*, coll. Oxford Data Protection et Privacy Law, Oxford, Oxford University Press, 2020.

136 Art. 17(1) RGPD.

137 Art. 17(2) RGPD. Le responsable du traitement doit notifier à chaque destinataire auquel les données ont été communiquées tout effacement de données effectué, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires, si celle-ci en fait la demande (art. 19 RGPD).

138 Voy. l'article 17(3) du RGPD.

139 Art. 18 RGPD. Lorsque le traitement a été limité, ces données ne peuvent, à l'exception de la conservation, être traitées qu'avec le consentement de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice, ou pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre. Le responsable du traitement ne peut lever la limitation au traitement qu'après en avoir informé la personne concernée. Par ailleurs, le responsable du traitement doit notifier à chaque destinataire auquel les données à caractère personnel ont été communiquées toute limitation du traitement effectué, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires, si celle-ci en fait la demande (art. 19 RGPD).

4. lorsque la personne concernée s'est opposée au traitement pour des raisons tenant à sa situation particulière, et ce, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement ne prévaudraient pas sur ceux de la personne concernée.

F. Le droit à la portabilité des données

Le RGPD prévoit expressément que, lorsque les données sont traitées sur la 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 utilisé et lisible par machine, les données qu'elle lui a fournies[140]. 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[141]. 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[142].

Une 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. De manière générale, le Comité européen de protection des données considère que les données fournies par la personne incluent celles qui découlent de l'observation de ses activités. En revanche, il rejette les données générées par le responsable du traitement, fût-ce à partir des données observées ou fournies directement par la personne concernée[143]. Il donne, d'ailleurs, expressément le cas d'une appréciation relative à la santé d'un utilisateur. Le Comité européen de protection des données exclut les données déduites ou dérivées, ce qui comprend les données créées par un prestataire de services.

G. Le droit d'opposition

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 commerciale. L'existence de ce double droit est 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[144].

1. Le droit de s'opposer au traitement de données pour des raisons tenant à la situation particulière de la personne concernée

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[145]. 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. À la suite de 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.

2. Le droit de s'opposer au traitement de données à des fins de prospection

La personne concernée a le droit de s'opposer à tout moment, et sans avoir à se justifier, au traitement des données qui la concernent ou au profilage réalisé dans une finalité de prospection. Lorsque la personne concernée s'oppose au traitement à des fins de prospection, les données à caractère personnel ne sont plus traitées à ces fins.

H. Le droit de ne pas être soumis à une décision individuelle automatisée en ce compris au profilage

La personne concernée a 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[146].

Comme auparavant, ce droit ne peut pas être invoqué lorsque la décision automatisée[147] :

1. est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;

140 Au sujet du droit à la portabilité, voy. not. S. Elfering, *Unlocking the Right to Data Portability. An Analysis of the Interface with the Sui Generis Database Right*, Nomos, Munich Intellectual Property Law Center Studies, 2019, p. 38.

141 Voy. l'article 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.

142 Groupe de travail « Art. 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.

143 *Ibid.*, p. 12.

144 Voy. l'article 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.

145 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 (voy. l'article 21(6) du RGPD).

146 Voy. l'article 22 du RGPD.

147 Toutefois, les décisions automatisées ne peuvent pas se fonder sur les catégories particulières de données, à moins que (i) la personne concernée n'ait donné son consentement explicite ou que le traitement ne soit le traitement nécessaire pour des motifs d'intérêt public importants et (ii) que, dans les deux hypothèses, des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée soient mises en œuvre.

2. 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
3. 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 comme les données concernant la santé, 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 importants 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 mises en œuvre.

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.

VII. L'Autorité de protection des données, les recours et les sanctions

Dans la droite ligne de ce qui avait été prévu dès l'origine, mais de manière plus complète et plus élaborée, le RGPD prévoit des organes, des recours et des sanctions spécifiques afin d'assurer l'effectivité du cadre juridique qui encadre les traitements de données et les droits des personnes concernées[148].

Ainsi, chaque État membre a le droit de disposer d'une ou plusieurs autorités publiques *indépendantes* chargées de surveiller l'application du RGPD afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement de données et de faciliter le libre flux des données au sein de l'Union[149]. C'est l'Autorité de protection des données qui remplit cette fonction en Belgique.

Le RGPD a remplacé le Groupe de travail de l'article 29 par le Comité européen de la protection des données. Le Secrétariat de ce comité est assuré par le Contrôleur européen de la protection des données.

