GenEditorial

ÉDITORIAL SUR LES ENJEUX ÉTHIQUES, JURIDIQUES ET SOCIAUX DE LA GÉNÉTIQUE HUMAINE

(2006) 4:1 *GenEdit,* 1-8

L'ENCADREMENT JURIDIQUE DU TRAITEMENT INFORMATISÉ DES DONNÉES RELATIVES À LA SANTÉ : PERSPECTIVE EUROPEO-CANADIENNE

Cynthia Chassigneux[1], Pierre Trudel[1], Bartha Maria Knoppers[1]

Le recours aux technologies de l'information et de la communication dans tous les domaines de la vie politique, économique et sociale doit s'accompagner d'une réflexion quant à la pertinence ou non de compléter, de réviser en tout ou en partie l'encadrement juridique applicable à un secteur donné. Cette orientation est particulièrement importante lorsqu'il s'agit d'informatiser le traitement des données relatives à la santé. Pour appréhender les éléments cruciaux de cette problématique, les auteurs s'intéressent à l'encadrement actuel et à certains enjeux inhérents à cette « nouvelle » façon d'envisager la gestion de ces données et ce dans une perspective europeo-canadienne.

Le recours aux technologies de l'information et de la communication dans le secteur de la santé et des services sociaux ou encore le développement de réseaux de recherche multicentriques et internationaux présente des bénéfices pour la société : meilleur suivi de l'état de santé des personnes physiques, meilleure qualité des soins, meilleure maîtrise des dépenses, meilleure communication entre les professionnels de la santé, par exemple[1]. Toutefois, cette approche relance une problématique : celle relative à la protection de la vie privée, plus particulièrement au traitement des données relatives à la santé d'un individu.

Ces données sont qualifiées de sensibles notamment par la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*[2] du Conseil de l'Europe (ci-après « Convention n°108 ») et la *Directive 95/46/CE* du Parlement européen et du Conseil, du 24 octobre 1995, *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*[3] (ci-après « Directive 95/46/CE »). Compte tenu de la nature de ces données, leur traitement est interdit sauf si la personne concernée y consent ou dans les cas prévus par les législations nationales. Cette conception trouve écho, en France, dans la *Loi n°78-17 du 6 janvier*

1. Université de Montréal, Centre de recherche en droit public

 ISSN 1718-9306

1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la *Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* du 6 août 2004[4] (ci après « Loi 78/17 modifiée en 2004 »), dont l'article 8 prévoit une série d'exceptions levant cette interdiction[5].

Cependant, une telle particularité ne se retrouve pas dans toutes les législations. Une analyse des textes européen et canadien permet, en effet, de noter que, le plus souvent, ces données sont enchâssées dans la définition même des notions de « renseignements personnels » ou de « données à caractère personnel »[6] – c'est-à-dire toute information permettant d'identifier, directement ou non, une personne physique. Dans cette optique « tous les renseignements permettant d'identifier une personne, quelle qu'en soit la portée ou le degré de sensibilité, sont donc considérés comme des renseignements personnels bénéficiant de l'égale protection de la loi »[7]. Par contraste, la *Loi* fédérale canadienne *sur la protection des renseignements personnels et les documents électroniques*[8] (ci-après « LPRPDÉ ») de même que les législations des provinces de l'Alberta[9], de l'Ontario[10], du Manitoba[11] et de la Saskatchewan[12] ont adopté des définitions spécifiques aux renseignements personnels de santé.

Face à cette situation, est-ce à dire que le traitement – informatisé ou non – des données relatives à la santé diffère selon l'entendement qu'en a le législateur ? La lecture, là encore, des normes européenne et canadienne nous conduit à répondre par la négative. En effet, on constate que par « traitement », les législateurs font référence aux évènements qui surviennent tout au long du cycle de vie des données, c'est-à-dire en partant de la collecte jusqu'à la destruction de celles-ci.

