La théorie des risques dans les traitements de données médicales en droit européen

Herveg, Jean

Published in:
Revista de Direito Medico e da Saùde

Publication date:
2007

Document Version
le PDF de l'éditeur

LA THEORIE DES RISQUES DANS LES TRAITEMENTS DE DONNÉES MÉDICALES EN DROIT EUROPEEN

Jean Herveg
Maître de conférences aux FUNDP - Faculté de Droit – D.E.S. D.G.T.I.C.
Centre de Recherches Informatique et Droit
Avocat au barreau de Bruxelles

INTRODUCTION

1. La directive 95/46/EC 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[1] poursuit un double objectif dans son oeuvre d'harmonisation des législations des Etats membres de la Communauté européenne[2] : elle vise à permettre la libre circulation des données à caractère personnel, affirmée comme nécessaire à l'établissement et au

[1] Journal officiel des Communautés européennes, n° L 281 du 23 nov. 1995, pp. 31 –50. Pour une présentation de la directive, voyez déjà : Y. Poullet, M.-H. Boulanger, C. de Terwangne, Th. Leonard, S. Louveaux et D. Moreau, « La protection des données à caractère personnel en droit communautaire », *Journal des Tribunaux de droit européen*, Bruxelles, Ed. Larcier, 1997, p. 121 et s. (en trois parties).

[2] L'adoption de la directive se base sur l'article 95 (anciennement 100 A) de la version consolidée du traité instituant la Communauté européenne. L'article 95.3 précise que, en matière de santé, de sécurité, de protection de l'environnement et de protection des consommateurs, la Commission prend pour base un niveau de protection élevé en tenant compte notamment de toute nouvelle évolution basée sur des faits scientifiques. Elle ajoute que le Parlement européen et le Conseil doivent également s'efforcer d'atteindre cet objectif. L'article 95.8 prévoit que lorsqu'un Etat membre soulève un problème particulier de santé publique dans un domaine qui a fait préalablement l'objet de mesures d'harmonisation, il en informe la Commission, qui examine immédiatement s'il y a lieu de proposer des mesures appropriées au Conseil (voyez aussi l'article 95.10 pour l'insertion de clause de sauvegarde dans les cas appropriés pour permettre à un Etat membre de prendre des mesures provisoires soumises à une procédure communautaire de contrôle pour une ou plusieurs des raisons non économiques visées à l'article 30 du même traité – soit des raisons de moralité publique, d'ordre public, de sécurité publique, de protection de la santé et de la vie des personnes et des animaux ou de préservation des végétaux, de protection des trésors nationaux ayant une valeur artistique, historique ou archéologique ou de protection de la propriété industrielle ou commerciale –, sans que ces raisons puissent constituer un moyen de discrimination arbitraire ou un restriction déguisée dans le commerce entre les Etats membres). D'une certaine façon, ces éléments s'inscrivent déjà dans une logique de gestion des risques mais au niveau de l'adoption des normes applicables.

fonctionnement du marché commun[3], tout en assurant le respect des libertés et droits fondamentaux des personnes (physiques)[4].

Pour éliminer les obstacles à la libre circulation des données à caractère personnel au sein du marché intérieur, il est apparu fondamental que les législations nationales soient harmonisées afin que tous les Etats membres offrent un niveau équivalent – mais élevé – de protection des droits et libertés des personnes à l'égard du traitement de ces données[5]. En effet, après cette harmonisation de leur législation en la matière, les Etats membres ne pourront plus se prévaloir de raisons relatives à la protection des droits et libertés des personnes, dont le droit au respect de la vie privée, pour s'opposer à la libre circulation des données à caractère personnel[6]. Cependant, il s'en déduit que, au regard de la directive, les Etats membres peuvent restreindre la circulation des données à caractère personnel pour des raisons autres que celles relatives à la protection des libertés et droits fondamentaux des personnes[7], et ce, sans préjudice des articles 95.8 et 95.10 du traité instituant la Communauté européenne[8] ou de toute autre règle

[3] En ce sens et à ce propos, voyez déjà les considérants 3, 5, 6, 7, et 9 de la directive, sans pour autant que le principe de la libre circulation des données à caractère personnel soit réellement justifié – sauf à se contenter d'une nécessité formelle pour la constitution du marché intérieur.

[4] En ce sens, voyez déjà les considérants 2, 3, 10 et 11 de la directive.

[5] Directive précitée, considérant 8. Voyez aussi l'art. 1 de la directive et son considérant 9. Il s'en déduit aussi qu'il existe, au sein du marché intérieur, un marché des données à caractère personnel. Il demeure à s'entendre sur la signification à lui donner. Le marché des données à caractère personnel se réduit-il aux prestations et services de la société de l'information en ce qu'ils concernent les données à caractère personnel ou s'étend-il en outre à la patrimonialisation ou à la commercialisation des données en tant que telles ? En principe, l'éventuelle rémunération ne devrait refléter que l'indemnisation des frais – voire la procuration d'un incitatif raisonnable – dans le chef de la personne concernée, ainsi que le paiement du prix du traitement, mais elle ne devrait pas porter sur l'acquisition de droits sur la donnée elle-même, celle-ci étant soumise au principe de sa libre circulation. En d'autres termes, la perception d'une rémunération dans le cadre d'un traitement de données n'empêche pas que celles-ci fassent l'objet d'un autre traitement

[6] Comme l'ordre public ou les bonnes moeurs.

[7] Comme l'ordre public ou les bonnes moeurs.

[8] Au sujet des articles 95.8 et 95.10, voyez la note infra-paginale n° 2. Ce qui laisse en l'espèce une marge d'appréciation aux Etats membres lors de la transposition de la directive (en ce sens, voyez le considérant 9 de la directive),

susceptible de s'opposer à une restriction à la circulation des données au sein des Etats membres ou du marché intérieur.

2. Afin de fixer ce cadre juridique commun, mais incomplet en un sens, aux Etats membres en matière de traitements de données à caractère personnel dans la Communauté européenne, la directive a procédé à une évaluation, tant qualitative que quantitative, dans la mesure de ses compétences[9], des risques que les traitements de ces données étaient susceptibles de faire courir aux droits et libertés des personnes, et ce, à tous les niveaux de son intervention. C'est en ce sens que la directive détermine son champ d'application matériel (*cf.* chapitre I de la directive)[10] en fonction des situations qui requièrent une protection, ce qui implique d'apprécier les risques pour les droits et libertés des personnes. Par exemple, la directive ne s'applique qu'aux traitements[11] de données à caractère personnel[12],

conformément à la notion même de directive (à ce sujet, voyez l'article 249 du traité instituant la Communauté européenne).

[9] Sur le champ d'application de la directive, voyez notamment : C.J.C.E., 20 mai 2003, Rechnungshof et consorts, C-465/00, C-138/01 et C-139/01 ; C.J.C.E., 6 nov. 2003, Bodil Lindqvist, affaire C-101/01, obs. C. de TERWANGNE, « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », *Revue du droit des technologies de l'information*, Bruxelles, Ed. Bruylant, 2004, pp. 67-99.

[10] Sur le champ d'application de la directive, voyez notamment : C.J.C.E., 20 mai 2003, Rechnungshof et consorts, C-465/00, C-138/01 et C-139/01 ; C.J.C.E., 6 nov. 2003, Bodil Lindqvist, affaire C-101/01, obs. C. de TERWANGNE, « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », *Revue du droit des technologies de l'information*, Bruxelles, Ed. Bruylant, 2004, pp. 67-99.

