Instituts de recherche en santé du Canada | Canadian Institutes of Health Research

Canada

# Sélection de normes juridiques internationales et étrangères régissant la protection des renseignements personnels dans le contexte de la recherche en santé

IRSC CIHR
Instituts de recherche en santé du Canada | Canadian Institutes of Health Research

Décembre 2001

**Instituts de recherche en santé du Canada**
**410, avenue Laurier ouest**
**Ottawa (Ontario) K1A 0W9**
**www.irsc.ca**

© Travaux publics et Services gouvernementaux Canada, 2001
Nº de cat. MR21–31/2001F–IN
ISBN 0–662–86567–7

Instituts de recherche en santé du Canada | Canadian Institutes of Health Research

Canada

# Sélection de normes juridiques internationales et étrangères régissant la protection des renseignements personnels dans le contexte de la recherche en santé


Décembre 2001

# Survol du document

*(La table able des matières détaillée suit.)*

# Table des matières détaillée

# Liste des abréviations utilisées dans ce rapport

| | |
|---|---|
| AMM | Association médicale mondiale |
| *Avis du Groupe européen d'éthique* | *Avis nº 13 sur les Aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information* |
| BMA | *British Medical Association* [Association médicale britannique] |
| CE | Conseil de l'Europe |
| CEDH | *Convention européenne des droits de l'homme* |
| CEE | Communauté économique européenne |
| *Charte de l'UE* | *Charte des droits fondamentaux de l'Union européenne* |
| CNIL | Commission nationale de l'informatique et des libertés de France |
| *Convention CE 108/1981* | *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* |
| *Convention CE sur les droits de l'homme et la biomédecine* | *Convention de 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.* |
| *Déclaration de l'OMS* | *Déclaration de l'OMS sur la promotion des droits des patients en Europe* |
| *Déclaration de l'UNESCO* | *Déclaration universelle sur le génome humain et les droits de l'homme* |
| *Déclaration universelle* | *Déclaration universelle des droits de l'homme* |
| *Directive de l'UE relative aux données à caractère personnel* | *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* |
| DPA | *Data Protection Act* [Loi sur la protection des données] |
| É.-U. | États-Unis |
| FAQ | Foire Aux Questions |
| HHS | US Department of Health and Human Services [Ministère de la santé et des services sociaux (des États-Unis)] |
| HIPAA | *Health Insurance Portability and Accountability Act* [Loi sur le transfert des régimes d'assurance-maladie et les redditions de compte à leur sujet] |

| | |
|---|---|
| HIPC | *Health Information Privacy Code* [Code sur les renseignements personnels ayant trait à la santé]. |
| HREC | Human Research Ethics Committee [Comité d'éthique pour la recherche sur l'être humain] |
| IPP | The Public Sector Standards: Information Privacy Principles (partie du *Privacy Act* d'Australie) [Principes d'information et de protection de la vie privée, applicables au secteur public] |
| IRSC | Instituts de recherche en santé du Canada |
| Joint NHMRC/AVCC Statement | Joint NHRC/AVCC Statement and Guidelines on Research Practice [Exposé conjoint et Lignes directrices de pratique pour la recherche du National Health and Medical Research Council et de l'Australian Vice-Chancellors' Committee] |
| Lignes directrices de l'OCDE | Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel |
| *Loi nº 78-17* | *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Law 78-17)* |
| *Loi nº 78-18* | *Loi nº 78-18 du 6 janvier 1979 relative aux archives* |
| LPRPDE | *Loi sur la protection des renseignements personnels et les documents électroniques* |
| *Medical Treatment Contract Act* | Wet geneeskundige behandelingsovereenkomst [Loi sur le contrat de traitement médical] |
| MRC | Medical Research Council (UK) [Conseil pour la recherche médicale (du R.-U.)] |
| MRC Guides | *Medical Research Council Guidelines on Research and Personal Data* [Lignes directrices du MRC sur la recherche et les données personnelles] |
| NHMRC | National Health and Medical Research Council of Australia [Conseil national pour la santé et la recherche médicale d'Australie] |
| Normes de l'HIPAA | *Standards for Privacy of Individually Identifiable Health Information* [Normes de protection des renseignements sur la santé d'individus identifiables] |
| NPP | The Private Sector: National Privacy Principles (partie du *Privacy Act* d'Australie) [Principes nationaux de protection de la vie privée, applicables au secteur privé] |
| OCDE | Organisation de coopération et de développement économiques |
| OMS | Organisation mondiale de la Santé |

