

## RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

### Confidentialité et sécurité pour les applications de télémédecine en droit européen

Herveg, Jean

*Published in:*  
Lex Electronica

*Publication date:*  
2007

*Document Version*  
le PDF de l'éditeur

[Link to publication](#)

*Citation for pulished version (HARVARD):*

Herveg, J 2007, 'Confidentialité et sécurité pour les applications de télémédecine en droit européen', *Lex Electronica*, VOL. 12, Numéro 1. <<http://www.lex-electronica.org/articles/v12-1/herveg.htm>>

#### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

#### Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# Confidentialité et sécurité pour les applications de télémédecine en droit européen\*

Jean Herveg\*\*

*Lex Electronica*, vol. 12 n°1 (Printemps / Spring 2007)

<http://www.lex-electronica.org/articles/v12-1/herveg.htm>  
<http://www.lex-electronica.org/articles/v12-1/herveg.pdf>

---

## Les applications de télémédecine

1. La télémédecine peut être définie comme étant l'application des technologies de l'information et de la communication aux activités du secteur des soins de santé<sup>1</sup>. A ce titre, la télémédecine offre de nombreux produits et services. Ainsi, par exemple :

- ♣ le dossier du patient est informatisé et le patient peut y accéder par voie télématique,
- ♣ l'imagerie médicale devient numérique et circule plus rapidement,
- ♣ les praticiens s'envoient des courriers électroniques sécurisés,
- ♣ les prescriptions de médicaments prennent une forme électronique,
- ♣ l'Internet offre au patient l'accès à de multiples sites d'information sur la santé dont certains sont labellisés, garantissant de cette façon une sorte de fiabilité quant à leur contenu informatif,
- ♣ de nouveaux dispositifs médicaux implantables ou ambulatoires apparaissent comme les systèmes de télésurveillance,
- ♣ les bases de données médicales sont mises en réseau à l'échelle locale, régionale, européenne, internationale et mondiale à des fins très variées, mais principalement aujourd'hui à des fins de prise en charge optimale du patient, de contrôle de la qualité et des dépenses des soins de santé, ou de recherche scientifique,
- ♣ les vêtements intelligents font leur apparition : ils sont munis de capteurs pour collecter différents paramètres ou ils permettent la délivrance à distance de substances directement au patient,
- ♣ le travail coopératif entre les praticiens de la santé est facilité par des applications supportées par des réseaux télématiques qui autorisent aussi les prestations de santé à distance comme la téléconsultation ou la téléchirurgie,
- ♣ la prise en charge individuelle et collective du patient peut être gérée de manière informatique notamment pour la prise de rendez-vous et la gestion de l'occupation des lits d'hôpitaux,

---

\* Ce texte est une suite à la contribution faite lors de la réunion scientifique de la Société Européenne de Télémédecine le 26 septembre 2005 à Paris. Cette contribution était intitulée « *Introduction à la protection des données médicales en droit européen : interdiction de traiter et exceptions* ».

\*\* Chercheur au Centre de Recherche en Informatique et Droit (CRID – <http://www.crid.be>), Facultés Universitaires Notre-Dame de la Paix, Namur, Belgique. Courriel : [jean.herveg@fundp.ac.be](mailto:jean.herveg@fundp.ac.be).

<sup>1</sup> Voyez en ce sens la 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 (COM(2004)356 final).

- ♣ l'assistance automatisée aux prestations de soins de santé se développe grâce à des outils d'aide au diagnostic, au traitement et à la médication, transférant la connaissance médicale à la machine et en transformant le praticien de la santé en une sorte d'interface en contact avec le patient,
- ♣ et les activités de contrôle et de financement des soins de santé créent leurs propres systèmes d'information afin de réaliser plus efficacement leurs missions.