[11] La notion de traitement de données à caractère personnel est définie à l'article 2.b de la directive (voyez aussi le considérant 14 de la directive) : c'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] La notion de données à caractère personnel est définie à l'article 2.a de la directive : c'est 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. Il est important de souligner le fait que pour être à

automatisé en tout ou en partie[13], ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier[14][15], et elle ne s'applique pas au traitement de données à caractère personnel effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques[16]. Ensuite, la directive définit les conditions générales de licéité des traitements de données à caractère personnel (*cf.* chapitre II de la directive). Elle crée des recours juridictionnels propres à la protection des données et instaure une responsabilité spécifique au responsable du traitement de données, sans omettre la question des sanctions en cas de méconnaissance de certaines règles (*cf.* chapitre III de la directive). La directive règle encore les flux de données à caractère personnel vers des pays tiers à l'Union européenne (*cf.* chapitre IV de la directive). Enfin, elle aborde la question des Codes de conduites (*cf.* chapitre V de la directive) et crée des institutions et organes spéciaux, à savoir les autorités nationales de contrôle, le Groupe de protection des personnes à l'égard du traitement des données à caractère personnel (Groupe 29) (*cf.* chapitre VI de la directive), et le Comité des Représentants des Etats membres auprès de la Commission européenne en ce qui concerne les mesures d'exécution communautaires (Comité 31) (*cf.* chapitre VII de la directive).

caractère personnel, l'information ne doit pas nécessairement révéler in se un aspect de la personnalité de la personne concernée : il faut, mais il suffit, qu'elle concerne une personne physique identifiée ou identifiable. Ceci s'explique aisément par l'objectif poursuivi par la réglementation : il s'agit de protéger les droits et libertés des individus contre les risques générés par l'utilisation d'informations qui les concernent.

[13] Voyez aussi le considérant 15 de la directive : les traitements de données à caractère personnel ne sont couverts par la directive que s'ils sont automatisés.

[14] Voyez aussi le considérant 15 de la directive : les traitements de données à caractère personnel ne sont couverts par la directive que si les données sur lesquelles ils portent sont contenues ou sont 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.

[15] Directive précitée, art. 3.1.

[16] Directive précitée, art. 3.2. Cela vise notamment la correspondance et la tenue de répertoires d'adresses (considérant 12 de la directive). Cette exclusion s'explique par l'appréciation du risque présenté par ces traitements pour les droits et libertés de la personne concernée. Voyez sur cette exclusions : C.J.C.E., 6 nov. 2003, Bodil Lindqvist, affaire C-101/01, obs. C. de TERWANGNE, précité.

3. Envisagée de manière globale, la directive développe une gestion en quatre temps des risques présentés par les traitements de données à caractère personnel. Dans un premier temps, elle pose le cadre juridique commun à tous les traitements de données à caractère personnel, en ce compris les données « sensibles »[17]. Dans un second temps, elle fixe des règles spéciales pour légitimer les traitements de données « sensibles », étant entendu que, pour le surplus, le cadre juridique commun à tous les traitements de données à caractère personnel leur est applicable. Dans un troisième temps, la directive impose des mesures complémentaires pour les traitements de données à caractère personnel qui présentent des risques particuliers pour les droits et libertés des personnes concernées. Cette troisième approche se superpose aussi aux deux précédentes ; elle n'écarte pas leur application pour le surplus du traitement. Dans un quatrième et dernier temps, la directive règle les transferts de données à caractère personnel vers des pays tiers à la Communauté européenne.

La présente contribution envisage la gestion des risques spécifiquement liés aux traitements de données médicales[18]. A cet effet, les traitements de données médicales peuvent être répartis selon qu'ils présentent des risques ordinaires ou particuliers[19].

[17] Habituellement, les données sensibles regroupent les données relatives à la santé et à la vie sexuelle, les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ainsi que l'appartenance syndicale.

[18] La notion de donnée médicale vise toute information relative à tout aspect, tant physique que psychique, de la santé, passée, actuelle et future, bonne ou mauvaise, d'une personne physique vivante ou décédée. Sur la définition des données médicales, voyez déjà : Rapport explicatif de la Convention n° 108, considérant 45 ; Rec. (97) 5 du Conseil de l'Europe relative à la protection des données médicales, art. 1 de l'annexe ; C.J.C.E., 6 nov. 2003, Bodil Lindqvist, affaire C-101/01, obs. C. de TERWANGNE, précité ; Groupe européen d'éthique des sciences et des nouvelles technologies, avis n° 13 du 30 juillet 1999 sur les aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information.

[19] Par conséquent, la présente analyse ne porte pas sur le cadre juridique commun aux traitements de « simples » données à caractère personnel (soit celles qui ne sont pas sensibles). Cela exclut par exemple d'envisager en l'espèce les voies de recours comme mode de régulation des risques. Nous ne considérerons pas non plus les transferts de données à caractère personnel en-dehors de l'Union européenne.

I. La gestion des risques ordinaires présentés par les traitements de données médicales

A. L'évaluation des risques présentés par les traitements de données médicales

4. L'évaluation des risques pour les droits et libertés des personnes concernées par les traitements de données à caractère personnel répond à un principe relativement simple : le risque ne dépend pas du contenu des données, mais du contexte dans lequel elles sont utilisées[20]. Autrement dit, le risque dépend de la finalité poursuivie par le traitement des données à caractère personnel. Par conséquent, la dangerosité – tant potentielle que réelle – d'un traitement de données pour les droits et libertés de la personne concernée s'apprécie au regard de la finalité poursuivie par le responsable du traitement de données.

5. Toutefois, cette manière d'évaluer les risques doit être nuancée pour les données dites « sensibles », ce qui inclut les données médicales. En effet, il est communément admis que le seul contenu des données « sensibles » expose déjà la personne concernée à des risques d'atteinte à ses droits et libertés, sans préjudice de la prise en considération de la finalité poursuivie par leur traitement. En d'autres mots, toute utilisation de ces données expose immanquablement la personne concernée à des risques d'atteintes à ses droits et libertés [21]. C'est en ce sens que les données « sensibles » requièrent une protection particulière en ce qu'elle doit tenir compte tant de leur contenu que de la finalité poursuivie par leur traitement.

B. L'interdiction de traiter les données médicales

6. Dans cette logique, la directive a interdit le traitement des données « sensibles » [22] pour la raison que « *les données qui sont susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée ne devraient pas faire l'objet d'un traitement (...)* » [23]. Formulée différemment, cette interdiction de traitement représente la protection particulière voulue par la directive pour les données sensibles – en ce compris les données médicales. Etant interdits, les traitements de données médicales ne sont pas susceptibles de présenter un risque pour les droits et libertés des personnes concernées. C'est en quelque sorte l'application d'une politique de réduction maximale des risques présentés par les traitements des données médicales.

C. Les exceptions à l'interdiction de traiter les données médicales

7. Après cette pétition de principe, la directive prévoit une série d'hypothèses dans lesquelles l'interdiction de traiter les données médicales ne s'applique pas. Dans ces hypothèses, la légitimité du traitement de données médicales (son caractère admissible) est présumée. En effet, ces hypothèses sont de nature à *justifier* une dérogation à l'interdiction de traiter les données médicales, sans préjudice du respect des autres règles applicables aux traitements de données à caractère personnel. Il faut insister sur le fait que ces exceptions à l'interdiction de traiter les données médicales doivent être strictement interprétées et qu'à défaut de correspondre à l'une de ces hypothèses, le traitement de données médicales est interdit.

Dans chacune de ces hypothèses, le risque présenté par le traitement de données médicales pour les droits et libertés de la personne concernée est considéré comme adéquatement maîtrisé. Il faut immédiatement dire que ces hypothèses ne reposent pas sur une absence de risque, mais bien sur une mise en balance des intérêts en présence, ce qui requiert de mesurer les

[20] Rapport explicatif de la Convention n° 108, considérant 43.
[21] En ce sens : Rapport explicatif de la Convention n° 108, considérant 43. Directive 95/46/CE, art. 8.1. 22

[22] En ce sens : Rapport explicatif de la Convention n° 108, considérant 43. Directive 95/46/CE, art. 8.1.