| | |
|---|---|
| ONU | Organisation des Nations Unies |
| PDPA | *Personal Data Protection Act (Wet bescherming persoonsgegevens)* [Loi sur la protection des données personnelles] |
| PIDCP | *Pacte international relatif aux droits civils et politiques* |
| PIDESC | *Pacte international relatif aux droits économiques, sociaux et culturels* |
| *Principes directeurs de l'ONU* | *Principes directeurs pour la réglementation des fichiers personnels informatisés* |
| *Recommandation R(97) 5 CE* | *Recommandation nº R (97) 5 du comité des ministres aux États membres relative à la protection des données médicales* |
| RHIR | Health Retention of Health Information Regulations (1996) [Règlement sur la conservertion des renseignements sur la santé pour les fins de la santé] |
| R-U | Royaume-Uni |
| UE | Union européenne |
| UNESCO | Organisation des Nations Unies pour l'éducation, la science et la culture |
| US | États-Unis |

# Sommaire

En avril 2000, IRSC (Instituts de recherche en santé du Canada) a publié un *Recueil des dispositions législatives canadiennes sur la protection des renseignements personnels*. La publication de ce recueil s'inscrit dans le cadre d'une contribution plus générale au débat actuel sur la meilleure façon de concilier le droit des individus à la protection de leurs renseignements personnels et l'accès à de tels renseignements par les chercheurs en santé et ce, en vue d'améliorer la santé des Canadiennes et des Canadiens, bonifier les services de santé et renforcer le régime de santé au Canada.

Le présent document se veut un complément au recueil publié en 2000 en donnant une vue d'ensemble des normes internationales de protection des renseignements personnels. Cette perspective internationale permet de situer le Canada dans un contexte mondial. L'analyse des approches retenues par d'autres pays dans ce domaine et l'identification des tendances de la législation de protection du droit à la vie privée peut fournir des modèles dont le Canada pourra s'inspirer, ou qu'il pourra s'efforcer d'éviter à l'heure où il faut aborder d'épineux problèmes.

Ainsi, le rythme croissant de la recherche concertée en santé à l'échelle internationale, les révolutions dans les domaines des technologies de l'information et des communications entre pays, ainsi que les nouvelles lois transnationales sur la protection de la vie privée mondialisent tant la recherche scientifique que les normes internationales sur la protection de la vie privée. Certaines de ces normes internationales influent sur les normes gouvernementales et les politiques publiques canadiennes. De nouvelles lois, tant fédérales que provinciales, font leur apparition. Tandis que la société canadienne évolue dans le sens de l'élaboration et du perfectionnement de ces lois, il peut s'avérer utile de cerner nos points de convergence et nos points de divergence avec d'autres pays avant d'arrêter notre choix sur des normes de protection pour les renseignements personnels au Canada.

La présente étude est sélective, et non exhaustive. Dans une Deuxième partie, l'on décrit l'avènement du droit au respect de la vie privée comme principe de droit international, parallèlement à l'élaboration de droits de la personne et de normes éthiques connexes durant la période qui a suivi la Seconde Guerre mondiale (de 1945 à 1970). Sont examinées dans cette partie les normes résultant des *Procès de Nuremberg* (1947), celles de la *Déclaration universelle des droits de l'homme* de 1948, de la *Convention européenne des droits de l'homme* de 1950, du *Pacte international relatif aux droits civils et politiques* et du *Pacte international relatif aux droits économiques, sociaux et culturels* (des années 60 et 70), ainsi que de la *Déclaration de Genève* de 1949 et des *Déclarations d'Helsinki* de 1964, 1975 et 2000 de l'Association médicale mondiale. Les principes fondamentaux du droit au respect de la vie privée, de la confidentialité et du consentement ont une même fin : la valorisation et la protection de la dignité humaine. Lorsqu'on les applique cependant, ces droits et ces obligations suscitent parfois des dilemmes. Certains des instruments de protection des droits de la personne apparus après la Seconde Guerre mondiale prévoient des normes qui peuvent aider à composer avec la tension qui oppose des valeurs importantes du bien commun et peuvent aider à nuancer les critères permettant de concilier le droit à la vie privée avec d'autres besoins sociétaux. Dans ces instruments, le recours à un critère clair dit de « nécessité » pour justifier les atteintes au droit à la vie privée, conformes à la loi, est recommandé en vue de répondre à des besoins aussi importants que la sécurité publique ou la protection de la santé qui se font de plus en plus sentir en démocratie.