L'objectif est que la protection des données se développe dans un cadre juridique qui soit à la fois effectif et coercitif, c'est-à-dire qui permette de contraindre les individus, les entreprises et les autorités publiques à se soumettre à ses règles. À cet effet, la personne concernée a le droit de saisir l'autorité de contrôle compétente d'une violation de la protection des données à propos d'un traitement qui la concerne. Par ailleurs, un recours peut être introduit contre l'autorité de contrôle ainsi que contre un responsable du traitement ou un sous-traitant. La personne concernée a le droit d'être indemnisée en cas de dommage et l'autorité de contrôle peut infliger des amendes administratives au responsable du traitement ou au sous-traitant. En tout état de cause, chaque État membre doit mettre en place des sanctions effectives, proportionnées et dissuasives pour les violations de la protection des données[150].

L'imposition d'amendes administratives importantes est un des points régulièrement mis en avant dans la mise en œuvre du RGPD. Il faut toutefois distinguer entre le « simple » responsable du 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[151].

Au sens de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, sont des autorités publiques :

1. l'État fédéral, les entités fédérées et les autorités locales ;
2. les personnes morales de droit public qui dépendent de l'État fédéral, des entités fédérées ou des autorités locales ;
3. les personnes, quelles que soient leur forme et leur nature, qui :
   - ont été créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial ; et
   - sont dotées de la personnalité juridique ; et
   - dont soit l'activité est financée majoritairement par les autorités publiques ou organismes mentionnés au 1° ou 2°, soit la gestion est soumise à un contrôle de ces autorités ou organismes, soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par ces autorités ou organismes ;
4. les associations formées par une ou plusieurs autorités publiques visées ci-dessus.

148 Cette section reprend des extraits remaniés et mis à jour de deux publications antérieures : J. Herveg et J.-M. Van Gyseghem, « Un nouveau métier de la santé : la sous-traitance des données du patient », *op. cit.*, pp. 747-764 ; J. Herveg, « Réflexions autour de la protection des données et des vulnérabilités », *op. cit.*, 2018, pp. 333-392.

149 Voy. l'article 51 du RGPD sur le principe de l'indépendance et l'article 55 du RGPD sur la question des compétences de l'autorité de contrôle (elle est compétente pour le territoire de l'État membre dont elle relève ; pour les traitements nécessaires pour le respect d'une obligation légale à laquelle le responsable du traitement est soumis ou pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, c'est l'autorité de contrôle de l'État membre concerné qui est compétente, et l'article 56 du RGPD ne s'applique pas à propos de la compétence de l'autorité de contrôle chef de file). Conformément à l'article 4(22) du RGPD, une autorité de contrôle est concernée lorsque :

1. le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de contrôle relève ;
2. des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être ;
3. une réclamation a été introduite auprès de cette autorité de contrôle.

Il est, par ailleurs, expressément prévu que les autorités de contrôle ne sont pas compétentes pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leurs fonctions juridictionnelles (art. 55(3) RGPD). Les missions et les pouvoirs des autorités de contrôle sont détaillés aux articles 57 et 58 du RGPD.

150 Voy. les articles 77 et suivants du RGPD.

151 Voy. l'article 83(7) du RGPD.

Il résulte de l'article 221, § 2, de cette même loi que l'Autorité de protection des données ne peut pas imposer d'amendes administratives aux hôpitaux qui répondent à cette définition de la notion d'autorité publique, sauf s'il s'agit de personnes morales de droit public qui offrent des biens ou services sur un marché.

Enfin, il faut rappeler que la loi du 30 juillet 2018 incrimine toute une série de violations du RGPD[152].

Conclusion

Le Règlement général sur la protection des données est d'application depuis le 25 mai 2018 et il concerne les hôpitaux au même titre que tous les autres acteurs de la vie économique, sociale et culturelle.

Le RGPD ne porte pas atteinte aux règles relatives au secret professionnel, pas plus qu'à celles contenues dans la loi relative aux droits du patient ou à celles contenues dans la loi relative à la qualité de la pratique des soins de santé.

Le RGPD s'applique à tous les traitements de données du patient qui interviennent au sein de l'hôpital, en ce compris ceux qui portent sur les données concernant la santé du patient.

L'hôpital est le responsable du traitement des données du patient et, moyennant le respect d'un certain nombre de conditions, il peut faire appel à un sous-traitant pour effectuer des traitements de données à sa place et pour son compte. Le personnel médical, infirmier, administratif ou technique, bénévole ou non, salarié ou indépendant, tombe dans la catégorie des personnes qui traitent des données sous l'autorité de l'hôpital, étant entendu que cette notion d'autorité ne correspond pas à celle connue en droit du travail ; il s'agit d'un concept autonome de droit européen.