[23] Directive 95/46/CE, considérant 33. La Convention n°108 n'est pas aussi explicite. Elle dispose seulement en son article 6 que « *Les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. (...)* ».

risques pour les droits et libertés des personnes concernées afin de pouvoir apprécier le caractère admissible du traitement des données médicales.

Sept hypothèses permettent de lever l'interdiction de traiter les données médicales.

8. La première hypothèse qui permet de lever l'interdiction de traiter les données médicales est l'obtention du *consentement explicite* de la personne concernée à cet effet[24]. La directive prend ainsi le parti de confier à la personne concernée le pouvoir d'autoriser le traitement de ses données médicales[25]. A cet effet, il appartient à la personne concernée de mettre en balance les intérêts en présence et de prendre attitude en conséquence. Dans cette mesure, la personne concernée apprécie elle-même le risque présenté par le traitement de ses données médicales pour ses droits et libertés[26]. Autrement dit, la directive considère que les risques pour les droits et libertés de la personne concernée sont présumés maîtrisés dès lors que celle-ci a valablement consenti au traitement de ses données médicales.

Cette attribution de pouvoir à la personne concernée représente incontestablement une expression forte de son autodétermination informationnelle – sa maîtrise sur l'information qui la concerne – [27]. Elle

[24] Directive 95/46/EC précitée, art. 8.2.a.
Directive 95/46/CE, considérant 33. La directive ne donne pas d'indication formelle pour savoir s'il faut accorder un statut privilégié à cette base de légitimité pour le traitement des données « sensibles ».

[25] Directive 95/46/EC précitée, art. 8.2.a.
Directive 95/46/CE, considérant 33. La directive ne donne pas d'indication formelle pour savoir s'il faut accorder un statut privilégié à cette base de légitimité pour le traitement des données « sensibles ».

[26] Ce qui pose bien entendu la question de savoir qui prend en compte les intérêts des tiers et de la collectivité : le responsable du traitement, la personne concernée ou personne ? Voyez *infra* à ce sujet.

[27] Brièvement sur l'autodétermination informationnelle : Fr. RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Paris, Bruylant, L.G.D.J., 1990, p. 588-589, n° 532 : « (...) *La juridiction constitutionnelle a déduit du droit de la personnalité l'un de ses attributs, à savoir : « le pouvoir reconnu à l'individu et résultant*

peut aussi étonner; la personne concernée est-elle toujours en mesure de prendre une décision quand il s'agit de ses données médicales ? N'est-il pas dangereux de s'en remettre à l'individu alors qu'il représente le plus souvent la partie « faible » ou à tout le moins en position de « demande », dans le cadre du traitement de ses données médicales ? Par exemple, est-il possible pour un patient de refuser le traitement de ses données médicales à des fins scientifiques par le médecin qui le soigne? Comment s'assurer de la validité de son consentement pour qu'il ne se réduise pas à une pantalonnade? C'est pour tous ces motifs et afin de limiter les risques pour ses droits et libertés, que le consentement de la personne concernée doit répondre à un certain nombre d'exigences imposés par la directive.

9. Le consentement de la personne concernée s'entend de « *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* » [28]. D'abord, le consentement doit être indubitable. Ensuite, pour être libre, le consentement doit être exempt de tout vice, de toute contrainte ou pression[29]. En outre, le consentement doit être spécifique et informé. Le caractère spécifique rappelle avec insistance que la personne concernée doit savoir exactement ce à quoi elle acquiesce, ce qui implique d'ailleurs nécessairement une information préalable adéquate. A défaut d'une information préalable et suffisante, le consentement de la personne concernée ne pourra pas être

de la notion d'auto-détermination, de décider en premier lieu lui-même quand et dans quelle mesure des faits relatifs à sa propre existence sont divulgués (...) Cet attribut du droit de la personnalité est appelé « droit à la maîtrise des données personnelles » (...) Il n'est toutefois pas sans limite. (...) ». Voyez aussi : Conseil de l'Europe, Résolution 1165 (1998) du 26 juin 1998, *Droit au respect de la vie privée* (24e séance), point 5.

[28] Directive 95/46/EC précitée, art. 2, h)

[29] A cet égard, le fait que la personne concernée puisse tirer un profit direct [par exemple, pour l'amélioration de son état de santé] ou indirect [par exemple, en participant au progrès de la science] du traitement de ses données médicales, ne vicie pas nécessairement son consentement. La perception d'une rémunération – au-delà de la simple couverture des frais éventuels – invaliderait-elle le consentement ? Une réponse négative de principe ne semble pas devoir être adoptée. Tout dépend du cas d'espèce et de la manière dont le droit applicable a entendu protéger la personne concernée.

spécifique ; il ne sera donc de toute façon pas valable. Toute la question réside alors dans le degré de précision de cette information dont le minimum est décrit aux articles 10 et 11 de la directive. Elle doit à tout le moins permettre la mise en oeuvre de tous les aspects du traitement de données – qualité des données, droits de la personne concernée, mesures de sécurité et de confidentialité, notification à l'autorité de contrôle, etc. –. Il est cependant certain que l'information doit être d'autant plus précise et complète que le traitement porte sur des données sensibles comme les données médicales. En tout état de cause, la technique du blanc-seing est proscrite. Les exigences de spécificité du consentement et de son information préalable renforcent cette proscription. Les traitements ultérieurs incompatibles avec la finalité pour laquelle les données ont été collectées, sont de même interdits (art. 6, 1.b). Il faut rappeler que le consentement peut être donné à l'avance, c'est-à-dire indépendamment du moment où les données sont collectées. Enfin, le consentement de la personne concernée au traitement de ses données médicales doit être explicite[30]. *A contrario*, le caractère explicite devrait exclure le recours au consentement implicite – quelle que puisse être la difficulté à définir cette notion –. A ce sujet, au-delà du caractère indubitable du consentement, son caractère explicite suppose qu'il s'exprime. Souvent, l'écrit signé qui le consigne en constitue la meilleure trace. Plusieurs législations européennes ont d'ailleurs ainsi traduit cette exigence. Cependant, d'autres actes de la personne concernée sont de nature à lui conférer cette caractéristique notamment au regard du contexte dans lequel ils sont posés. En effet, le consentement explicite peut s'exprimer au travers d'actions positives comme la participation à des recherches contre la maladie dont la personne concernée est atteinte, ou comme la demande d'être traité dans un service médical connu notoirement pour être un lieu de recherche. La directive précise enfin que la législation d'un Etat membre peut prévoir que l'interdiction ne peut pas être levée dans certaines hypothèses par le seul consentement de la personne concernée [31].

[30] Voyez : Directive 95/46/EC précitée, art. 8.2, a) et le considérant 33.
[31] Directive 95/46/EC précitée, art. 8.2, a)

10. Lorsque toutes ces conditions sont remplies, le consentement de la personne concernée permet de présumer la légitimité du traitement de ses données médicales. On présume qu'elle a effectué la balance des intérêts en présence et qu'elle a agi en conséquence. Si elle ne l'a pas fait et que les intérêts en présence ne sont pas respectés, son consentement ne pourra pas fonder le traitement de ses données médicales ; il ne sera pas légitime de ce chef. En d'autres mots, le consentement de la personne concernée ne dispense pas le responsable du traitement de données de poursuivre un intérêt légitime [ce qui suppose la mise en balance des intérêts en présence], et le consentement de la personne concernée ne permet pas de couvrir le caractère illégitime de l'intérêt poursuivi par le responsable du traitement.