2. Le nombre et le type d'applications ou de services et produits de télémédecine paraissent illimités. En effet, ces applications ne comprennent pas seulement les logiciels dans les ordinateurs<sup>2</sup>. Elles sont aussi variées que les informations à gérer. Ces informations se rapportent tant aux patients qu'au personnel soignant et qu'à leurs collaborateurs. Elles concernent tant la pratique et l'organisation de l'activité médicale que son encadrement en termes de santé publique et de financement, les activités de recherches visant au développement de nouveaux médicaments et dispositifs médicaux, et l'affirmation du patient comme acteur de sa santé. Le développement de ces applications est d'autant plus utile que, depuis plusieurs décennies, la médecine permet de produire de plus en plus d'informations, de meilleure qualité de surcroît, sur l'état de santé des patients et les soins qui leur sont prodigués, que ceux-ci soient considérés individuellement ou collectivement. Les avancées scientifiques en la matière vont des analyses du sang à l'ingénierie génétique, en passant par l'évolution vertigineuse de l'imagerie médicale. Corrélativement, les traitements médicaux se sont encore améliorés tout en essayant d'être moins invasifs.

### **Les infrastructures de télécommunication et les futurs systèmes d'information à deux niveaux dans les soins de santé**

3. Fréquemment, les applications de télémédecine recourent à des solutions de télécommunication qui leur sont spécialement dédiées, que ce soit via l'Internet ou par des réseaux télématiques fermés. Par conséquent, à une application donnée correspond souvent une solution de télécommunication qui lui est spécialement adaptée. L'exemple type est le système de télécommunication qui relie les différentes bases de données au sein d'un hôpital. C'est le premier âge de la télémédecine. Toutefois, aujourd'hui, des projets visent à créer des infrastructures télématiques permanentes que les applications de télémédecine pourront utiliser de manière indifférenciée. Ces infrastructures seraient donc créées sans référence à une application déterminée de télémédecine. Elles devraient pouvoir supporter n'importe quel produit ou service de télémédecine. Si ces projets aboutissent, ce sont de véritables autoroutes de l'information qui feront leur apparition dans le secteur des soins de santé. Dans ce contexte, les futures applications de télémédecine se présenteront sous la forme de systèmes d'information à deux niveaux. Le premier niveau du système d'information sera constitué par l'infrastructure [permanente] de télécommunication proprement dite (ce qui implique généralement la collecte et le traitement de données à caractère personnel nécessaires à cette fin, cf. *infra*). Le second niveau du système d'information sera constitué par les applications de télémédecine que l'infrastructure de télécommunication va permettre de supporter. Ces systèmes d'information à deux niveaux caractérisent le deuxième âge de la télémédecine. La Belgique s'est résolument engagée dans cette voie avec le projet Be-Health<sup>3</sup> du gouvernement fédéral.

<sup>2</sup> Ils incluent aussi, par exemple, les logiciels intégrés dans les dispositifs médicaux.

<sup>3</sup> Voyez à propos de Be-Health :

[https://portal.health.fgov.be/portal/page?\\_pageid=56,4280428&\\_dad=portal&\\_schema=PORTAL](https://portal.health.fgov.be/portal/page?_pageid=56,4280428&_dad=portal&_schema=PORTAL).

4. Ces nouveaux projets relèvent principalement d'une politique structurelle de création d'infrastructures télématiques dans le secteur des soins de santé. C'est aussi le passage d'une conception verticale de l'organisation de la santé en ligne, à une conception qui, dans un premier temps, est abstraite, horizontale et transversale, et puis qui, dans un second temps, est verticale et concrète. La simple existence de ces nouvelles infrastructures télématiques dans le secteur des soins de santé ouvre la porte au partage de bases de données scientifiques, implique l'identification des praticiens et des patients grâce à des registres spéciaux, etc. A terme, ces réseaux vont modifier profondément l'organisation de la santé publique et tous les acteurs des soins de santé seront concernés : les praticiens, les patients, les organes de santé publique et de sécurité sociale, les laboratoires médicaux, etc.