Dans la Troisième partie, on expose les grandes lignes des principes et des règles internationaux contemporains de protection des données personnelles qui ont commencé à apparaître au cours des années 80. Faisant fond sur les normes internationales de protection de la vie privée élaborées au cours de la période allant de 1945 aux années 70, ces principes et ces règles vont plus loin; ils établissent des normes particulières plus

détaillées qui cherchent à établir un juste équilibre entre le droit à la protection de la vie privée et les utilisations sociétales légitimes des renseignements personnels. Sont examinées dans cette Partie les normes proposées par l'Organisation de coopération et de développement économiques (OCDE), par le Conseil de l'Europe, par l'Union européenne (UE) et par l'Organisation des Nations Unies (ONU). Les normes mises de l'avant par chacune de ces organisations ont eu une influence internationale appréciable.

Les principes de 1980 de l'OCDE ont jeté les bases d'un régime conçu pour minimiser les obstacles à la libre circulation transfrontalière des données tout en assurant le respect du droit à la vie privée. Ils ont influencé les instruments internationaux et nationaux ultérieurs de protection des données personnelles et ils ont orienté les délibérations, les politiques et les lois des quelque trente États membres de l'OCDE.

Le Conseil de l'Europe prend aussi depuis longtemps des initiatives dans le domaine, proposant des mesures de protection des données personnelles à l'échelle européenne. Il a adopté une convention générale sur la protection des données et il a défini des normes pour les renseignements médicaux. L'ONU a adopté une variante des principes de l'OCDE en 1990. Elle a ajouté des normes sur le consentement, la confidentialité et la protection des données personnelles dans la *Déclaration universelle sur le génome humain et les droits de la personne*, adoptée en 1997 par l'UNESCO. L'instrument le plus influent des dernières années est sans doute la *Directive de 1995 de l'Union européenne à l'égard du traitement des données à caractère personnel*. La Directive veut harmoniser les normes en obligeant les quinze États membres de l'Union européenne à rendre leur droit national conforme à la Directive. Parce qu'elle est obligatoire et détaillée, et parce qu'elle interdit en règle générale les échanges de données personnelles avec les pays qui n'assurent pas une protection « suffisante » de la vie privée, la Directive a contribué à la réforme des lois de protection des données et de la vie privée dans l'ensemble des pays européens, ainsi qu'en Australie, aux États-Unis et au Canada.