Cette absence de statut spécifique des données de santé fait écho aux principes fondamentaux énoncés, dès 1980, dans les *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*[13] de l'Organisation de Coopération et de Développement Économiques (ci-après « Lignes directrices de l'OCDE ») auxquelles les pays membres de l'Union européenne et le Canada ont adhéré. Est-ce que cela veut dire qu'il est alors possible de communiquer électroniquement ces données entre l'Europe et le Canada sans prendre de précautions particulières ? Si nous sommes enclins à répondre par la négative, il convient toutefois de préciser que cette question oblige à repenser la place que l'on entend accorder à la personne concernée par les données, c'est-à-dire au patient, au participant à un projet de recherche ou encore aux représentants légaux. Elle oblige également à reconsidérer l'administration du système de santé. En effet, le cadre de gestion de ces échanges doit-il se faire en silo ou s'envisager dans une optique en réseau ?

Privilégier cette dernière avenue, comme nous entendons le faire et comme illustré par des projets comme le Système d'Information du Réseau Intégré de Laval (SI-RIL) au Québec, le dossier médical personnel[14] ou encore la carte Vitale en France, entraîne une révision du principe de finalité afin de s'assurer que les informations utilisées sont de qualité adéquate pour servir aux fins envisagées, non ériger la redondance qui résulte de l'imposition de collectes répétées en garantie de la vie privée. Elle nécessite également de repenser le cadre de la protection des renseignements personnels en considérant que les citoyens interagissent avec un ensemble d'entités ce qui requiert l'établissement d'un climat de confiance, de transparence car « plus les informations demandées sont susceptibles d'être sensibles, plus il faut multiplier les précautions afin de garantir le niveau de confiance nécessaire »[15].

L'appréhension des éléments cruciaux du droit de la protection des données de santé passe par l'examen de l'encadrement actuel (I) afin de considérer les enjeux du traitement informatisé des données relatives à la santé (II).

 ISSN 1718-9306

I. Le traitement informatisé des données relatives à la santé : l'encadrement actuel

Les instruments normatifs visent à encadrer le traitement des renseignements personnels dans une société fonctionnant de façon croissante en réseau. L'observation des cadres juridiques classiques mène au constat que ces textes entendent « fixer […] des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances »[16], ou encore s'assurer que le développement de l'informatique ne porte « atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »[17]. Malgré que ces textes ont vocation à s'appliquer quel que soit le support envisagé, les principes qui y sont prescrits ne sont pas forcément applicables à un environnement en réseau, soit des espaces interconnectés dans lesquels l'information circule d'un pôle à l'autre, de façon multidirectionnelle et non hiérarchique[18].

Dès lors, comment concilier les nécessaires besoins d'échanges de données entre les professionnels de la santé et/ou les chercheurs et la nécessité de protéger les attentes raisonnables en matière de vie privée des personnes concernées ? Comment faire en sorte que les normes juridiques protégeant ces attentes s'imposent aux partenaires du réseau, tout en veillant à ce que l'interprétation de ces normes tienne compte des impératifs de fonctionnalité et d'efficience de ce même réseau et permette aux personnes d'avoir les meilleurs services ?

Le **consentement** doit-il encore être l'élément devant prévaloir dans le cadre de l'informatisation du système de santé et des services sociaux et du développement croissant des projets de recherche multicentriques et internationaux ? La place accordée au consentement n'est-elle pas de nature à réduire la circulation des données ? N'est-il pas de nature à favoriser la démultiplication des données détenues par le système de santé ?

Alors qu'une importante partie de la communauté juridique semble encore attachée à la prépondérance du consentement,[19] celui-ci se révèle un outil peu adapté à la protection des droits dans les univers en réseaux. Tel que pratiqué, suivant une conception formaliste, le consentement paraît de plus en plus comme un leurre dès lors qu'il s'agit d'assurer la maîtrise par les personnes physiques de leurs données. Le nombre considérable d'exceptions permettant d'y passer outre de même que la façon dont circulent désormais les données font paraître le consentement comme un instrument au mieux naïf, au pire carrément contre-indiqué si l'on veut vraiment protéger la vie privée des sujets. Face à cette situation, il importe de revenir à l'essence même de la relation s'établissant avec un professionnel de la santé et/ou un chercheur. Il s'agit ici de redonner ses lettres de noblesses à la notion de confiance.

