La sous-traitance des données du patient au regard de la directive 95/46

Herveg, Jean; Van Gyseghem, Jean-Marc

Published in:
Lex Electronica

Publication date:
2004

Document Version
le PDF de l'éditeur

LA SOUS-TRAITANCE DES DONNEES DU PATIENT AU REGARD DE LA DIRECTIVE 95/46

Herveg J. et Van Gyseghem J.M.*

Lex Electronica, vol. 9 n° 3, Été 2004,
http://www.lex-electronica.org/articles/v9-3/herveg_vangyseghem.htm

---

Introduction[1]

1. L'information relative au patient occupe une place significative dans la pratique de l'art de guérir. Il s'agit de toute information qui renseigne le praticien de la santé sur son patient et permet de lui prodiguer les soins de santé[2] les plus adéquats.

Le patient représente à cet égard une première source d'information, directe et indirecte. Il donne déjà de l'information au praticien de la santé lors de l'anamnèse. Celle-ci peut se définir comme étant les « *renseignements fournis par le sujet interrogé sur son passé et sur l'histoire de sa maladie* ». C'est une évocation par le patient de son passé. Cette « *instruction médicale* » est importante mais délicate à mener. En effet, le patient se raconte avec des mots. Or, ceux-ci passent par le filtre subjectif de la perception de son vécu. De même, l'auscultation du patient fournit d'autres informations nécessaires aux soins de santé à prodiguer. Le verbe n'est pas le vecteur premier de cette source d'information, et le patient est susceptible d'influencer cette information par la maîtrise éventuelle de ses réactions physiologiques. Le praticien de la santé doit conjuguer ces deux sources d'information et faire œuvre interprétative pour dégager l'information utile à l'octroi des soins de santé.

La production de l'information relative au patient se déroule fréquemment dans des situations complexes, dans lesquelles le patient est pris en charge par plusieurs praticiens de la santé, appartenant à une même équipe de soins ou agissant soit conjointement soit successivement dans la prise en charge

---

* Les auteurs sont chercheurs au Centre de Recherche Informatique et Droit (CRID) de la Faculté de droit de Namur (FUNDP) en Belgique. Ils sont tous deux avocats au Barreau de Bruxelles (Belgique).

1 This work was supported by the EC under Research Contract IST-2001-37153 GEMSS. Cet article a fait l'objet d'une présentation orale par Jean Herveg à l'occasion du Congrès de la *World Association for Medical Law* qui s'est tenu à Sydney (Australie) du 01 au 05.08.2004.

2 La notion de soins de santé doit être comprise largement ; elle vise tant les aspects curatifs que préventifs, etc.

du patient. Cela vise les hôpitaux, les cliniques, les polycliniques, les centres médicaux, les maisons médicales, etc. Chaque praticien de la santé intervient et produit de l'information au sujet du patient, en fonction de son rôle et de ses compétences dans sa prise en charge.

La coordination de l'information produite dans ces situations complexes devrait être organisée en parallèle avec la coordination de l'intervention des différents praticiens de la santé impliqués dans la prise en charge du patient. On pourrait songer dans ce cas à désigner un praticien responsable de cette coordination.

Il arrive fréquemment que le praticien ou l'équipe de praticiens de la santé ne dispose pas *en interne* de toute la connaissance requise pour la prise en charge du patient, ou du matériel requis pour produire ou gérer l'information nécessaire afin de le soigner. Dans cette hypothèse, appel sera fait à des praticiens de la santé *extérieurs* à leur propre structure. Il peut s'agir d'un laboratoire d'analyses médicales, de services d'imageries médicales, d'un confrère plus spécialisé, etc. Ceux-ci vont également produire de l'information relative au patient. Dans de nombreux cas, ils interviendront en outre activement dans la prise en charge du patient, au-delà de la simple production d'information à son sujet.

Dans le même temps, l'évolution des techniques médicales permet la fourniture d'une plus grande quantité d'informations relatives au patient, plus complètes et plus fiables. Ces informations se présentent souvent sous une forme informatisée.