11. Ceci étant, la directive ne donne pas d'indication formelle quant à la nature du consentement donné par la personne concernée. De même, la question de savoir s'il y a formation d'un contrat doit être résolue au regard de la manière dont le droit applicable envisage d'une part la relation entre la personne concernée et le responsable du traitement de données et, d'autre part, la relation entre la personne concernée et l'information qui la concerne, ceci sans préjudice des particularités auxquelles serait obligatoirement soumis ce contrat par exemple en termes de qualité des données, de droits de la personne concernée, du niveau de la sécurité et de la confidentialité du traitement de données, d'obligation de notification à l'autorité de contrôle, etc. Il appartient aussi au droit applicable de déterminer le seuil de la capacité juridique en ce qui concerne les personnes mineures ou incapable.

12. Le consentement régulièrement octroyé est-il irrévocable ? Non, la personne concernée peut toujours retirer son consentement au traitement de ses données médicales, sans avoir à se justifier. Les conséquences de ce retrait sont controversées. Signifie-t-il simplement que, désormais, de nouveaux traitements ne pourront pas être possibles (sans toutefois remettre en cause ceux déjà mis en place sous l'empire du consentement), ou faut-il considérer en outre que les traitements de données effectués sur base du consentement initial ne peuvent plus être poursuivis? Dès lors que le consentement initial a été révoqué, la seconde hypothèse s'impose

logiquement puisque le traitement de données initial n'a plus de base de légitimité. Mais ce n'est pas pour autant que les opérations passées deviennent illégitimes. Elles ne peuvent simplement plus être poursuivies, sauf à pouvoir se prévaloir d'une autre source de légitimité.

13. Au regard de ces développements, il n'est pas sûr que le seul consentement explicite de la personne concernée représente le fondement le plus solide des traitements de ses données médicales, et ce, tant pour la personne concernée que pour le responsable du traitement, même s'il est régulièrement présenté comme la première base de légitimité pour le traitement des données médicales. Heureusement, la directive prévoit d'autres hypothèses dans lesquelles l'interdiction de traiter les données médicales peut être levée. Dans ces hypothèses, la finalité poursuivie permet aussi de présumer que le risque représenté par le traitement des données médicales pour les droits et libertés de la personne concernée est correctement maîtrisé par une mise en balance formelle des intérêts en présence.

14. C'est ainsi que l'interdiction de traiter les données médicales peut être levée lorsque « *le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates* » [32].

Il faut insister sur le fait que le traitement de données médicales doit être nécessaire à cette finalité, et pas seulement utile. Le responsable du traitement doit par conséquent pouvoir établir la nécessité de procéder à ce traitement pour respecter ses droits et obligations spécifiques en matière de droit du travail. Le traitement de données doit en outre être autorisé par une législation nationale qui doit prévoir des garanties adéquates pour la protection des données, sans que celles-ci ne soient autrement définies.

[32] Directive 95/46/EC précitée, art. 8.2.b. Cette finalité semble inclure la médecine du travail.

15. La troisième hypothèse dans laquelle le traitement des données médicales peut être légitime est celle où « *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 trouve dans l'incapacité physique ou juridique de donner son consentement* » [33].

La notion d'intérêt vital vise expressément et exclusivement la situation de péril imminent à la vie d'une personne physique, qu'il s'agisse de la personne concernée ou de toute autre personne physique. Cependant, dans ce dernier cas, la directive précise que la personne concernée doit être dans l'incapacité physique ou juridique de consentir au traitement de ses données médicales au profit de cette autre personne. Il ne peut pas en être déduit que la personne concernée, capable physique et juridiquement de consentir, pourrait, sans autre forme de procès, refuser d'autoriser le traitement de ses données médicales lorsque les intérêts vitaux d'une autre personne sont en jeu. Il conviendrait alors d'examiner la qualification à donner à ce comportement au regard du droit applicable.

16. Dans une quatrième hypothèse, le traitement de données médicales peut être légitime si « *le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées* » [34].

[33] Directive 95/46/EC précitée, art. 8.2.c.
[34] Directive 95/46/EC précitée, art. 8.2. d)
Directive 95/46/EC précitée, considérant 33, 35

Pour pouvoir se prévaloir de cette autorisation de traiter les données médicales, l'organisme doit poursuivre un but non lucratif et avoir un objet social qui concerne l'exercice de libertés fondamentales [35].

17. L'interdiction de traiter des données médicales est encore levée dans une cinquième hypothèse lorsque « *le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice* » [36].

Il faut insister sur le fait que, même manifestement rendues publiques, le traitement de ces données tombe toujours dans le champ d'application de la directive et que toutes les autres règles applicables à leur traitement doivent être scrupuleusement respectées.

18. La directive lève l'interdiction de traiter des données médicales dans une sixième hypothèse « *lorsque 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* » [37].

L'hypothèse vise la finalité thérapeutique entendue largement[38], en ce compris la gestion de services de santé, ce qui devrait englober les finalités

[35] Directive 95/46/EC précitée, art. 8.2, d)
Directive 95/46/EC précitée, considérant 33, 35

[36] Directive 95/46/EC précitée, art. 8.2, e)
[37] Directive 95/46/EC précitée, art. 8.3.
Quoique la directive semble ne viser que certaines fins relatives à la santé. Voyez à ce sujet la formulation du considérant 33, 38

[38] Directive 95/46/EC précitée, art. 8.3.

accessoires nécessaires pour assurer l'octroi de soins de santé, telles que la réception des patients, le secrétariat médical, les services informatiques, etc.

Par contre, cette hypothèse ne comprend pas les finalités de sécurité de sociale ou de santé publique, puisqu'elles sont reprises dans les exceptions pour motifs d'intérêt public important (cf. *infra*, n° 19).

En outre, le traitement des données médicales doit être effectué par un praticien de la santé, sans que cette notion ne soit autrement définie. Ce dernier doit être soumis par le droit national, ou par des règles adoptées par les autorités nationales compétentes, au secret professionnel.

A défaut d'être effectué par un praticien de la santé, le traitement peut être effectué par une autre personne si elle est soumise à une obligation de secret équivalente, notamment par voie statutaire ou par stipulation contractuelle.

On pourrait se demander si, dans cette dernière hypothèse, le consentement de la personne concernée n'a pas été confondu avec le consentement aux soins prodigués ?

19. Enfin, la directive permet aux Etats membres de prévoir d'autres hypothèses dans lesquelles les données médicales peuvent être traitées, à condition de pouvoir se prévaloir d'un motif d'intérêt public important [39], ce qui suppose la démonstration effective de son existence dans chaque cas d'espèce par l'Etat membre.

La directive visait principalement des motifs d'intérêt public important en matière de santé publique et de protection sociale « *particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le*

Quoique la directive semble ne viser que certaines fins relatives à la santé. Voyez à ce sujet la formulation du considérant 33, 38

[39] Directive 95/46/EC précitée, art. 8.4.

régime d'assurance maladie »[40]. Elle visait aussi la recherche scientifique et les statistiques publiques[41].

Les cas où les données médicales peuvent ainsi être traitées doivent être prévus soit par la législation nationale, soit par une décision de l'autorité nationale de contrôle.

Mais, dans ces hypothèses, les Etats membres ne peuvent autoriser le traitement de données médicales que sous la réserve de prévoir des garanties appropriés pour protéger les droits fondamentaux et la vie privée de la personne concernée[42]. La directive ne précise cependant pas ces garanties.

En tout état de cause, les Etats membres doivent notifier à la Commission européenne les dérogations à l'interdiction de traiter les données médicales prises sur cette base[43].