Dans la Quatrième partie, on expose les grandes lignes de certaines lois nationales de protection des données : celles de l'Australie, de la France, des Pays-Bas, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis. Tout comme le Canada, la plupart de ces pays ont récemment révisé leurs lois nationales sur la protection des données personnelles, qui reprenaient ou reflétaient à l'origine les principes initiaux de l'OCDE. L'Australie, à l'échelon fédéral, a récemment modifié son *Privacy Act* (Loi sur la vie privée) par l'ajout de nouvelles normes applicables au secteur privé, en harmonie avec les normes révisées, applicables à la recherche en santé financée au moyen des deniers publics. Sa voisine, la Nouvelle-Zélande, possède un *Privacy Act* similaire. Il autorise le Commissaire à la protection de la vie privée à élaborer des codes de conduite sectoriels, comme la version récemment révisée du *Health Information Privacy Code* (Code de protection des renseignements personnels sur la santé) de 1994. Le Royaume-Uni a récemment procédé, lui aussi, à une mise à jour de son ancienne loi sur la protection des données de manière à la rendre conforme à *la Directive de l'UE relative aux données à caractère personnel*. Le *Medical Research Council* (le Conseil pour la recherche médicale) et la *British Medical Association* (l'Association médicale britannique) ont ajouté à cette loi révisée, pour la compléter, des lignes directrices détaillées concernant l'utilisation des renseignements personnels dans la recherche en santé. Un projet de loi portant révision de la loi française sur la protection des données est présentement à l'étude à l'Assemblée nationale française, bien que la France ait déjà modifié sa loi en 1994 en y ajoutant notamment des dispositions particulières au sujet de la recherche en santé. De même, les Pays-Bas ont déjà adopté une nouvelle loi sur la protection des données. Dans cette partie, on aborde également le droit américain, notamment le *Privacy Act* fédéral de 1974, les nouvelles normes fédérales sur la protection des renseignements sur la santé et la récente réponse américaine à la *Directive de l'UE relative aux données à caractère personnel*.

Pour faciliter la comparaison, le rapport présente ces lois nationales et ces normes internationales en fonction des aspects suivants : *a*) le champ d'application de la loi; *b*) les définitions pertinentes; *c*) les protections spéciales prévues pour les données sensibles; *d*) l'obligation d'obtenir un consentement pour la

collecte, l'utilisation et la communication des données; *e*) les exceptions générales autorisant le traitement sans consentement de données personnelles, en mettant un accent particulier sur les besoins de la recherche; *f*) aspects concernant la conservation et la sécurité des données; *g)* les autres dispositions intéressantes le cas échéant.

Cette analyse comparative des normes étrangères met en relief des tendances et des problèmes qui se posent au regard de l'élaboration des normes canadiennes de traitement des renseignements personnels dans le contexte de la recherche en santé et de leur perfectionnement. Par exemple, les lois sur la protection des données de pays comme le Royaume-Uni, l'Australie et les États-Unis, ainsi que celles en vigueur au sein de l'Union européenne, définissent des termes tels que « renseignements de personnes identifiables », « consentement » et « recherche ». Certaines des législations nationales étudiées définissent également les renseignements sur la santé comme une catégorie de données sensibles appelant des protections et des normes particulières. L'obtention d'un consentement demeure l'exigence d'ordre général requise pour le traitement de ce genre de renseignements.

Dans des circonstances exceptionnelles, certaines lois et normes autorisent le traitement sans consentement de données personnelles dans des cas particuliers où cette utilisation vise à répondre à d'autres besoins sociétaux pressants. Dans de nombreux cas, ces exceptions incluent expressément la recherche statistique ou scientifique. Les critères précis de l'exception varient d'un pays à l'autre. Généralement, il doit être démontré que le traitement sans consentement de renseignements de personnes identifiables est nécessaire aux fins de la recherche effectuée, obtenir le consentement des personnes concernées doit être objectivement à peu près impossible, des mesures de sécurité adéquates doivent être prises pour protéger la confidentialité et la vie privée des dites personnes concernées, et le traitement des données doit se limiter au minimum nécessaire en fait d'étendue, de durée et de conservation.

Par ailleurs, en Australie et en Nouvelle-Zélande, par exemple, la loi prévoit expressément des processus publics coordonnés entre la Commission fédérale de protection de la vie privée et le ministre de la Santé aux fins de l'élaboration de normes détaillées et de codes de conduite pour le secteur de la santé conformes au droit fédéral sur la protection de la vie privée.

# I. Introduction

Le présent document s'ajoute au *Recueil des dispositions législatives canadiennes sur la protection des renseignements personnels dans le contexte de la recherche en santé* (avril 2000) publié par IRSC (Instituts de recherche en santé du Canada)[1]. Dans la préparation de ce recueil, IRSC s'est inspirée des tendances récentes et des importants progrès accomplis en ce domaine, récapitulant les normes internationales régissant la protection des renseignements personnels.