Mais, encore une fois, ce qui différencie ces nouveaux systèmes d'information, leur nouveauté, c'est l'idée de la permanence de leur infrastructure de télécommunication de base par rapport à leurs exploitations futures. Ainsi, l'opportunité de créer ces infrastructures ne se mesure plus directement par rapport aux finalités précises et concrètes qu'elles vont permettre de réaliser. L'opportunité de les créer va être évaluée de manière abstraite au regard de catégories de finalités dont le contenu précis et concret sera défini ultérieurement. Il existe donc un changement dans le degré de précision et de matérialité requis pour apprécier les finalités poursuivies pour créer l'infrastructure télématique et pour son exploitation future.

5. Forts de ces développements, les promoteurs de la télémédecine souhaitent créer des réseaux télématiques à l'échelle locale, régionale, nationale, européenne, internationale, voire même mondiale. Ces réseaux vont au-delà de la sphère usuelle d'influence des acteurs de la santé et de leurs activités présentes. En effet, ils impliquent de plus en plus d'intermédiaires, de techniciens, et quantité d'autres acteurs comme, par exemple, les organismes publics et privés qui participent aux politiques de santé publique et de sécurité sociale. Les raisons qui sous-tendent ces projets sont nombreuses notamment en termes de santé publique, de participation du citoyen, de financement des soins de santé et de contrôle de leur qualité, de recherche scientifique, de découverte de nouveaux médicaments ou dispositifs médicaux. Ces nouveaux réseaux s'articulent autour de l'information (entendue largement), des acteurs des soins de santé, des produits et services de la santé en ligne qu'ils soutiennent et des infrastructures particulières complémentaires propres à ces derniers. De même, ces infrastructures télématiques offrent la possibilité d'étoffer encore plus les applications de télémédecine prédécrites.

### **L'encadrement juridique de la télémédecine et la protection des données médicales**

6. Les questions juridiques suscitées par l'émergence de la télémédecine sont particulièrement nombreuses notamment en termes d'encadrement opérationnel des nouvelles applications de télémédecine, de responsabilités, d'aspects internationaux, de reconnaissance des pratiques et des praticiens, en n'omettant pas de distinguer correctement les différents niveaux des systèmes d'information envisagés. Parmi ces questions, la protection des données médicales du patient occupe une place centrale. La Cour européenne des droits de l'homme a d'ailleurs eu l'occasion d'insister sur la nécessité de les protéger dans les arrêts *Z c Finlande* et *M.S. c Suède*<sup>4</sup> :

*« La Cour rappelle que la protection des données à caractère personnel, et spécialement des données médicales, revêt une importance fondamentale pour*

---

<sup>4</sup> C.E.D.H., *Z c Finlande*, 25 févr. 1997 ; *M.S. c Suède*, 27 août 1997.

*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 ».*

7. En Europe, la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données<sup>5</sup> constitue le socle<sup>6</sup> commun aux Etats membres en matière de protection des données à caractère personnel, ce qui englobe la protection des données médicales. Cette directive agit à différents niveaux pour assurer l'effectivité de la protection des données à caractère personnel. D'abord, elle structure son champ d'application en fonction des compétences de la Communauté européenne d'une part et d'autre part en fonction des situations qui requièrent une protection (*cf.* chapitre I de la directive)<sup>7</sup>. Ensuite, la directive définit les conditions générales de licéité des traitements de données à caractère personnel (*cf.* chapitre II de la directive). Elle impose l'existence de recours juridictionnels 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).

Parmi les conditions générales de licéité des traitements de données à caractère personnel figurent la confidentialité et la sécurité des traitements<sup>8</sup>. Ces dernières sont au cœur du présent exposé en matière de protection des données médicales. Il convient d'insister sur le fait que la confidentialité et la sécurité des traitements de données ne sont qu'une partie des règles qui assurent la protection des données médicales. Il existe d'autres conditions générales de licéité notamment en termes de droits de la personne concernée (information, droits d'accès, de rectification et d'opposition), de notification du traitement de données à l'autorité nationale de

<sup>5</sup> A ce sujet, voyez principalement : Y. Pouillet, 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).