D. Le contrôle concret de la légitimité du traitement de données médicales

20. Il ne suffit pas de se prévaloir d'une de ces exceptions à l'interdiction de traiter les données médicales pour que le traitement de données soit légitime, même dans le cas du consentement de la personne concernée. Il ne s'agit en effet que d'hypothèses où la légitimité du traitement est présumée. La légitimité du traitement de données médicales – la mise en balance des intérêts en présence – doit en outre et surtout être vérifiée concrètement. Cette appréciation doit être menée avant sa mise en oeuvre et même après à intervalles réguliers en fonction des circonstances. En effet, la directive ne

[40] Directive 95/46/EC précitée, considérant 34.
[41] Directive 95/46/EC précitée, considérant 34.
Directive 95/46/EC précitée, considérant 34.

[42] Directive 95/46/EC précitée, considérant 34.
Directive 95/46/EC précitée, considérant 34.

[43] Directive 95/46/EC précitée, art. 8.6.

se contente pas d'une approche *a priori* et formelle de l'appréciation des risques pour les droits et libertés des personnes ; ceux-ci doivent être appréciés *in concreto*. Ce constat vaut *a fortiori* lors du traitement de leurs données médicales.

Pour apprécier concrètement la légitimité du traitement de données, il faut d'abord identifier les intérêts en présence. S'agit-il seulement des seuls intérêts du responsable du traitement et de la personne concernée ou faut-il tenir compte en outre des tiers éventuellement concernés et des intérêts de la collectivité ? A notre sens, ces deux dernières catégories d'intérêts doivent être prises en considération pour apprécier la légitimité du traitement de données.

Ensuite, si le consentement valable et explicite de la personne concernée présume, jusqu'à preuve du contraire, l'existence d'un équilibre acceptable entre les intérêts en présence dans le traitement de ses données médicales, il paraît cependant difficile d'en déduire *de facto* la prise en considération adéquate des autres intérêts que ceux de la personne concernée. En tout état de cause, si l'équilibre entre tous les différents intérêts en présence n'a pas été respecté, le traitement des données médicales sera illégitime, nonobstant le consentement régulier de la personne concernée. Par contre, en présence d'une autre base de légitimité, obtenir en plus le consentement de la personne concernée est de nature à renforcer la légitimité du traitement de ses données médicales. C'est la raison pour laquelle il faut approuver et recommander fermement la pratique éthique qui consiste à agir en ce sens. Cette pratique se rencontre fréquemment dans le cadre des essais cliniques et dans le cadre de la constitution de réseaux télématiques dans le secteur des soins de santé.

Enfin, le responsable du traitement ne peut pas fonder le traitement de données médicales sur d'autre base que celles énumérées ci-avant. Ceci exclut nécessairement le recours aux hypothèses de légitimation formelle énumérées à l'article 7 de la directive 95/46/EC pour les « simples » données à caractère personnel. Ainsi, par exemple, le responsable du

traitement ne peut pas justifier le traitement de données médicales en effectuant une mise en balance des intérêts en présence, sans répondre à une hypothèse de légitimation du traitement de données médicales.

E. Les numéros nationaux d'identification et les autres identifiants à portée générale

21. Les États membres doivent déterminer les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement de données[44]. En principe, la sensibilité des identifiants ne provient pas de leur contenu mais bien des finalités de leurs utilisations potentielles ou réelles. La question de l'identification du patient et des professionnels des soins de santé est délicate, surtout à raison des risques pour les personnes concernées. Elle doit néanmoins être résolue dans le cadre des projets de réseaux télématiques dans le secteur des soins de santé. A cet égard, le recours à des identifiants contextuels (spécifiques aux finalités poursuivies) représente une piste de réflexion intéressante.

II. La gestion des risques particuliers présentés par les traitements de données médicales

22. Si la directive pose un cadre juridique commun aux traitements des données à caractère personnel et fixe des règles spéciales pour légitimer le traitement des données « sensibles », elle envisage en outre l'hypothèse dans laquelle, nonobstant le respect de cette double protection, certains traitements de données à caractère personnel sont quand même susceptibles de présenter des risques *particuliers* au regard des droits et libertés des personnes concernées [45].

23. La directive précise en 1995 que, au regard de tous les traitements mis en oeuvre dans la société, le nombre de ceux présentant de tels risques

[44] Directive 95/46/EC précitée, art. 8.7.
[45] Directive 95/46/EC précitée, considérant 53.
Directive 95/46/EC précitée, considérant 54.

particuliers devrait être très restreint[46]. Dix ans après l'adoption de la directive et vu l'évolution des nouvelles technologies de l'information et de la communication, il n'est pas sûr que cette affirmation puisse être maintenue, surtout dans le secteur des soins de santé. Bien au contraire, aujourd'hui, le nombre de traitements présentant des risques particuliers pour les droits et libertés des personnes ne serait-il pas plutôt très élevé, notamment en ce qui concerne les données médicales ? Ainsi, depuis 1995, les évolutions technologiques ont permis la mise en place de larges réseaux télématiques dans le secteur des soins de santé pris au sens large, ces réseaux reliant des bases de données médicales substantielles sur une grande échelle [47], sans omettre le développement de bases de données génétiques également insérées dans des réseaux télématiques nationaux, européens voire, de plus en plus fréquemment, mondiaux. Tous ces développements n'ont-ils pas ouvert la porte à un nombre inouï de traitements présentant des risques particuliers pour les droits et libertés des personnes concernées ?

24. Aux dires de la directive, ces risques *particuliers* sont ceux qui résultent de la nature même du traitement poursuivi, de sa portée ou de ses finalités [48]. Elle donne pour exemple des finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat. Ces risques particuliers peuvent aussi résulter de l'usage particulier d'une technologie nouvelle [49].

Traditionnellement, les exemples de traitements de données à caractère personnel présentant des risques particuliers sont ceux mis en oeuvre par une autorité publique et portant sur l'ensemble ou une grande partie de la population [50]u des traitements portant sur des données médicales[51]. Les

[46] Directive 95/46/EC précitée, considérant 53.
Directive 95/46/EC précitée, considérant 54.

[47] Le cas du réseau mis en place par l'EORTC ne manque pas d'interpeller, ainsi que ceux mis en place par les grandes firmes pharmaceutiques de par le monde.
[48] Directive 95/46/EC précitée, considérant 53.
[49] Directive 95/46/EC précitée, considérant 53
[50] Comme les recensements de la population.

bases de données génétiques et les réseaux télématiques dans le secteur des soins de santé représentent autant de traitements de données susceptibles de poser des risques particuliers pour les droits et libertés des personnes concernées. Il faut déjà être attentif à la personne du responsable du traitement[52], à la sensibilité des données traitées, aux finalités poursuivies [53], à l'ampleur du traitement de données médicales, aux catégories de personnes concernées[54] et au respect des droits de ces dernières[55], sans oublier la question des flux transfrontières de données. En bref, il faut être attentif à tout ce qui serait de nature à créer des risques particuliers aux droits et libertés des personnes concernées, sans pour autant faire basculer tous les traitements de données « sensibles » sous cette protection particulière complémentaire, et sans exclure *a priori* les traitements des « simples » données à caractère personnel, dès lors qu'ils sont aussi susceptibles de présenter des risques particuliers pour les droits et libertés des personnes concernées[56].

Au regard du développement des réseaux télématiques dans le secteur des soins de santé, les risques particuliers sont surtout liés au fait que maintenant, les données médicales sont l'objet de plusieurs finalités, ce qui pose déjà la question de la possibilité de traiter des données médicales pour des finalités multiples, mais aussi la question de la détermination préalable, précise et concrète de ces finalités, sans omettre la question des traitements ultérieurs « éventuels ». En effet, nous constatons aujourd'hui une tendance

[51] M.-H. BOULANGER, C. de TERWANGNE, Th. LEONARD, S. LOUVEAUX, D. MOREAU et Y. POULLET, o.c., *Journal des Tribunaux de Droit Européen*, 1997, p. 152, n° 62. Ces exemples sont repris par : D. DE BOT, *Verwerking van persoongegevens*, Kluwer, 2001, p. 294, n° 406.