2. Le praticien de la santé isolé ou l'équipe de praticiens de la santé utilisent aussi les ressources récentes de l'informatique et de la télématique pour gérer au mieux l'information relative à leurs patients, en fonction des besoins spécifiques de leur pratique professionnelle.

A cet égard, il devient très fréquent que des tiers leur proposent des services relatifs à la gestion *technique* de l'information relative au patient. Ils leur offrent ainsi des services de stockage de l'information (voire d'archivage), de maintenance des systèmes informatiques, des outils supportant la communication et le partage de l'information relative au patient entre les différents professionnels de la santé participant à sa prise en charge collective ou conjointe notamment par le biais de réseaux télématiques, etc. Des sites Internet offrent même des services dédicacés au traitement de données liées à des thématiques particulières telles que la génétique ou des maladies particulières.

3. Le praticien ou l'équipe de praticiens de la santé en charge du patient sont donc de moins en moins seuls dans la gestion de l'information relative à son patient. Des personnes extérieures à leur structure interviennent fréquemment dans la gestion de cette information.

Deux catégories de prestataires ont ainsi été distinguées. D'une part, les prestataires qui sont des praticiens de la santé et qui *produisent ou gèrent* à ce titre de l'information relative au patient. D'autre part, les prestataires qui ne sont pas des praticiens de la santé et ne participent pas à la prise en charge médicale du patient, mais qui, par la nature des services qu'ils offrent, participent à la gestion *technique* de l'information relative au patient. De nombreuses variations existent bien entendu entre ces deux catégories.

Le recours à la première catégorie de prestataires est ordinaire. Par contre, l'intervention de la seconde catégorie de prestataires augmente sensiblement dans la gestion technique de l'information relative au patient.

Quoiqu'il en soit, ces deux catégories ont en commun de ne pas appartenir à la structure de travail du praticien ou de l'équipe en charge du patient et dès lors de ne pas travailler sous leur direction. Ils leur sont *extérieurs*, ce qui justifie de s'intéresser aux règles juridiques applicables à leur intervention dans la gestion des données du patient.

I. Directive Vie Privée : champ d'application et définitions

4. La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (dénommée ci-après « *directive « Vie Privée »* »)[3], intéresse plusieurs aspects juridiques de la gestion de l'information relative au patient, et est susceptible de fournir une partie de la réponse à la question du statut juridique des tiers intervenant dans cette gestion, qu'ils soient praticiens de la santé ou non.

La directive vise à ce que « *Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel* »[4]. Elle « (…) *s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* »[5].

Les « données à caractère personnel » sont « *toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* »[6].

---

[3] D., 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281, 23/11/1995, pp. 0031-0050, art. 3.1. A son propos, voyez not. [Boulanger et al. 1997].

[4] D., 95/46/CE, *o.c.*, art. 1.1.

[5] D., 95/46/CE, *o.c.*, art. 3.1. L'article 3.2 ajoute que :
« *La présente directive ne s'applique pas au traitement de données à caractère personnel:*
- mis en oeuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal,
- effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. »
Le considérant (12) donne la correspondance et la tenue de répertoires d'adresses comme exemple d'activités exclusivement personnelles ou domestiques.
Sur la possibilité de la législation nationale d'étendre le champ d'application de la protection à des domaines non couverts par la directive « Vie Privée », voyez : C.J.C.E., arrêt du 06 nov. 2003, Bodil Lindqvist, C-101/01 : « (…) *6) Les mesures prises par les États membres pour assurer la protection des données à caractère personnel doivent être conformes tant aux dispositions de la directive 95/46 qu'à son objectif consistant à maintenir un équilibre entre la libre circulation des données à caractère personnel et la protection de la vie privée.* ***En revanche****, rien ne s'oppose à ce qu'un État membre étende la portée de la législation nationale transposant les dispositions de la directive 95/46 à des domaines non inclus dans le champ d'application de cette dernière, pour autant qu'aucune autre disposition du droit communautaire n'y fasse obstacle*. »

[6] D., 95/46/CE, *o.c.*, art. 2, a.