Plutôt qu'un acte de consentement figé dans le temps, un **lien de confiance** requis dans le cadre d'une relation nécessitant une forme d'abandon de la part de l'une des parties, doit pouvoir s'exprimer tout au long du cycle de vie des renseignements personnels, et plus particulièrement des données relatives à la santé. Un dialogue véritable doit s'établir entre l'émetteur et le destinataire de la confiance, que la relation s'effectue sous le signe de la transparence et non de l'opacité, pour éviter que la méfiance ne prenne le pas sur la confiance. Ce sentiment, nécessaire dans le cadre d'une activité commerciale[20], doit aussi prévaloir lorsque l'on envisage le traitement informatisé des données relatives à la santé.

Pour cela, il importe que la personne concernée soit informée des finalités, ce qui englobe le fait que les données puissent faire ou non l'objet d'une communication, d'un partage, d'un transfert électronique vers un autre territoire. À cela s'ajoute la

transparence quant aux mesures de sécurité prises pour assurer la confidentialité et la qualité des données tout au long de leur cycle de vie ou encore quant la possibilité d'accéder à ses données. Les enjeux du traitement informatisé des données relatives à la santé se situent à ce niveau plutôt qu'à celui de la recherche et la gestion du consentement.

II. Le traitement informatisé des données relatives à la santé : les enjeux

Pour permettre un développement des traitements informatisés de données relatives à la santé compatible avec le respect effectif de la vie privée, tant par le biais de l'interconnexion des établissements de santé, du recours à un dossier médical personnel, à l'instauration d'une carte à puce ou encore à la constitution de projets de recherche multicentriques et internationaux, il convient de s'intéresser aux enjeux inhérents à cette réalité. Sans prétendre tous les examiner[21], il peut être utile d'insister sur la gestion des droits d'accès et les flux transfrontières de données.

Ainsi tant les normes européennes que les normes canadiennes commandent que les traitements s'effectuent dans le respect des droits des personnes concernées : **confidentialité et droit d'accès**. Ces deux préceptes sont antinomiques en apparence seulement. En effet, confidentialité ne signifie pas que le professionnel de la santé ou le chercheur ayant collecté des données de santé relatives à un individu ne peut les communiquer, les transférer ou les partager avec des tiers. Si l'on considère la kyrielle d'exceptions contenues dans les différents instruments visant à protéger les informations identifiant, directement ou non, une personne physique[22] ces préceptes signifient que ces échanges doivent s'établir entre les seules personnes autorisées et aux seules fins énoncées. En somme, le partage des données de santé est une pratique répandue et cela se fait habituellement pour d'excellentes raisons et dans le respect de la vie privée des personnes.

Il convient donc de veiller à ce qu'il n'y ait pas de bris de confidentialité dans la chaîne des échanges, c'est-à-dire lors de la transmission ou pendant le stockage des données dans une banque, par exemple. C'est pourquoi confidentialité rime avec mesures de sécurité[23]. Dans un tel contexte, la **gestion des droits d'accès** devient un outil crucial de protection. La régulation des droits d'accès concerne non seulement les personnes autorisées – c'est-à-dire généralement les professionnels de la santé et/ou les chercheurs dans le cadre d'un projet de recherche, mais aussi les personnes concernées – c'est-à-dire le patient, le participant à une recherche ou encore les représentants légaux.

Concernant les personnes autorisées, il convient de déterminer si l'accès doit être entier ou réduit à certains éléments du dossier de santé et/ou du dossier de recherche. Dès lors, selon le choix arrêté, au cas par cas, il faudra établir des procédures permettant d'identifier la personne souhaitant accéder à un dossier et, corrélativement de déterminer ses droits. Cette mesure est prescrite notamment dans deux recommandations du Conseil de l'Europe : une relative à la réglementation applicable aux banques de données médicales automatisées[24] et une autre portant sur la protection des données médicales[25] (ci-après « Recommandation n°R(97)5 »).