L'importance accrue de la collaboration internationale dans la recherche menée dans le domaine de la santé, la véritable révolution marquant les technologies de l'information et des communications, et de nouvelles législations transnationales sur la protection des renseignements personnels, favorisent la mondialisation, tant de la recherche scientifique que des normes internationales de protection des renseignements personnels. Il est clair que certaines de ces normes internationales influencent les normes gouvernementales et les politiques canadiennes. Non seulement, donc, le Canada a-t-il en tout cela un intérêt, mais il doit en outre assumer pleinement son rôle et ses responsabilités s'il veut pouvoir lui-même influer sur les nouvelles tendances qui s'expriment dans le monde.

Parallèlement à cette évolution internationale, le Parlement du Canada a récemment promulgué de nouvelles normes fédérales dans le cadre de la *Loi sur la protection des renseignements personnels et les documents électroniques*[2] *(LPRPDE)*; les provinces et les territoires devraient bientôt en faire autant et adopter des lois semblables pour l'essentiel. Les normes adoptées dans ce domaine s'appliquent aussi bien au gouvernement qu'aux universités, aux chercheurs, aux détenteurs et aux utilisateurs des renseignements en question, ainsi qu'aux personnes spécialisées dans l'analyse des politiques publiques et enfin, à l'ensemble des citoyens. Le Canada entend donc parfaire sa législation en ce domaine, d'où la pertinence de mieux comprendre dans quelle mesure elle se rapproche ou s'écarte de celle des autres pays.

Ce document recense et analyse les normes et les approches, établies et nouvelles, de la communauté internationale en matière de protection des renseignements personnels sur la santé. Dans certains cas, elles s'écartent de la pratique canadienne et, dans certains autres, ce sont à peu près les mêmes. Cette étude examine essentiellement les normes juridiques internationales et étrangères pouvant être comparées aux lois fédérales régissant la protection de la vie privée, la protection des données et la confidentialité. Seront en outre examinées certaines normes éthiques, déontologiques et gouvernementales en raison de leur influence sur les politiques publiques nationales et internationales. L'étude se veut sélective plutôt qu'exhaustive, non seulement en ce qui concerne les pays étudiés, mais également à l'échelle de ces pays, car il s'agit surtout de citer les exemples qui nous paraissent les plus pertinents.

Cette introduction donne un aperçu général de l'étude. Les Deuxième et Troisième parties ont trait aux normes adoptées principalement par diverses organisations intergouvernementales, dont les Nations Unies (l'ONU), l'Organisation de coopération et de développement économiques (l'OCDE), l'Union européenne (l'UE) et le Conseil de l'Europe (le CE). Ces normes sont énoncées dans des instruments juridiques interna-

---

1 *Instituts de recherche en santé du Canada, Recueil des dispositions législatives canadiennes sur la protection des renseignements personnels dans le contexte de la recherche en santé,* Travaux publics et Services gouvernementaux du Canada, Ottawa, 2000.

2 *Loi sur la protection des renseignements personnels et les documents électroniques, L.C. (2000), ch. 5 (LPRPDE).* Site Web : http://www.privcom.gc.ca

tionaux, anciens et récents, et dans des déclarations d'adoption de politiques publiques ou de formulation de principes d'éthique. Dans une Quatrième partie sont étudiées les approches retenues dans certains pays : l'Australie, la France, le Royaume-Uni (R.-U.), les Pays-Bas, la Nouvelle-Zélande, et les États-Unis (É.-U.).

Afin de faciliter l'analyse comparative, l'état du droit dans chacun de ces pays est exposé en considérant les questions suivantes :

a. *Champ d'application* : La loi ou la politique est-elle applicable au secteur public, au secteur privé ou à des organismes particuliers?

b. *Définitions** : Quelle est la définition donnée de termes tels que « renseignements personnels », « renseignements personnels sur la santé », « traitement des données » et « consentement », si tant est que ces termes soient définis? (Notons que dans l'étude, l'expression « traitement des données » fait en général référence à la collecte, à l'utilisation et à la communication de données. Toutefois les directives et les lois applicables dans certains pays peuvent retenir, pour « traitement des données » une définition différente.)