Pour déterminer si une personne est *identifiable*, il convient de considérer l'ensemble des moyens susceptibles d'être *raisonnablement* mis en oeuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne[7].

La notion de « données à caractère personnel » englobe les données constituées par des *sons* et des *images* relatives à des personnes physiques[8]. De même, les adresses IP attribuées aux internautes sont des données à caractère personnel au sens de la directive « Vie Privée »[9].

Logiquement, la directive « Vie Privée » ne s'applique donc pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiée ni identifiable[10]. Par contre, elle s'applique aux données codées.

La directive « Vie Privée » ne s'applique que si les données à caractère personnel font l'objet d'un traitement automatisé ou si les données sur lesquelles il porte sont contenues ou destinées à être contenues dans un fichier structuré selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause[11].

Elle précise à cet égard que le « traitement de données à caractère personnel » est « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* »[12], et qui s'inscrivent dans la même finalité.

Le «fichier de données à caractère personnel» est, quant à lui, défini comme « *tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique*. »[13]

---

7 D., 95/46/CE, *o.c*., considérant (26).

8 D., 95/46/CE, *o.c*., considérant (14).

9 En ce sens, voyez [Working Party 2002].

10 D., 95/46/CE, *o.c*., considérant (26). Les codes de conduite au sens de l'article 27 de la directive « Vie Privée » peuvent être des instruments utiles pour fournir des indications sur les moyens par lesquels les données peuvent être rendues anonymes et conservées sous une forme ne permettant plus l'identification de la personne concernée (ibidem).

11 D., 95/46/CE, *o.c*., considérant (15).

12 D., 95/46/CE, *o.c*., art. 2, b. Pour un exemple de traitement de données à caractère personnel, voyez : C.J.C.E., arrêt du 06 nov. 2003, o.c. :
« *1) L'opération consistant à faire référence, sur une page Internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un "traitement de données à caractère personnel, automatisé en tout ou en partie," au sens de l'article 3, paragraphe 1, de la directive 95/46 /CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données .*
2) Un tel traitement de données à caractère personnel ne relève d'aucune des exceptions figurant à l'article 3, paragraphe 2, de la directive 95/46. »

13 D., 95/46/CE, *o.c*., art. 2, c. Le considérant (27) précise que « *la protection des personnes doit s'appliquer aussi bien au traitement de données automatisé qu'au traitement manuel; que le champ de cette protection ne doit pas en effet dépendre des techniques utilisées, sauf à créer de graves risques de détournement; que, toutefois, s'agissant du traitement*

Le «responsable du traitement » de données à caractère personnel est « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres,* ***détermine les finalités et les moyens*** *du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire*. »[14]

Le responsable du traitement peut recourir aux services d'un «sous-traitant». Il s'agit de « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme, qui traite des données à caractère personnel pour le compte du responsable du traitement.* »[15]

Le «tiers» au traitement de données à caractère personnel est « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données*. »[16]

II. Principes de la Directive Vie Privée

5. La directive « Vie privée » pose les conditions générales de licéité des traitements de données à caractère personnel[17]. A cet effet, elle affirme les principes relatifs à la qualité des données[18], ainsi que ceux relatifs à la légitimation des traitements de données[19]. Elle établit des règles spéciales pour des catégories particulières de traitements[20], dont les traitements de données relatives à la santé[21] à raison

---

manuel, la présente directive ne couvre que les fichiers et ne s'applique pas aux dossiers non structurés; que, en particulier, le contenu d'un fichier doit être structuré selon des critères déterminés relatifs aux personnes permettant un accès facile aux données à caractère personnel; que, conformément à la définition figurant à l'article 2 point c), les différents critères permettant de déterminer les éléments d'un ensemble structuré de données à caractère personnel et les différents critères régissant l'accès à cet ensemble de données peuvent être définis par chaque État membre; que les dossiers ou ensembles de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés n'entrent en aucun cas dans le champ d'application de la présente directive. »