Ainsi, dans un projet comme le *Canadian Molecular Cytogenetic Platform* (ci-après « CMCP »)[26] il a été décidé qu'un médecin et/ou chercheur associé au projet peut consulter les dossiers constitués par les autres membres du *CMCP*. Il est important de préciser que ces dossiers ne contiennent aucune information nominative relative à la personne concernée, comme énoncé notamment dans l'*Énoncé de politique des trois Conseils relatif à l'éthique de la recherche avec des êtres humains*[27], la *Recommandation n°R(97)5*[28] ou encore la *Loi 78/17 modifiée en 2004* [29].

 ISSN 1718-9306

De plus, l'accès autorisé ne concerne pas l'ensemble des informations contenues dans la banque centrale, mais seulement celles issues du ou des réseau(x) de recherche auxquels il est associé. Il y a donc ici un contrôle et une hiérarchisation des droits d'accès lors de la saisie de l'identifiant et du mot de passe.

Au regard des personnes concernées, il est généralement reconnu que celles-ci ont le droit d'accéder à leurs données[30]. Toutefois, compte tenu des répercussions sur l'état de santé susceptibles d'intervenir lors de la communication des informations, doit-on avoir une approche paternaliste de ce droit ? Ainsi le patient ou le participant à un projet de recherche peut-il exercer directement ce droit ou doit-il demander au professionnel de la santé et/ou au chercheur d'exercer ce droit pour lui ? Si certains pays ont depuis longtemps reconnu à toute personne concernée le droit d'agir directement, d'autres n'ont accepté cette possibilité que depuis quelques années, tout en maintenant le recours à un intermédiaire, comme illustré, en France, par la *Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé* qui a adopté cette avenue à l'article L. 1111-7 au Code de la santé publique[31].

Que ce droit s'exerce directement ou non, celui-ci a pour corollaire de permettre à la personne concernée de demander la rectification, voire la suppression de ses données à l'exception toutefois des données dites agrégées dans un projet de recherche, par exemple. Ce droit – d'accès et de rectification – doit se faire auprès de la personne responsable du traitement des données.

Cette action de la personne concernée lui donne également la possibilité de connaître si ses données ont fait l'objet d'un **flux transfrontières**. En effet, que l'on considère les instruments européen[32] (*Directive 95/46/CE* en particulier) ou canadien, on constate que ceux-ci prennent tous en considération la possibilité de communiquer, de partager, de transférer des données relatives à la santé des personnes physiques vers une autre province, un autre pays, étant entendu que cette possibilité ne doit pas permettre un contournement des règles applicables en matière de protection des renseignements personnels sur le territoire d'origine.

Par conséquent, le responsable du traitement doit veiller à ce que le territoire destinataire des données offre une protection semblable à celle existant dans le pays d'origine. Cette précaution doit faire l'objet d'une évaluation approfondie des normes en présence, par exemple, lorsque l'on envisage de confier la conservation des données à un opérateur situé en dehors du territoire national ou de développer un projet de recherche regroupant différents pays ou provinces.

En cette matière, il est permis de dire que l'encadrement appliqué aux renseignements personnels, qu'ils soient ou non relatifs à la santé, tant dans les pays Membres de l'Union européenne qu'au Canada, s'apparente. Comme indiqué précédemment, ces deux ensembles mettent de l'avant les mêmes principes fondamentaux en matière de protection des informations permettant d'identifier, directement ou non, une personne physique. Il est, dès lors, possible de procéder à des traitements informatisés des données relatives à la santé entre ces deux espaces géographiques en prenant soin d'effectuer au préalable une analyse des risques.

Conclusion

Cette analyse de l'encadrement juridique du traitement informatisé des données relatives à la santé indique la nécessité de reconsidérer les principes entourant la protection des renseignements personnels afin de les adapter aux environnements électroniques. Les mutations induites par le recours aux technologies de l'information et de la communication dans le secteur de la santé et des services sociaux doivent conduire à une redéfinition, d'une part, du rôle de chacun des acteurs, en faisant la distinction entre les personnes autorisées et celles qui sont concernées par les données et, d'autre part, de l'espace dans lequel circulent les renseignements personnels.