Le traitement des données du patient à l'hôpital doit être conforme aux principes applicables à tous les traitements de données : licéité, loyauté, transparence, limitation des finalités, minimisation des données, exactitude des données, durée de conservation, intégrité et confidentialité des données et, enfin, responsabilité. Il doit, en outre, être licite, c'est-à-dire pouvoir se prévaloir d'une base juridique énoncée dans le RGPD sous l'article 6 pour les données « ordinaires » ou sous l'article 9 pour les catégories particulières de données, ce qui englobe les données concernant la santé du patient.

L'hôpital doit se conformer aux obligations générales en matière de traitement de données et veiller à la sécurité des données. Il est en tout cas obligé de réaliser une analyse d'impact et de désigner un délégué à la protection des données.

Le patient se voit reconnaître les mêmes droits que toute autre personne concernée. Toutefois, son droit d'accès à son dossier de patient est modalisé par la loi du 22 août 2002 relative aux droits du patient.

L'accès par un praticien professionnel de la santé aux données du patient détenues par un autre professionnel de la santé est modalisé par la loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé.

Aucune de ces deux « restrictions » ou « modalités » ne paraît déraisonnable, donc contraire au RGPD, même s'il faut quand même vérifier au cas par cas si elles sont concrètement justifiées dans chaque cas d'espèce, sauf à courir le risque de se faire reprocher de violer le droit au respect de la vie privée du patient.

Les patients ne doivent pas hésiter à réclamer et à prendre connaissance des fichiers contenant la liste des personnes ayant accédé à leur dossier ni à revendiquer réparation lorsque l'hôpital a méconnu ses obligations en matière de protection des données.

L'Autorité de protection des données ne peut pas imposer d'amendes administratives aux hôpitaux qui ont la qualité d'autorités publiques au sens de la loi du 30 juillet 2019, sauf s'ils agissent en qualité de personnes morales de droit public qui offrent des biens ou services sur un marché.

Maintenant, toute la question est de savoir si l'application du RGPD a réellement profité à la protection des données du patient et si son coût n'a pas largement dépassé ses bénéfices… À ce jour, sauf en matière de droit d'accès, les patients ne semblent pas vraiment avoir expérimenté une réelle augmentation de leur maîtrise sur les données qui les concernent (le rêve d'un droit à l'autodétermination informationnelle n'a jamais semblé aussi lointain) et les ressources qui sont affectées à la mise en œuvre du RGPD sont autant d'argent qui n'est pas investi dans l'amélioration de l'accès aux soins et aux médicaments.

Il faut aussi voir que plusieurs principes de la protection des données ne sont tout simplement plus tenables (comme le principe de la minimisation des données à l'âge du « *big data* », de l'intelligence artificielle et du « *machine learning* » ou comme l'exigence de traitements restreints aux seules données « strictement nécessaires » dans un contexte thérapeutique ou de recherche scientifique).

La notion de données à caractère personnel est tellement large que la question n'est plus tant de savoir si une donnée est à caractère personnel que de savoir s'il existerait encore des données qui ne seraient pas à caractère personnel. De plus, sauf pour des raisons culturelles ou historiques, il n'est pas non plus certain qu'il soit utile de maintenir une distinction entre données « ordinaires » et données « sensibles », puisque le risque pour la personne n'est pas lié au contenu informationnel mais bien à l'usage qui est fait de l'information, étant entendu que le contenu des données « sensibles » est de nature à accroître ce risque. Cela ne justifie toutefois pas le maintien de cette distinction.

Les subtilités liées à l'identification des responsables du traitement et des sous-traitants sont stupéfiantes et ne laissent pas de surprendre d'autant qu'*in fine*, tout le monde est soumis, en quelque sorte, *mutatis mutandis*, aux mêmes conditions pour traiter des données.

Il est temps de simplifier les règles de la protection des données et d'aboutir à une véritable protection des données qui soit praticable par tout le monde : tant par ceux qui ont besoin de traiter des données que par ceux qui sont concernés par le traitement de leurs données : les citoyens européens.

Jean Herveg
Avocat au barreau de Bruxelles
Directeur de l'unité de recherche LIS à l'UNamur,
Faculté de Droit, CRIDS

152 Voy. les articles 222 à 230 de la loi du 30 juillet 2018.