[14] D., 95/46/CE, *o.c*., art. 2, d. Lorsqu'un message contenant des données à caractère personnel est transmis via un service de télécommunications ou de courrier électronique dont le seul objet est de transmettre des messages de ce type, c'est la personne dont émane le message, et non celle qui offre le service de transmission, qui sera normalement considérée comme responsable du traitement de données à caractère personnel contenues dans le message. Toutefois, les personnes qui offrent ces services seront normalement considérées comme responsables du traitement des données à caractère personnel supplémentaires nécessaires au fonctionnement du service (considérant 47).

[15] D., 95/46/CE, *o.c*., art. 2, e.

[16] D., 95/46/CE, *o.c*., art. 2, f.

[17] D., 95/46/CE, *o.c*., art. 5 à 21.

[18] D., 95/46/CE, *o.c*., art. 6.1 : les données doivent être traitées loyalement et licitement ; collectées pour des finalités déterminées, explicites et légitimes ; adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ; exactes et si nécessaire mises à jour ; conservées pendant un délai déterminé sans oublier les finalités historiques, statistiques ou scientifiques.

[19] D., 95/46/CE, *o.c*., art. 7 : cinq hypothèses légitiment le traitement de données à caractère personnel.

[20] D., 95/46/CE, *o.c*., art. 8 et 9.

[21] Le traitement de données à caractère personnel relatives à la santé est interdit (D., 95/46/CE, o.c., art. 8.1). Cette interdiction ne s'applique pas, principalement lorsque :
(1) la personne concernée a donné son *consentement* explicite à un tel traitement, à moins que la législation de l'État membre prévoie que cette interdiction ne peut pas être levée par le consentement de la personne concernée (D., 95/46/CE, o.c., art. 8.2, a) ;

de leur caractère particulièrement sensible[22]. La personne concernée doit recevoir un certain nombre d'informations au sujet du traitement de ses données et se voit aussi reconnaître un droit d'accès à ses données[23]. Elle peut aussi, sous certaines conditions, s'opposer au traitement de ses données[24]. La confidentialité et la sécurité du traitement de données doivent être assurés[25].

La directive « Vie Privée » organise encore la notification préalable du traitement de données à une autorité de contrôle[26], ainsi que la publicité des traitements de données[27]. Elle prévoit aussi des contrôles juridictionnels[28], une responsabilité spécifique dans le chef du responsable du traitement de données[29], et des sanctions appropriées[30].

Le *transfert* de données à caractère personnel vers des pays tiers à l'Union européenne répond à des règles spéciales[31]. La directive « Vie Privée » prévoit à cet égard que le transfert vers un pays tiers de

---

(2) le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouverait dans l'incapacité physique ou juridique de donner son consentement (D., 95/46/CE, o.c., art. 8.2, c) ;
(3) le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente (D., 95/46/CE, o.c., art. 8.3).
Ceci étant, la directive ne définit pas les données relatives à la santé et ne fournit pas d'indices pour élaborer une quelconque définition. Pour un exemple récent de données relatives à la santé, voyez : C.J.C.E., arrêt du 06 nov. 2003, o.c. : « *3) L'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, paragraphe 1, de la directive 95/46.* »

22 Dans son document de travail sur les données génétiques du 17 mars 2004, le groupe 29 (Groupe de protection des données) a rappelé que « *Selon l'article 8 paragraphe 1 de la directive, les catégories de données personnelles dont la sensibilité requiert un niveau de protection plus élevé comprennent les « données relatives à la santé.* » *Les données génétiques peuvent, dans une certaine mesure, donner une image détaillée de la condition physique d'un individu et de son état de santé et pourraient, à ce titre, être considérées comme des « données relatives à la santé ». »*

23 D., 95/46/CE, *o.c.*, art. 10, 11, 12, et 13. Toute personne doit pouvoir bénéficier du droit d'accès aux données la concernant qui font l'objet d'un traitement, afin de s'assurer notamment de leur exactitude et de la licéité de leur traitement (considérant 41). Dans l'intérêt de la personne concernée ou en vue de protéger les droits et libertés d'autrui, les droits d'accès et d'information peuvent être limités. Ainsi, par exemple, il peut être prévu que l'accès aux données à caractère médical ne peut être obtenu que par l'intermédiaire d'un professionnel de la santé (considérant 42).