[1] Voir notamment, Liliane DUSSERRE, « La sécurité des échanges électroniques d'informations médicales nominatives entre médecins », Rapport adopté lors de la session du conseil national de l'Ordre des médecins, avril 2001, <http://www.web.ordre.medecin.fr/rapport/echangeselectroniques.pdf> (page consultée le 01 mars 2006). Ce rapport est également accessible dans Anne-Marie DUGUET, *Séminaire d'actualité de droit médical. Le secret professionnel. Aspects légaux et déontologiques. Comparaison avec l'étranger*, Bordeaux, Les Études Hospitalières, 2002, pp. 167-180.

[2] Strasbourg, 28 janvier 1981, <http://conventions.coe.int/treaty/fr/Treaties/Html/108.htm> (page consultée le 01 mars 2006).

[3] Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050, <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=fr&numdoc=31995L0046&model=guichett> (page consultée le 01 mars 2006).

[4] Journal Officiel du 7 août 2004, article 1er, <http://www.cnil.fr/index.php?id=301> (page consultée le 01 mars 2006).

[5] Voir à ce sujet l'article 8 de cette loi qui dispose qu' « : *I. - Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.*

II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I :

1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ;

2° Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle;

6° Les traitements nécessaires 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 mis en oeuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ; […];

8° Les traitements nécessaires à la recherche dans le domaine de la santé selon les modalités prévues au chapitre IX [Traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé].

III. - Si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25 [autorisation de la Commission nationale de l'informatique et des libertés]. Les dispositions des chapitres IX et X [Traitement de données de santé à caractère personnel à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention] ne sont pas applicables.

IV. - De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au I de l'article 25 ou au II de l'article 26.

[6] Même si ces notions réfèrent toutes deux aux informations permettant d'identifier, directement ou non, une personne physique, il convient de préciser, d'une part, que l'expression « données à caractère personnel » est la terminologie retenue par les pays Membres de l'Union européenne en écho à la *Directive 95/46/CE*. D'autre part, l'expression « renseignement personnel » est davantage employé au Canada comme l'illustre la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch.5, <http://www.iijcan.org/ca/loi/p-8.6/tout.html> (page consultée le 01 mars 2006), la *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels*, L.R.Q., c. A-2.1, <http://www.iijcan.org/qc/legis/loi/a-2.1/index.html> (page consultée le 01 mars 2006) et, *la Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q. c. P-39.1, <http://www.iijcan.org/qc/legis/loi/p-39.1/index.html> (page consultée le 01 mars 2006) par exemple.

[7] Richard E. LANGELIER, « Numérisation des dossiers de santé et protection des renseignements personnels, Impératifs techniques, intérêts économiques, considérations politiques et émergence de nouvelles normes », *Lex Electronica*, vol. 9, n°3, Été 2004, p. 2, <http://www.lex-electronica.org/articles/v9-3/langelier.htm> (page consulté le 01 mars 2006). Partant de ce constat, l'auteur préciser qu'au Québec, pour contourner cette situation, le législateur a adopté de nombreux textes, dont la *Loi sur les services de santé et les services sociaux* (L.R.Q., c. S-4.2), instituant un régime d'exception à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

[8] Ainsi, pour la LPRPDÉ, précitée note 9, concernant un individu vivant ou décédé, constitue un renseignement personnel sur la santé : 1) tout renseignement ayant trait à sa santé physique ou mentale; 2) tout renseignement relatif aux services de santé fournis à celui-ci; 3) tout renseignement relatif aux dons de parties du corps ou de substances corporelles faits par lui, ou tout renseignement provenant des résultats de tests ou d'examens effectués sur une partie du corps ou une substance corporelle de celui-ci; 4) tout renseignement recueilli dans le cadre de la prestation de services de santé à celui-ci; 5) tout renseignement recueilli fortuitement lors de la prestation de services de santé à celui-ci.

[9] *Health Information Act*, R.S.A. 2000, c. H-5, <http://www.iijcan.org/ab/laws/sta/h-5/index.html> (page consultée le 01 mars 2006).