c. *Protections spéciales : données sensibles* : Les renseignements personnels sur la santé relèvent-ils du régime général de protection des renseignements personnels ou font-ils l'objet de dispositions particulières?

d. *Consentement : collecte, utilisation et communication des données* : Quelles normes régissent le consentement à la collecte, à l'utilisation ou à la communication des renseignements personnels et des renseignements personnels sur la santé?

e. *Exceptions et recherche* : A-t-on prévu des exceptions particulières pour la collecte, l'utilisation ou la communication de renseignements personnels aux fins de la recherche?

f. *Conservation et sécurité des données* : Les normes applicables imposent-elles des procédures particulières pour assurer la sauvegarde des données, impartissant des délais de conservation ou fixant les conditions d'élimination de celles-ci?

g. *Autres dispositions intéressantes* : La loi ou la politique étudiée contient-elle d'autres dispositions intéressantes, novatrices ou utiles?

Précisons qu'en général les informations recueillies l'ont été avant la fin du mois de mai 2001.

* N.d.T. : Dans cette version française de l'étude, les termes définis sont repris de la version française de la LPRPDE ou sont d'usage courant au Canada dans les milieux spécialisés.

# II. Les principes internationaux généraux de protection de la vie privée appliqués après la Seconde Guerre mondiale (de 1945 aux années 70).

Dans cette partie, nous étudierons les principes de protection de la vie privée, leur développement et leur évolution; ces principes, adoptés immédiatement après la Seconde Guerre mondiale, émanent principalement du droit international sur les droits de la personne. Plusieurs normes juridiques internationales régissant ce domaine remontent d'ailleurs à cette époque. Elles constituent les fondements des règles et des principes internationaux de protection des données personnelles actuels.

## A. Les grands principes hérités de Nuremberg : la dignité de la personne humaine, le consentement et le respect de la vie privée dans le contexte de la recherche

Si le respect de la vie privée est devenu un principe fondamental en droit international contemporain régissant les droits des personnes, c'est en partie en réponse aux excès et aux atrocités commis au cours de la Seconde Guerre mondiale. En 1945, la communauté internationale a réagi en créant l'Organisation des Nations Unies, proclamant « la dignité et la valeur de la personne humaine » et s'engageant à respecter et à défendre les libertés fondamentales[3].

Par ailleurs, des médecins, des scientifiques et d'autres qui, à l'instigation des nazis, s'étaient livrés à des expériences médicales sur des prisonniers de guerre sans obtenir le moindre consentement[4] furent traduit en justice. Les procès de Nuremberg mettant en accusation, pour crimes contre l'humanité, des médecins et des chercheurs, s'achevèrent à l'été de 1947. Dans son arrêt, le tribunal énonça ce qui allait devenir le *Code de Nuremberg*, dégageant les principes fondamentaux qu'il fallait respecter en matière d'expérimentation médicale impliquant des êtres humains pour répondre aux exigences de la morale, de l'éthique et du droit[5]. Dans ce Code, on trouve un certain nombre de principes qui concernent les objectifs de la recherche, les risques et les bénéfices pour les personnes qui y participent, les obligations incombant aux chercheurs et les qualifications exigées d'eux. Mais le principe fondamental énoncé était : « le consentement libre du sujet humain est absolument essentiel ». Le tribunal de Nuremberg ayant principalement insisté sur le caractère volontaire de toute participation à la recherche sur des sujets humains, on ne trouve rien dans le Code sur la protection de la vie privée et de la confidentialité. Néanmoins, le Code appartient à cette série de grands instruments sur les droits internationaux de la personne élaborés dans la période qui a suivi la Seconde Guerre mondiale, partageant un même esprit, les mêmes procédures et les mêmes fins de défense de la dignité humaine qui ont contribué à définir les normes internationales de base de la recherche sur des sujets humains.

---

3 Nations Unies, *Charte des Nations Unies*, Préambule, Conférence de San Francisco des Nations Unies, juin 1945.

4 *Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No. 10.*, volume 2. Washington, DC: U.S. Government Printing Office, 1949, p. 181-182.