24 D., 95/46/CE, *o.c.*, art. 14. A propos des décisions individuelles automatisées, voyez l'article 15.

25 D., 95/46/CE, *o.c.*, art. 16 et 17.

26 D., 95/46/CE, *o.c.*, art. 18 à 20. Les autorités de contrôle sont visées à l'article 28 de la directive. Le Groupe de protection des personnes à l'égard du traitement des données à caractère personnel est créé par l'article 29 de la directive (voyez l'art. 30 pour la mission conférée à ce groupe de protection).

27 D., 95/46/CE, *o.c.*, art. 21.

28 D., 95/46/CE, *o.c.*, art. 22.

29 D., 95/46/CE, *o.c.*, art. 23.

30 D., 95/46/CE, *o.c.*, art. 24.

31 D., 95/46/CE, o.c., art. 24 à 26. A propos de la notion de « transfert vers un pays tiers de données », voyez : C.J.C.E., arrêt du 06 nov. 2003, o.c. : « *4) Il n'existe pas de "transfert vers un pays tiers de données" au sens de l'article 25 de la directive 95/46 lorsqu'une personne qui se trouve dans un État membre inscrit sur une page Internet, stockée auprès d'une personne physique ou morale qui héberge le site Internet sur lequel la page peut être consultée et qui est établie dans ce même État ou un autre État membre, des données à caractère personnel, les rendant ainsi accessibles à toute personne qui se connecte à Internet, y compris des personnes se trouvant dans des pays tiers*. »

données à caractère personnel faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat[32]. Si le pays tiers n'offre pas un niveau de protection adéquat, le transfert de données à caractère personnel vers ce pays doit être interdit[33], sauf exceptions[34].

III. Directive Vie Privée et sous-traitance de données

6. La plupart des prestataires extérieurs qui interviennent dans la gestion de l'information relative au patient (repris *supra*, n° 3) sont susceptibles de traiter des données à caractère personnel relatives à sa santé, soit, pour la première catégorie de prestataires praticiens de la santé, en les *produisant*, soit, pour la seconde catégorie de prestataires non praticiens de la santé, en participant à leur gestion *technique*.

La directive « Vie Privée » apporte des précisions à propos de l'intervention de ces prestataires extérieurs dans la gestion des données du patient.

Si ces prestataires extérieurs agissent pour le compte du responsable du traitement, *sans être placés sous l'autorité directe de celui-ci*, ils devraient recevoir la qualification de « sous-traitant » de données à caractère personnel au sens de la directive « Vie Privée ».

Le responsable du traitement de données à caractère personnel doit alors choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer, et il doit veiller au respect de ces mesures[35]. A cet égard, il faut rappeler que le responsable du traitement doit mettre en oeuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de

---

32 D., 95/46/CE, *o.c.*, art. 25.1. Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées (D., 95/46/CE, *o.c.*, art. 25.2) (voyez aussi le considérant 56).

33 D., 95/46/CE, *o.c.*, considérant (57).

34 L'article 26 prévoit des dérogations à l'interdiction de transférer des données à caractère personnel vers un pays tiers qui n'assure pas un niveau de protection adéquat (voyez aussi à ce propos les considérants 58 et 59). Cela vise notamment le consentement de la personne concernée, le transfert nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée, le transfert nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers, le transfert nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice, le transfert nécessaire à la sauvegarde de l'intérêt vital de la personne concernée. Le transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25.2, peut aussi être autorisé lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants, ces garanties pouvant notamment résulter de clauses contractuelles appropriées. La Commission européenne a rédigé des clauses modèles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/EC, conformément à l'article 26.4 de la directive (voyez la décision de la Commission du 15 juin 2001).