[10] *Loi sur la protection des renseignements personnels sur la santé*, L. O. 2004, c. 3, ann. A, <http://www.iijcan.org/on/legis/loi/2004c.3ann.a/index.html> (page consultée le 01 mars 2006).

[11] *Personal Health Information Act*, C.C.S.M., c. P33.5, <http://www.canlii.org/mb/laws/sta/p-33.5/index.html> (page consultée le 01 mars 2006).

[12] *Health Information Protection Act*, S.S. 1999, c. H-0.021, < http://www.iijcan.org/sk/laws/sta/h-0.021/index.html>

[13] Paris, 23 septembre 1980.

[14] La notion de dossier médical personnel a été introduite en droit français par la *Loi n°2004-810 du 13 août 2004 relative à l'assurance maladie* « afin de favoriser la coordination, la qualité et la continuité des soins, gage d'un bon niveau de santé, chaque bénéficiaire de l'assurance maladie dispose […] d'un dossier médical personnel constitué […] notamment des informations qui permettent le suivi des actes et prestations de soins ». Parmi les nombreux

 ISSN 1718-9306

commentaires relatifs à l'établissement d'un tel dossier, voir entre autres : Olivier DUPUY, *La gestion des informations relatives au patient. Dossier médical et dossier médical personnel*, Bordeaux, Les Études Hospitalières, 2005.

[15] Pierre TRUDEL, « La vie privée dans les réseaux de soins au Québec », Conférence donnée lors des activités de l'Institut International de Recherche en Éthique Biomédicale (IIREB), Faculté de droit, Université de Montréal, 20 février 2003. Voir également, Pierre TRUDEL, « La protection de la vie privée dans les systèmes d'information relatifs à la santé. Ajuster les concepts aux réalités des réseaux », dans Christian HERVÉ, Bartha Maria KNOPPERS, Patrick A. MOLINARI, *Les pratiques de recherche biomédicale visitées par la bioéthique*, Paris, Dalloz, 2003, pp. 163 à 176.

[16] LPRPDÉ, précitée note 9, article 3.

[17] Loi 78/17 modifiée en 2004, précitée note 7.

[18] Voir à ce sujet, Pierre TRUDEL, « État de droit et effectivité de la protection de la vie privée dans les réseaux du e-gouvernement », Communication présentée lors du colloque national « Technologies, vie privée et justice », tenu à Toronto par l'Institut canadien d'administration de la justice (ICAJ) du 28 au 30 septembre 2005, <http://www.chairelrwilson.ca/activites/icaj.html> (page consulté le 01 mars 2006); Pierre TRUDEL, «Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage de données personnelles », [2004] 110 *Revue française d'administration publique* 257-266.

[19] Pour illustrer cet état des choses, il est possible de consulter l'article L 161-36-1A du Code de la sécurité sociale. Cet article, créé par la *Loi n°2004-810 du 13 août 2004 relative à l'assurance maladie*, dispose que « deux ou plusieurs professionnels de santé peuvent toutefois, sauf opposition de la personne dûment avertie, échanger des informations … », <http://www.legifrance.gouv.fr/html/actualite/actualite_legislative/decrets_application/2004-810.htm> (page consultée le 01 mars 2006). Il est également possible de lire l'article 19 de la *Loi sur les services de santé et les services sociaux*, modifié par le Projet de loi n°83 sanctionné le 30 novembre 2005, confirmant que « le dossier d'un usager est confidentiel et nul ne peut y avoir accès, si ce n'est avec le consentement de l'usager ou de la personne pouvant donner un consentement en son nom ». Pour une analyse éthique du consentement, voir entre autres : Christian BOUDREAU, Monica TREMBLAY, Bernard DUVAL et Nicole BOULIANNE, « Éthique du consentement à l'ère des réseaux d'information en matière de santé », *in* (2004) 6-2 *Éthique publique. Revue internationale d'éthique sociétale et gouvernementale* 54.

[20] À ce sujet, voir notamment Cynthia CHASSIGNEUX, *Vie privée et commerce électronique*, Montréal, Les Éditions Thémis, 2005.