<sup>6</sup> Sans oublier la Convention n° 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et les recommandations du Conseil de l'Europe (essentiellement la recommandation (97) 5 du 13 février 1997 relative à la protection des données médicales), ce socle peut déjà à tout le moins être complété par la 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).

<sup>7</sup> 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, *Revue du droit des technologies de l'information*, Bruxelles, Ed. Bruylant, 2004, pp. 67-99.

<sup>8</sup> Section VIII du chapitre II consacré aux conditions générales de licéité des traitements de données à caractère personnel : « Confidentialité et sécurité des traitements ».

contrôle, ainsi que d'autres règles que les conditions générales de licéité. Il faut retenir que la confidentialité et la sécurité des traitements de données médicales sont importantes dans la mesure où elles interviennent aussi dans l'appréciation de la légitimité du traitement de données et la possibilité d'un traitement ultérieur. Ainsi, l'existence de garanties sérieuses en termes de confidentialité et de sécurité permet de contrebalancer dans une certaine mesure le risque présenté par un traitement de données sensibles et, partant, de consolider le cas échéant sa légitimité lors de la mise en balance des intérêts en présence.

## **La confidentialité et la sécurité des traitements de données médicales**

**8.** Les notions de confidentialité et de sécurité des traitements de données à caractère personnel, en ce compris ceux portant sur des données médicales, doivent s'envisager au regard des deux niveaux des nouveaux systèmes d'information qui apparaissent dans le secteur des soins de santé, soit au niveau de l'infrastructure télématique et au niveau de l'application. Ces deux niveaux doivent être considérés séparément et globalement.

L'infrastructure de télécommunication doit être sécurisée et stable. Elle doit aussi assurer la sécurité et la confidentialité des traitements de données à caractère personnel réalisés dans le cadre du second niveau, sans préjudice de la confidentialité et de la sécurité des traitements de données réalisés au premier niveau pour la constitution et le fonctionnement de l'infrastructure de télécommunication.

Concernant les traitements de données à caractère personnel à identifier<sup>9</sup> tant au niveau de la création et du fonctionnement de l'infrastructure de télécommunication qu'au niveau des applications de télémédecine, le respect de la *confidentialité* implique que toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant<sup>10</sup>, ainsi que le sous-traitant lui-même, et 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<sup>11</sup>.

La *sécurité* des traitements implique que le responsable du traitement, en collaboration étroite avec le « responsable de l'infrastructure de télécommunication », 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 traitement illicite. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise

---

<sup>9</sup> Le traitement de données à caractère personnel est défini par la finalité qu'il poursuit ; il est constitué de l'ensemble des opérations effectuées sur des données pour réaliser cette finalité. Il faut ensuite identifier tous les acteurs du traitement de données et leurs droits et obligations (principalement le responsable du traitement, c'est-à-dire celui qui définit les moyens et les finalités du traitement, le sous-traitant éventuel, et la personne concernée).

<sup>10</sup> La notion de sous-traitant est différente de celle de responsable du traitement. Le sous-traitant traite des données à caractère personnel dans le cadre strict de la mission déterminée qui lui est impartie par le responsable du traitement. Il ne peut pas utiliser les données à caractère personnel pour d'autres finalités. La notion de sous-traitant est très importante et très utile dans le contexte des infrastructures et des réseaux télématiques dans le secteur des soins de santé. Elle permet de qualifier les fonctions de plusieurs intermédiaires techniques (par exemple, une entreprise qui offre des capacités de stockage de l'information, les plates-formes HealthGRID, ou les fournisseurs secondaires pour les applications de télémédecine et dans certains cas les laboratoires d'analyses médicales et les spécialistes extérieurs).

<sup>11</sup> Directive 95/46/CE, art. 16.

en oeuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger<sup>12</sup>.

Lorsqu'il confie à un tiers la réalisation du traitement de données à caractère personnel, le responsable du traitement doit choisir à cet effet un *sous-traitant* qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures<sup>13</sup>.