35 D., 95/46/CE, o.c., art. 17.2.

traitement illicite[36]. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger[37].

L'existence de labels de « sécurité » pourrait faciliter la sélection des sous-traitants par le responsable du traitement[38]. Il resterait à définir la qualité de l'organe de labellisation, ainsi que les modalités de son attribution et de son retrait.

Le sous-traitant et toute personne agissant sous son autorité, qui accède à des données à caractère personnel, ne peut les traiter que sur *instruction* du responsable du traitement, sauf en vertu d'obligations légales[39].

La réalisation d'un traitement de données à caractère personnel en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que[40] :

- le sous-traitant n'agit que sur la seule instruction du responsable du traitement,

- les mesures techniques et d'organisation à mettre en œuvre pour protéger les données à caractère personnel[41] incombent également au sous-traitant.

À des fins probatoires, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures techniques et d'organisation, sont consignés par écrit ou sous une autre forme équivalente[42].

Si ce sous-traitant fait appel à un autre sous-traitant de données, l'intervention de ce dernier doit également être régie par un contrat ou un acte juridique qui le lie ***directement*** au responsable du traitement, et pas seulement au premier sous-traitant.

---

36 D., 95/46/CE, *o.c.*, art. 17.1.

37 D., 95/46/CE, o.c., art. 17.1. La protection des droits et libertés des personnes concernées à l'égard du traitement de données à caractère personnel exige que des mesures techniques et d'organisation appropriées soient prises tant au moment de la conception qu'à celui de la mise en oeuvre du traitement, en vue d'assurer en particulier la sécurité et d'empêcher ainsi tout traitement non autorisé. Il incombe aux États membres de veiller au respect de ces mesures par les responsables du traitement. Ces mesures doivent assurer un niveau de sécurité approprié tenant compte de l'état de l'art et du coût de leur mise en oeuvre au regard des risques présentés par les traitements et de la nature des données à protéger (considérant 46). Pour un exemple de mesures de sécurité en matière d'imageries médicales à distance, voyez [Middleton 2004].

38 En ce sens, en matière d'imageries médicales, voyez not. [Herveg 2003]. Dans le même ordre d'idées, les États membres et la Commission, dans leurs domaines de compétence respectifs, doivent encourager les milieux professionnels concernés à élaborer des codes de conduite en vue de favoriser, compte tenu des spécificités du traitement de données effectué dans certains secteurs, la mise en oeuvre de la présente directive dans le respect des dispositions nationales prises pour son application (considérant 61). L'article 27 de la directive concerne spécifiquement les codes de conduite.

39 D., 95/46/CE, *o.c.*, art. 16.

40 D., 95/46/CE, *o.c.*, art. 17.3.

41 Telles que définies par la législation de l'État membre dans lequel le sous-traitant est établi (D., 95/46/CE, *o.c.*, art. 17.3).

42 D., 95/46/CE, *o.c.*, art. 17.4.

La licéité de l'intervention de ces prestataires extérieurs doit aussi être justifiée au regard de l'interdiction de traiter des données relatives à la santé. A cet effet, ils doivent répondre à une des principales hypothèses suivantes[43] :

(1) le patient a donné son consentement explicite au traitement des données relatives à sa santé,

(2) le traitement est nécessaire à la défense de ses intérêts vitaux ou d'une autre personne dans le cas où la personne concernée est dans l'incapacité physique ou juridique de donner son consentement,

(3) le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé, ***et*** le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel ou par une autre personne également soumise à une obligation équivalente de secret[44].

IV. Sous-traitance de données et contrôle préalable

7. Mais ces mesures sont-elles suffisantes lorsqu'un prestataire extérieur intervient dans la gestion de données du patient particulièrement sensibles telles que des données génétiques, surtout quand il n'est pas un praticien de la santé et qu'il n'intervient pas autrement dans la prise en charge médicale du patient ? L'exemple le plus aigu à prendre en considération à ce titre serait le site Internet offrant une plate-forme pour traiter des données génétiques du patient.