[21] Les enjeux de l'informatisation du système de santé et des services sociaux nécessitent la révision de plusieurs principes inhérents à la protection des renseignements personnels et à leur circulation. Il en va ainsi notamment des principes relatifs à la collecte, aux finalités, à la transparence, à la qualité des données, à la responsabilité. Pour une démonstration de cette nécessité, voir entre autres : Pierre TRUDEL, « État de droit et effectivité de la protection de la vie privée dans les réseaux du e-gouvernement », *loc. cit.* note 21; Pierre TRUDEL, «Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage de données personnelles », *loc. cit.* note 21; Pierre TRUDEL, « La vie privée dans les réseaux de soins au Québec », *loc. cit.* note 18.

[22] Isabelle DUCLOS, « Qui, quand, pourquoi ? La confidentialité de votre dossier médical », (2005) 30-1 *Justice-Santé. La revue des usagers du réseau de la santé* 6.

[23] Liliane DUSSERRE, *loc. cit.* note 4 pp. 174-176.

[24] *Recommandation n°R(81)1 relative à la réglementation applicables aux banques de données médicales automatisées*, 23 janvier 1981, <http://cm.coe.int/ta/rec/1981/f81r1.htm> (page consulté le 01 mars 2006).

[25] *Recommandation n°R(97)5 relative à la protection des données médicales*, 13 février 1997, <http://cm.coe.int/ta/rec/1997/f97r5.html> (page consultée 01 mars 2006).

[26] Les auteurs de cet article, avec Mmes Mireille Lacroix et Rosario Duaso Calés de l'Université de Montréal, participent au développement de ce projet pancanadien multicentrique visant à la création d'un partenariat regroupant 13 centres de recherche de premier plan collaborant à l'évaluation d'une nouvelle technique pour l'identification d'anomalies chromosomiques chez des enfants souffrant d'un handicap mental grave dont la cause est inconnue. Voir à ce sujet <http://www.crdp.umontreal.ca/fr/activites/biotechnologie/005.html> (page consultée le 01 mars 2006).

[27] INSTITUTS DE RECHERCHE EN SANTÉ DU CANADA, CONSEIL DE RECHERCHES EN SCIENCES NATURELLES ET EN GÉNIE DU CANADA, CONSEIL DE RECHERCHE EN SCIENCES HUMAINES DU CANADA, *Énoncé de politique des trois Conseils : Éthique de la recherche avec des êtres humains*, 1998 (avec les modifications de 2000, 2002 et 2005), <http://www.pre.ethics.gc.ca/francais/policystatement/policystatement.cfm> (page consultée le 01 mars 2006).

[28] *Id*.

[29] Loi 78/17 modifiée en 2004, précitée note 7.

[30] Quant à l'importance du droit d'accès dans la société de l'information, voir entre autres : Herbert BURKERT, « Le droit d'accès en tant que droit de l'homme et l'éthique de la communication », *in* (2004) 6-2 *Éthique publique. Revue internationale d'éthique sociétale et gouvernementale* 42.

[31] Aux termes de l'article L. 1111-7 du Code de la santé publique, il est possible de lire que « toute personne a accès à l'ensemble des informations concernant sa santé détenues par des professionnels et établissements de santé (…) elle peut accéder à ces informations directement ou par l'intermédiaire d'un médecin qu'elle désigne et en obtenir communication (…) ».

[32] À ce sujet, il est possible de lire entre autres : Emmanuelle RIAL-SEBBAG, « Les échanges de données médicales en Europe et vers l'étranger », *in* Anne-Marie DUGUET, *op. cit.* note 4, pp. 155 à 165; A.-M. DUGUET, J. BIGA, S. GUINART-DOUSSET, E. RIAL, « Échanges de données et de fichiers dans la recherche », Anne-Marie DUGUET, *Séminaire d'actualité de droit médical. Réseaux de soins, de santé et de recherche médicale. Aspects légaux et responsabilités. Bilan des expériences*, Bordeaux, Les Études Hospitalières, 2003.