[52] Par exemples, l'employeur traitant des données médicales ou génétiques, une société commerciale traitant des données génétiques.

[53] Exclure les personnes concernées de certaines prestations ou de certains services, établir des profils individuels, collectifs ou semi-collectifs, les modes de financement des soins de santé. Nous pouvons également penser à la poursuite de finalités liées incompatibles entre elles (santé et commerce, par exemple).

[54] Les mineurs, les personnes fragilisées, etc.

[55] Le droit d'information, d'accès, de rectification, et d'opposition de la personne concernée.

[56] Par exemple, les « listes noires » en matière d'assurances, de location d'immeubles, etc.

forte à ne plus définir de manière préalable et précise les finalités des traitements de données médicales, mais plutôt à organiser un système d'information en combinaison avec un système technique de sécurisation et dont les finalités seront contrôlées *a posteriori*. Autrement dit, on assiste à la création de systèmes d'information à deux niveaux : d'abord, on crée l'infrastructure du système d'information (comme les infrastructures de télécommunications *mutatis mutandis*) – ce qui comprend parfois la collecte et le traitement de données dans un ensemble virtuel –, et ensuite, on définit les finalités (secondes) du traitement de données en oubliant que ces finalités reposent sur un traitement initial – la création du système d'information –. En effet, ce faisant, la mise en place du système d'information ne semble plus être constitutive de risque pour les droits et libertés des personnes concernées alors qu'en réalité, elle est l'origine fondamentale du risque ; elle constitue le premier traitement de données. Or, il faut évaluer tant le premier risque (la création du réseau) que les risques liés aux finalités (secondes) des traitements de données.

A cet égard, si le niveau de sécurité assuré contribue assurément à apprécier le risque encouru par le traitement de données, il n'est cependant pas exclusif de la prise en considération des autres critères pour apprécier la légitimité du traitement de données – qu'il soit au premier ou au second degré – surtout s'il s'agit de données sensibles comme les données médicales.

Ces systèmes d'information à étages et à finalités multiples posent d'ailleurs des problèmes au regard de l'exigence de la loyauté du traitement de données, dès lors que celle-ci renvoie à la nécessité de respecter les finalités (précises et concrètes) annoncées ainsi qu'à l'obligation d'informer la personne concernée. En effet, les multiples ramifications du système d'information ne sont pas transparentes, tant au niveau technique qu'au niveau des finalités, d'autant plus qu'elles sont évolutives (c'est la question de la boîte noire).

Cependant, les technologies de la communication et de l'information sont susceptibles de fournir des réponses à ces interrogations.

25. La maîtrise de ces risques particuliers impose que les Etats membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et qu'ils veillent à ce que ces traitements soient examinés avant leur mise en oeuvre[57]. Il ne faut pas s'y méprendre ; la directive impose bien l'obligation[58] aux Etats membres d'identifier ces traitements particuliers et de veiller à leur examen avant leur mise en oeuvre.

Pour rappel, le fait que les données médicales font déjà l'objet d'une protection particulière à raison de leur caractère sensible, ne les soustrait pas à la prise en compte de risques particuliers. Autrement dit, le traitement de données médicales qui présente des risques particuliers pour les droits et libertés des personnes concernées doit en outre faire l'objet d'un examen préalable.

26. L'examen préalable de ces traitements présentant des risques particuliers peut se dérouler de quatre façons.

Premièrement, il peut être réalisé par l'autorité de contrôle après la réception de la notification du traitement de données par le responsable du traitement[59]. 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 [60].

[57] Directive 95/46/EC précitée, art. 20.1. Voyez cependant la formulation du considérant 53.
En ce sens : M.-H. BOULANGER, C. de TERWANGNE, Th. LEONARD, S. LOUVEAUX, D.
[58] MOREAU et Y. POULLET, o.c., *Journal des Tribunaux de Droit Européen*, 1997, p. 152, n° 62.
[59] Directive 95/46/EC précitée, art. 20.2.
[60] Directive 95/46/EC précitée, considérant 54.

Deuxièmement, l'examen préalable peut être l'oeuvre du détaché à la protection des données[61] qui, en cas de doute, doit consulter l'autorité de contrôle[62]. A cet égard, la directive précise que celui-ci procède en coopération avec cette dernière [63].

Troisièmement, la directive prévoit que les Etats membres peuvent procéder à cet examen dans le cadre de l'élaboration d'une mesure du Parlement national qui définisse la nature du traitement et fixe des garanties appropriées [64].

Enfin, quatrièmement, les Etats membres peuvent aussi procéder à cet examen dans le cadre de l'élaboration d'une mesure fondée sur une telle mesure législative qui aussi définisse la nature du traitement et fixe des garanties appropriées [65].

Conclusions

27. La directive 95/46/EC 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 gère en quatre temps les risques présentés par les traitements de données à caractère personnel. Dans un premier temps, elle

Le détaché à la protection des données à caractère personnel est une personne désignée par le responsable du traitement, conformément au droit national auquel ce dernier est soumis, et qui est chargée notamment
[61] - d'assurer, d'une manière indépendante, l'application interne des dispositions nationales prises en application de la présente directive,
- 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 faux droits et libertés des personnes concernées (art. 18.2 de la directive).
La présence d'un détaché à la protection des données permet aux Etats membres de prévoir des simplifications ou des dérogations à l'obligation de notifier les traitements de données à caractère personnel à l'autorité de contrôle (art. 18.2 de la directive).

[62] Directive 95/46/EC précitée, art. 20.2
[63] Directive 95/46/EC précitée, considérant 54.
[64] Directive 95/46/EC précitée, art. 20.3
[65] Directive 95/46/EC précitée, art. 20.3.

pose le cadre juridique commun à tous les traitements de données à caractère personnel, en ce compris les données « sensibles ». Dans un second temps, elle fixe des règles spéciales pour légitimer les traitements de données « sensibles », étant entendu que, pour le surplus, le cadre juridique commun à tous les traitements de données à caractère personnel leur est applicable. Dans un troisième temps, la directive impose des mesures complémentaires pour les traitements de données à caractère personnel qui présentent des risques particuliers pour les droits et libertés des personnes concernées. Cette troisième approche se superpose aussi aux deux précédentes; elle n'écarte pas leur application pour le surplus du traitement. Dans un quatrième et dernier temps, la directive règle les transferts de données à caractère personnel vers des pays tiers à la Communauté européenne.

Dans ce contexte, les traitements de données médicales présentent des risques ordinaires et particuliers pour les droits et libertés des personnes concernées. S'agissant de la gestion des risques ordinaires présentés par les traitements de données médicales, l'interdiction de traiter les données médicales s'accommode d'une série d'exceptions. A cet égard, le consentement de la personne concernée consolide la légitimité du traitement de ses données médicales lorsqu'il accompagne une autre base de légitimation. Seul, le consentement de la personne concernée semble trop précaire pour assurer une maîtrise efficace des risques présentés par les traitements de données médicales, tant pour la personne concernée que pour le responsable du traitement. S'agissant de la gestion des risques particuliers présentés par les traitements de données médicales, la création de réseaux télématiques de grande ampleur doit interpeller tous les acteurs des soins de santé (en ce compris les patients) et susciter leur plus grande vigilance pour éviter les atteintes aux droits et libertés des personnes concernées tout en permettant le progrès des soins de santé pour tout le monde, sans discrimination.