Il peut sembler difficile de respecter ces contraintes, particulièrement lorsque ces infrastructures télématiques supposent l'intervention d'intermédiaires qui ne sont pas soumis en tant que tels aux règles du secret médical et de la déontologie médicale. Toutefois, les technologies de l'information et de la communication sont susceptibles de fournir des solutions à ces problèmes, de même que le recours à la labellisation des sous-traitants et à l'élaboration de codes de conduite sectoriels. Dans certaines hypothèses, outre les mesures classiques de sécurité, il convient d'apprécier l'opportunité et la nécessité d'avoir une personne détachée à la protection des données<sup>14</sup>, d'avoir d'autres organes et procédures de contrôle - tant interne qu'externe - des activités menées dans ces systèmes d'information, sans omettre la formation et la sensibilisation à intervalles réguliers du personnel aux règles applicables à la protection des données. Dans une certaine mesure, la confidentialité et la sécurité du traitement de données médicales sont aussi assurées par un contrôle reconnu au patient notamment sur les accès et utilisations de ses données médicales.

Par ailleurs, la directive 2002/58/CE prévoit des règles relatives à la sécurité et à la confidentialité des communications électroniques. Cependant, ces règles ne concernent que les infrastructures ouvertes et accessibles au public<sup>15</sup>.

**9.** En ce qui concerne les applications ou produits et services de télémédecine qui correspondent à des services de la société de l'information<sup>16</sup>, la directive 2000/31/CE a pour

---

<sup>12</sup> Directive 95/46/CE, art. 17.1.

<sup>13</sup> Directive 95/46/CE, art. 17.2. Les Etats Membres ont l'obligation d'identifier les traitements de données à caractère personnel qui présentent des risques particuliers et de les contrôler avant leur mise en œuvre (directive 95/46/CE, art. 20).

<sup>14</sup> Cette notion provient des articles 18.2 et 20.2 de la directive 95/46/CE. C'est une personne, employée ou non du responsable du traitement, qui doit être en mesure d'exercer ses fonctions en toute indépendance (considérant 49 de la directive précitée) et qui est principalement chargée d'assurer d'une manière indépendante l'application interne des dispositions nationales prises en application de la directive précitée (art. 18.2 de la directive précitée). Son existence permet au droit national applicable d'envisager des simplifications ou des dérogations à l'obligation de notifier le traitement de données à l'autorité de contrôle (art. 18.2 de la directive précitée). Le détaché à la protection des données peut également intervenir dans le cadre des traitements de données qui présentent des risques particuliers pour les droits et libertés des personnes concernées (art. 20.2 de la directive précitée).

<sup>15</sup> Directive 2002/58/CE, précitée (voir note infra-paginale n° 5), art. 4, 5, 6 et 9.

<sup>16</sup> La définition des services de la société de l'information figure dans la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information et dans la directive 98/84/CE du Parlement européen et du Conseil du 20 novembre 1998 concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel. Cette définition couvre tout service fourni, normalement contre rémunération, à distance au moyen d'équipement électronique de traitement (y compris la compression numérique) et de stockage des données, à la demande individuelle d'un destinataire de services. Les services visés dans la liste indicative figurant à l'annexe V de la directive 98/34/CE qui ne comportent pas de traitement et de stockage des données ne sont pas couverts. Les activités qui par leur nature ne peuvent pas être réalisés à distance et par voie électronique, comme l'examen physique du patient, ne sont pas des services de la société de l'information. Mais si la téléconsultation ne nécessite pas un contact physique avec le patient, ce pourrait être un service de la société de l'information (par exemple, les activités de télésurveillance).

objectif de garantir la sécurité juridique et la confiance du consommateur<sup>17</sup>, notamment en encadrant certains aspects juridiques des contrats passés par voie électronique, tandis que d'autres directives encadrent aussi la protection du consommateur<sup>18</sup>. Les nouveaux produits et services qui pourront être offerts par le biais de ces nouvelles infrastructures télématiques médicales renforceront la place du patient dans la relation médicale, notamment en tant que « consommateur » et en lui assurant de ce fait le bénéfice des droits découlant de cette nouvelle approche (sans omettre ses obligations subséquentes).