La Cour européenne des droits de l'homme a déjà fermement rappelé l'importance fondamentale de la protection des données médicales[45] :

> « (…) *la protection des données à caractère personnel, et spécialement des données médicales, revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention. Le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique de toutes les Parties contractantes à la Convention. Il est capital non seulement pour protéger la vie privée des malades mais également pour préserver leur confiance dans le corps médical et les services de santé en général. La législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention (...).* »

Ne serait-il dès lors pas opportun d'envisager, à propos de données très sensibles comme les données génétiques, l'organisation d'un contrôle préalable tel que prévu à l'article 20 de la directive « Vie

---

[43] A ce propos, voyez *supra*, la note infra-paginale n° 21. Il faut rappeler en outre que, sous réserve de garanties appropriées, les États membres peuvent prévoir, pour un motif d'intérêt public important, d'autres dérogations que celles prévues à l'article 8.2 de la directive « Vie Privée », soit par leur législation nationale, soit sur décision de l'autorité de contrôle (D., 95/46/CE, o.c., art. 8.4). Ces dérogations doivent être notifiées à la Commission européenne (D., 95/46/CE, o.c., art. 8.6).

[44] Une obligation contractuelle de secret est-elle équivalente ? L'équivalence doit être également envisagée sous l'angle des effets liés à la méconnaissance du secret et donc aux sanctions qui y sont attachées.

[45] C.E.D.H., M.S. v. Suède du 27 août 1997, § 41. L'arrêt fait référence à l'arrêt Z. c Finlande du 25 février 1997.

Privée » ? Cette disposition prévoit en effet que « *Les États membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre.* »[46] Elle précise que « *De tels examens préalables sont effectués par l'autorité de contrôle après réception de la notification du responsable du traitement ou par le détaché à la protection des données, qui, en cas de doute, doit consulter l'autorité de contrôle*. »[47] A la suite de cet examen préalable, l'autorité de contrôle peut, selon le droit national dont elle relève, émettre un avis ou autoriser le traitement des données[48].

L'intervention d'un détaché à la protection des données pourrait d'ailleurs être accompagnée d'une simplification ou d'une dérogation à l'obligation de notifier le traitement de données à l'autorité de contrôle[49].

V. Quel responsable de traitement de données pour quel sous-traitant de données ?

8. Si les prestataires extérieurs intervenant dans la gestion des données du patient agissent en qualité de sous-traitant, il reste à déterminer le responsable du traitement de données. A cet égard, sans préjudice de l'hypothèse où la loi fixe les finalités et les moyens et où le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire, la désignation concrète au cas par cas de la personne qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données, est fortement tributaire du poids socialement reconnu et attribué aux différents acteurs de la relation thérapeutique.

À ce jour, l'esprit est enclin à considérer que c'est le praticien de la santé en charge du patient qui détermine les finalités et les moyens du traitement de ses données. Il est le seul qui dispose des connaissances requises à cet effet ; en outre, c'est l'organisation de son activité professionnelle qui est en cause.

Mais ne pourrait-on pas considérer que c'est le patient qui détermine les finalités et les moyens du traitement ? Il s'agit en effet de sa santé, de sa personne. Le praticien de la santé serait le sous-traitant choisi par le patient pour fournir cette information ; il produirait de l'information pour compte de ce

---

[46] D., 95/46/CE, o.c., art. 20.1. Certains traitements sont susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées, du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, ***ou du fait de l'usage particulier d'une technologie nouvelle*** (considérant 53). Au regard de tous les traitements mis en oeuvre dans la société, le nombre de ceux présentant de tels risques particuliers devrait être très restreint (considérant 54).