CHOIX DE REFERENCES

§ 1. UNION EUROPEENNE

A. INSTRUMENTS JURIDIQUES

1. Traité instituant la Communauté européenne (cf. art. 152).
2. Charte des droits fondamentaux de l'Union européenne (cf. art. 7 & 8).
3. Règlement n° 1408/71 du Conseil du 14 juin 1971 relatif à l'application des régimes de sécurité sociale aux travailleurs salariés, aux travailleurs non salariés et aux membres de leur famille qui se déplacent à l'intérieur de la Communauté.
4. Recommandation 81/679/CEE de la Commission du 29 juill. 1981, concernant une convention du Conseil de l'Europe relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *J.O.C.E.*, n° L 246 du 29 août 1981, p. 31.
5. Résolution du Conseil et des Représentants des gouvernements des Etats membres, réunis au sein du Conseil, du 29 mai 1986, concernant l'adoption d'une carte sanitaire européenne d'urgence, *J.O.C.E.*, n° C 184, du 23 juill. 1986, pp. 4-7.
6. 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.
7. Décision 2001/497/CE de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE.
8. Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 déc. 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, *J.O.C.E.*, n° L 008 du 12 janv. 2001, pp. 1-22.
9. Décision 2002/16/CE de la Commission du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans pays tiers en vertu de la directive 95/46/CE.

10. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).
11. COM(2002) 667 final, Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des régions, « eEurope 2002 : Critères de qualité applicables au sites web consacrés à la santé », 29 nov. 2002, 20 p.
12. COM(2003) 265 final, Premier rapport de la Commission sur la mise en oeuvre de la directive relative à la protection des données (95/46/CE).
13. COM(2003) 73 final, Communication de la Commission relative à l'introduction de la carte européenne d'assurance maladie, 17 févr. 2003, 36 p.
14. COM(2004) 356 final, Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des régions, « Santé en ligne – améliorer les soins de santé pour les citoyens européens : plan d'action pour un espace européen de la santé en ligne », 30 avril 2004, 30 p.
15. Décision 2004/915/CE de la Commission du 27 décembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers.

B. Jurisprudence de la Cour de Justice de l'Union Européenne

1. C.J.C.E, arrêt du 20 mai 2003, Rechnungshof et consorts c. Autriche, affaires jointes C-465/00, C-138/01 et C-139/01, *Rec. Jur.*, 2003, p. I-04989.
2. C.J.C.E, arrêt du 6 nov. 2003, Bodil Lindqvist, affaire C-101/01, obs. C. de TERWANGNE, « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », *Revue du droit des technologies de l'information*, Bruxelles, Ed. Bruylant, 2004, pp. 67-99.

§ 2. Conseil de l'Europe

A. Instruments juridiques

1. Convention de sauvegarde des droits de l'homme et des libertés fondamentales, du 4 nov. 1950, *Série des Traités européens*, n° 5.
2. Résolution (1970) 428 du 23 janv. 1970 de l'Assemblée consultative du Conseil de l'Europe portant déclaration sur les moyens de communication de masse et les droits de l'homme.
3. Convention du 28 janv. 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des Traités européens, n° 108.
4. Recommandation n° R (83) 10 du 23 sept. 1983 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques.
5. Recommandation (1984) 979 du 22 mars 1984 de l'Assemblée parlementaire du Conseil de l'Europe relative à l'avenir des structures de santé.
6. Recommandation n° R (86) 1 du 23 janv. 1986 du Comité des Ministres aux Etats membres relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale.
7. Recommandation n° R (89) 4 du 6 mars 1989 du Comité des Ministres aux Etats membres sur la collecte de données épidémiologiques sur les soins de santé primaires.
8. Recommandation n° R (90) 8 du 30 mars 1990 du Comité des Ministres aux Etats membres relative à l'impact des nouvelles technologies sur les services de santé, particulièrement sur les soins de santé primaires.

9. Convention du 4 avril 1997 pour la protection des droits de l'homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine : Convention sur les droits de l'homme et la biomédecine, *Série des Traités européens*, n° 164.
10. Recommandation n° R (97) 5 du 13 févr. 1997 du Comité des Ministres aux Etats membres relative à la protection des données médicales.
11. Recommandation n° R (97) 18 du 30 sept. 1997 du Comité des Ministres aux Etats membres concernant la protection des données à caractère personnel, collectées et traitées à des fins statistiques.
12. Résolution (1998) 1165 du 26 juin 1998 de l'Assemblée parlementaire du Conseil de l'Europe, Droit au respect de la vie privée.
13. Recommandation n° R (2000) 5 du 24 févr. 2000 du Comité des Ministres aux Etats membres sur le développement de structures permettant la participation des citoyens et des patients au processus décisionnel concernant les soins de santé.
14. Recommandation Rec (2001) 13 du 10 oct. 2001 du Comité des Ministres aux Etats membres sur le développement d'une méthodologie dans l'élaboration de lignes directrices pour de meilleures pratiques médicales.
15. Recommandation Rec (2002) 9 du 18 sept. 2002 du Comité des Ministres aux Etats membres sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance.
16. Protocole additionnel du 24 janv. 2002 à la Convention sur les droits de l'homme et la biomédecine relatif à la transplantation d'organes et de tissus d'origine humain, *Série des Traités européens*, n° 186.
17. Recommandation (2003) 1626 du 1er oct. 2003 de l'Assemblée parlement du Conseil de l'Europe, La réforme des systèmes de santé en Europe : concilier équité, qualité et efficacité.
18. Recommandation Rec (2004) 17 du 15 déc. 2004 du Comité des Ministres aux Etats membres relative à l'impact des technologies de l'information sur les soins de santé – Le patient et Internet.
19. Résolution (2005) 1469 du 7 oct. 2005 de l'Assemblée parlementaire du Conseil de l'Europe, Accès aux soins et problèmes linguistiques dans la région de Bruxelles-Capitale en Belgique.

B. Jurisprudence de la Cour Européenne des Droits de l'Homme

1. Comm. Eur. D.H., décision du 20 mai 1998, requête n° 30039/96, Willy Brandt c. Suisse.
2. C.E.D.H., arrêt du 25 févr. 1997, affaire Z. c. Finlande.
3. C.E.D.H., arrêt du 27 août 1997, affaire M.S. c. Suède.

§ 3. Groupe européen d'éthique des sciences et des nouvelles technologies auprès de la Commission européenne

1. Avis n° 13 du 30 juillet 1999, « Aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information ».

§ 4. Unesco

1. Recommandation du 20 nov. 1974 concernant la condition des chercheurs scientifiques.
2. Recommandation du 27 nov. 1978 concernant la normalisation internationale des statistiques relatives à la science et à la technologie.
3. Déclaration universelle du 11 nov. 1997 sur le génome humain et les droits de l'homme.
4. Déclaration du 12 nov. 1997 sur les responsabilités des générations présentes envers les générations futures.
5. Charte du 15 oct. 2003 sur la conservation du patrimoine numérique.
6. Recommandation du 15 oct. 2003 sur la promotion et l'usage du multilinguisme et l'accès universel au cyberespace.
7. Déclaration internationale du 16 oct. 2003 sur les données génétiques humaines.
8. Déclaration universelle du 19 oct. 2005 sur la bioéthique et les droits de l'homme.