## Conclusions

**10.** Les applications de télémédecine se sont développées de manière quelque peu « anarchique » au gré des besoins des praticiens ou, le plus souvent, au gré des projets émanant du monde politique, du médicament ou de l'informatique. Ces applications combinent fréquemment des services et produits de télémédecine avec des infrastructures particulières de télécommunications basées sur l'Internet ou des réseaux fermés. Maintenant, des projets visent à développer des infrastructures permanentes de télécommunication dans les soins de santé pour faciliter un développement efficace et planifié de la télémédecine et de ses applications. Ce faisant, ces projets ouvrent le deuxième âge de la télémédecine. La Belgique s'est résolument engagée dans cette voie avec le projet « Be-Health » du gouvernement fédéral.

**11.** Les questions juridiques posées par la télémédecine sont nombreuses, mais celle portant sur la protection des données médicales est centrale et première. A deux reprises, la Cour européenne des droits de l'homme a rappelé avec vigueur la nécessité de les protéger. Au sein des règles assurant la protection des données médicales, la confidentialité et la sécurité des traitements de données médicales occupent une place particulière. Dans le second âge du développement de la télémédecine, la confidentialité et la sécurité des traitements de données médicales ne doivent pas s'envisager en vase clos au regard des seules applications de télémédecine mais bien en tenant compte de l'existence d'une infrastructure de télécommunication qui les supportent. Ces infrastructures jouent un rôle crucial dans la confidentialité et la sécurité des traitements de données médicales. A cet égard, il convient de réfléchir au-delà des mesures classiques destinées à assurer la confidentialité et la sécurité des traitements de données. En effet, dans les nouveaux systèmes d'information à deux niveaux dans les soins de santé, la confidentialité et la sécurité des traitements de données doivent s'apprécier aux deux niveaux considérés tant séparément que globalement. En tout cas, la confidentialité et la sécurité des traitements de données médicales requièrent la mise en place d'organes et de procédures de contrôle spécifiques portant tant sur le fonctionnement des applications de télémédecine que sur celui de l'infrastructure de télécommunications. Ces

---

<sup>17</sup> Directive 2000/31/CE, considérant 7.

<sup>18</sup> Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil (« directive sur les pratiques commerciales déloyales ») ; Directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain ; Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance ; Directive 1999/44/CE du Parlement européen et du Conseil, du 25 mai 1999, sur certains aspects de la vente et des garanties des biens de consommation ; Directive 2001/95/CE du Parlement européen et du Conseil du 3 décembre 2001 relative à la sécurité générale des produits ; Directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux.



organes et procédures participeront en outre à la transparence et à l'acceptabilité de ces nouveaux systèmes d'information dans les soins de santé en leur offrant une meilleure visibilité dans la société de l'information. A titre d'exemple, la création et le fonctionnement de ces systèmes d'information devraient être supervisés par des détachés à la protection des données. Ils devraient aussi être audités régulièrement tant par des organes internes qu'en externes. Des registres de l'ensemble des traitements de données effectués au-delà des seules applications - donc au niveau de l'infrastructure aussi – devraient être créés. De même, des codes de conduite sectoriels devraient être rédigés pour harmoniser et faciliter l'application des règles applicables aux traitements de données eu égard aux spécificités des activités considérées. Les sous-traitants devraient être labellisés et le personnel employé tant pour l'infrastructure que pour les applications devraient être régulièrement formés et sensibilisés aux règles applicables aux traitements de données. Enfin, le patient devrait pouvoir contrôler l'usage de ses données médicales, notamment en ayant accès à la liste des personnes ayant pris connaissance de ses données et en connaissant l'usage fait de ces dernières. De cette façon, l'application des technologies de l'information et de la communication aux soins de santé aura plus de chances de préfigurer un monde meilleur et d'écarter une suspicion citoyenne qui, à défaut, serait tout à fait légitime.