[47] D., 95/46/CE, o.c., art. 20.2. Les États membres doivent prévoir, pour ces traitements, un examen préalable à leur mise en oeuvre, effectué par l'autorité de contrôle ou par le détaché à la protection des données ***en coopération avec celle-ci*** (considérant 54). Les États membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées (D., 95/46/CE, o.c., art. 20.3).

[48] D., 95/46/CE, o.c., considérant 54.

[49] Conformément à l'article 18 de la directive « Vie Privée ». Le détaché à la protection des données est chargé notamment d'assurer, d'une manière indépendante, l'application interne des dispositions nationales prises en application de la présente directive, et de tenir un registre des traitements effectués par le responsable du traitement, contenant les informations visées à l'article 21.2, et garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées (D., 95/46/CE, o.c., art. 18.2). Ce détaché peut être employé ou non du responsable du traitement (considérant 49).

dernier. Le patient serait alors le responsable du traitement de ses données ; la finalité poursuivie serait celle de la prise en charge de sa santé et les moyens seraient attachés au praticien de la santé consulté.

La consécration de cette interprétation pourrait être considérée comme une application particulièrement forte, voire extrême, de l'autodétermination informationnelle du patient.

Mais la définition du responsable du traitement par la directive « Vie Privée » offre sans doute une perspective plus en harmonie avec la relation bien comprise du praticien de la santé et de son patient. En effet, le texte pose que le responsable du traitement de données est celui qui, ***seul ou conjointement avec d'autres***, détermine les finalités et les moyens du traitement de données. Ce faisant, il s'ouvre à une approche fondée sur le respect mutuel du praticien de la santé et du patient en permettant de prendre en considération leur place respective dans la relation thérapeutique. N'est-ce pas ensemble qu'ils déterminent les finalités et les moyens du traitement ? Le cas échéant, tous deux pourraient se voir reconnaître la qualité de responsable du traitement[50].

Ceci étant, l'Etat ne pourrait-il pas non plus se voir reconnaître la qualité de responsable du traitement à raison de son intervention ou son influence toujours croissantes dans la détermination des finalités et des moyens du traitement des données du patient, et plus particulièrement à propos des données relatives à sa santé ?

[50] Pour une réponse positive à la possibilité d'avoir plusieurs responsables pour un même traitement de données à caractère personnel, voyez : [Leonard 1999].

Bibliographie

Cour européenne des droits de l'homme, arrêt du 25 février 1997, Z. c Finlande, Recueil des arrêts, 1997, I.

Cour européenne des droits de l'homme, arrêt du 27 août 1997, M.S. c Suède, Recueil des arrêts, 1997, IV.

Cour européenne de Justice, arrêt du 06 novembre 2003, Bodil Lindqvist, Journal Officiel, C-101/01.

[Boulanger et al. 1997] Boulanger, M.-H., C. de TERWANGNE, Th. LEONARD, S. LOUVEAU, D. MOREAU, Y. POULLET, 1997. La protection des données à caractère personnel en droit communautaire. *Journal des Tribunaux – Droit européen,* Bruxelles, Larcier, 1997, pp. 121-127, 145-155 et 173-179.

[Herveg 2003] HERVEG, J., Y. POULLET, 2003. A global view on the European privacy legal framework regarding processing of patient's data considering GRID-enabled medical simulation services. Initial report on legal issues related to running GRID medical services. EC Research Contract IST-2001-37153 GEMSS (GRID-enabled Medical Simulation Services).

[Leonard 1999] LEONARD, Th., Y. POULLET, 1999. La protection des données à caractère personnel en pleine (r)évolution, La loi du 11 décembre 1998 transposant la directive 95/46/CE. *Journal des Tribunaux*, Bruxelles, Larcier, 1999, p. 377, n° 6.

[Middleton 2004] Middleton, S.E., J. Herveg, F. Crazzolara, D. Marvin, Y. Poullet. GEMSS : Privacy and security for a Medical Grid. *Methods of Information in Medicine,* à paraître.

[Working Party 2002] Working Party, 2002. Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments : the example of Ipv6, 30 May 2002, WP 58, p. 3.