§ 5. OCDE

1. « Les technologies du XXIe siècle. Promesses et périls d'un futur dynamique », O.C.D.E., *Science et Technologies de l'Information*, 1998, vol. 1998, n° 7, 194 p.
2. « Perspective de la science, de la technologie et de l'industrie », O.C.D.E., *Science et Technologies de l'Information*, 1998, vol. 1998, n° 8, 321 p.
3. « Les incidences économiques et sociales du commerce électronique, Résultats préliminaires et programme de recherche », O.C.D.E., *Science et Technologies de l'Information*, 1999, vol. 1999, n° 1, 186 p.
4. « OECD Proceedings Xenotransplantation : Internation Policy Issues », O.C.D.E., *Science et Technologies de l'Information*, 1999, vol. 1999, n° 3, 108 p.
5. « Perspectives des technologies de l'information de l'OCDE : TIC, commerce électronique et économie de l'information », O.C.D.E., *Science et Technologies de l'Information*, 2000, vol. 2000, n° 2, 286 p.
6. « Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique », O.C.D.E., *Science et Technologies de l'Information*, 2000, vol. 2000, n° 3, 41 p.
7. « Perspectives de la Science, de la Technologie et de l'Industrice de l'OCDE 2000 », O.C.D.E., *Science et Technologies de l'Information*, 2000, vol. 2000, n° 9, 285 p.
8. « Mesuring Expenditure on Health-related R&D », O.C.D.E., *Science et Technologies de l'Information*, 2001, vol. 2001, n° 6, 212 p.
9. « Les technologies de l'information et de la communication et le développement rural », O.C.D.E., *Science et Technologies de l'Information*, 2001, vol. 2001, n° 10, 203 p.
10. « Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données à caractère personne », O.C.D.E., *Science et Technologies de l'Information*, 2002, vol. 2002, n° 2, 72 p.
11. « Perspectives des technologies de l'information de l'OCDE, Les TIC et l'économie de l'information », O.C.D.E., *Science et Technologies de l'Information*, 2002, vol. 2002, n° 6, 356 p.
12. « Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information, Vers une culture de la sécurité », O.C.D.E., *Science et Technologies de l'Information*, 2002, vol. 2002, n° 9, 30 p.

13. « Les risques émergents au XXIe siècle, Vers un programme d'action », O.C.D.E., *Science et Technologies de l'Information*, 2003, vol. 2003, n° 2, 325 p.
14. « Protection de la vie privée en ligne : orientations politiques et pratiques de l'OCDE », O.C.D.E., *Science et Technologies de l'Information*, 2003, vol. 2003, n° 13, 437 p.
15. "Genetic Inventions, Intellectual Property Rights and Licensing Practices Evidence and Policies", O.C.D.E., *Science et Technologies de l'Information*, 2003, vol. 2003, n° 16, 112 p.
16. « Le projet de l'OCDE sur la Santé, Technologies de la santé et prise de décision », O.C.D.E., *Science et Technologies de l'Information*, 2005, vol. 2005, n° 16, 170 p.
17. "Report on GRIDS and Basic Reseach Programmes", O.C.D.E., *Global Science Forum*, 2 mars 2006.
18. "Workshop on the Future of the Internet", O.C.D.E., Paris, 8 mars 2006.

§ 6. DOCTRINE

1. BENNETT, B. (ed.), *e-Health Business and Transactional Law*, Washington, BNA Books, 2002, 734 p.

2. BOULANGER, M.-H., de TERWANGNE, C., LEONARD, Th., LOUVEAUX, S., MOREAU, D. & POULLET, Y., « La protection des données à caractère personnel en droit européen », Bruxelles, Larcier, *Journal des Tribunaux de Droit Européen*, 1997, p. 121 et s. (en trois parties)

3. CALLENS, S. (ed.), *e-Health and the Law*, The Hague, Kluwer Law International, 2003, 183 p.

4. CHABERT-PELTAT, C., « La télémédecine », Paris, *Revue Alain Bensoussan – Droit des Technologies Avancées*, 1999, n° 6/3-4, pp. 117-138.

5. Commission nationale de l'informatique et des libertés (CNIL-France), Délibération n° 97-049 du 24 juin 1997 portant avis sur la mise en oeuvre à titre expérimental d'un réseau de télémédecine sur Internet entre le Centre hospitalier d'Annecy et certains médecins de ville, Paris, *Revue Alain Bensoussan – Droit des Technologies Avancées*, 1999, n° 6/3-4, pp. 169-172.

6. DE BOT, D., *Verwerking van persoongegevens*, Kluwer, 2001.

7. de TERWANGNE, C., « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », obs. sous C.J.C.E. arrêt du 6 nov. 2003, Bodil Lindqvist, affaire C-101/01, *Revue du droit des technologies de l'information*, Bruxelles, Ed. Bruylant, 2004, pp. 67-99.

8. FLEISHER, L.D. & DECHENE, J.C., *Telemedicine and e-Health Law*, Law Journal Press, 2005.

9. HERVEG, J., « HealthGRID from a Legal Point of View », in *From GRID to HEALTHGRID*, IOS Publications, Studies in Health Technology and Informatics, 2005, Volume 112, part 5, pp. 312-318.

10. HERVEG, J. & VAN GYSEGHEM, J.-M., "La sous-traitance des données du patient au regard de la directive 95/46", *Lex Electronica*, vol. 9, n° 3, t. 2004, http://www.lex-electronica.org/articles/v9-3/herveg_vangyseghem.htm.

11. HERVEG, J., VERHAEGEN, M.-N. & 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 », Kluwer, *Revue de Droit de la Santé*, 2002-2003/2, pp. 56-84.

12. HERVEG, J., VAN GYSEGHEM, J.-M. & de TERWANGNE, C., *GRID-enabled medical simulation services and European Law*, Final Report on all the Legal Issues related to Running GRID Medical Services, European Research contract IST-2001-37153-GEMSS, 29 February 2005, 341 p.

13. IAKOVIDIS I., WILSON, P., Healy J.-Cl., *E-Health: Current Situation and Examples of Implemented and Beneficial E-Health Applications*, IOS Press, Studies in Health Technology and Informatics, 2004, Volume 100, 249 p.

14. KAPLAN, G. & Mc FARQUHAR, E., *e-Health Law Manual*, New-York, Aspen Publishers, 2003.

15. MIDDLETON, S.E., HERVEG, J., CRAZZOLARA, F., MARVIN, D. & POULLET, Y., « GEMSS : Security and Privacy for a Medical Grid », Stuttgart, Schattaeur, Verlag für Medizin und Naturwissenschaften, *Methods of Information in Medicine*, 2005, 44/2, p. 182-185.

16. RIENHOFF, O., LASKE, C., VAN EECKE, P., WENZLAFF, P. & PICCOLO, U., *A Legal Framework for Security in European Health Care Telematics*, Amsterdam, IOS Press, Studies in Health Technology and Informatics, 2000, vol. 74, 202 p.

17. RIGAUX, Fr., *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Paris, Bruylant, L.G.D.J., 1990.

19. ROGER-FRANCE, Fr., « Informations de santé, télématique et télémédecine, Perspectives d'ensemble à l'horizon 2000 », *Journal de réflexion sur l'informatique*, 1994, n° 30, pp. 7-9.

20. ROUSSEAU, A. & HERVEG, J., *Manuel d'informatisation des urgences hospitalières*, Louvain-la-Neuve, Presses Universitaires de Louvain, 2003, 183 p.

21. SILBER, D., *The case for eHealth*, Maastricht, Institut Européen d'Administration Publique (ed.), 2003, 32 p.

22. STANBERRY, B., *The Legal and Ethical Aspects of Telemedicine*, London, Royal Society of Medicine Press, 1998, 172 p.

23. VAN EECKE, P., "Electronic Health Care Services and the e-Commerce Directive", in *A decade of research @ the crossroads of law and ICT*, Gent, Larcier, 2001, pp. 365-379.

24. VILCHES ARMESTO, L., « IMS Health : dernier développement de la C.J.C.E. relatif au refus de licence en droit de propriété intellectuelle », note sous C.J.C.E., 29 avril 2004, Brussels, Larcier, *Revue du Droit des Technologies de l'Information*, 2004, n° 20, p. 59 et s.

25. WILSON, P., LEITNER, Chr. & MOUSSALI, A., *Mapping the Potential of eHealth, Empowering the citizen through eHealth tools and services*, Maastricht, European Institute of Public Administration (ed.), 2004, 52 p.