5 Annas G.J., Grodin M.A. *The Nazi Doctors and the Nuremberg Code: Human Rights in Human Experimentation.* New York: Oxford University Press, 1992. pp. 94-104.

À la vérité, dans les six mois qui ont suivi les jugements de Nuremberg sur les expériences médicales sur des sujets humains, l'Association médicale mondiale, les Nations Unies et les gouvernements européens adoptèrent chacun pour leur part divers instruments juridiques et déclarations solennelles sur la question. Il s'agissait de promouvoir la dignité de la personne humaine, en partie en s'engageant à respecter la liberté et l'autonomie individuelles, et la vie privée et la confidentialité. Chacun de ces grands engagements, à la fois moraux et juridiques, a donc contribué à sa façon — directement ou indirectement — à une volonté collective de faire de la vie privée et de l'autonomie des principes fondamentaux garantissant le respect de la dignité des êtres dans la recherche contemporaine. Dans les pages suivantes, on trouvera des extraits pertinents de ces documents.

## B. La *Déclaration universelle des droits de l'homme* de 1948

Quelques mois seulement après l'achèvement des procès de Nuremberg, l'Assemblée générale des Nations Unies adopta et proclama la *Déclaration universelle des droits de l'homme (Déclaration universelle)*[6]. La *Déclaration universelle*, c'est la reconnaissance par la communauté internationale des droits essentiels de la personne et son engagement à les défendre. Le préambule prévoit en effet « qu'il est essentiel que les droits de l'homme soient protégés par un régime de droit » et il donne certains des motifs qui sous-tendent cette affirmation :

> Considérant que la méconnaissance et le mépris des droits de l'homme ont conduit à des actes de barbarie qui révoltent la conscience de l'humanité (…). Considérant que dans la Charte [des Nations Unies] les peuples des Nations Unies ont proclamé à nouveau leur foi dans les droits fondamentaux de l'homme, dans la dignité et la valeur de la personne humaine (…).

Les trente articles de la *Déclaration universelle* couvrent un éventail très étendu de questions et ne lient pas juridiquement. Certains cependant ont acquis le caractère d'obligations juridiques par le fait de leur inclusion dans le droit international général des droits de la personne et dans les traités assurant la protection des données.

Au moins trois articles de la *Déclaration universelle* introduisent des éléments de base, des principes et des textes de la protection des données qui apparaîtront des dizaines d'années plus tard. Ainsi l'article 27 selon lequel « toute personne a le droit de prendre part librement (…) et de participer au progrès scientifique et aux bienfaits qui en résultent ». Cet article traduit un des intérêts et une des motivations sociétaux fondamentaux qui sous-tendent la recherche contemporaine menée dans le domaine des sciences de la santé.

L'article 12 de la *Déclaration universelle* fait de la protection de la vie privée un des droits fondamentaux de la personne en prévoyant que « nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ». Les dispositions législatives adoptées au cours des dernières décennies pour assurer la protection de la vie privée sont parfaitement conformes à l'article 12. Mais que se passerait-il si d'autres

[6] Assemblée générale des Nations Unies, *Déclaration universelle des droits de l'homme*, New York, Nations Unies, Adoptée par l'Assemblée générale dans sa résolution 217A(III) du 10 décembre 1948. Site Web : http://www.unhchr.ch/udhr/lang/frn.htm

principes ou d'autres valeurs exprimés dans la *Déclaration universelle* — et donc d'autres intérêts sociétaux — se trouvaient à être en conflit ou à porter atteinte au droit à la vie privée? Le texte de l'article 12 serait là encore utile car il n'interdit que les « immixtions arbitraires ». Cela veut dire que certaines immixtions pourraient être permises.

L'article 29 de la *Déclaration universelle* peut lui aussi se révéler utile en cas de conflits éventuel de ce genre. Il prévoit en effet la manière dont certains droits fondamentaux de la personne peuvent parfois subir certaines limites :

> Dans l'exercice de ses droits et dans la jouissance de ses libertés, chacun n'est soumis qu'aux limitations établies par la loi exclusivement en vue d'assurer la reconnaissance et le respect des droits et libertés d'autrui et afin de satisfaire aux justes exigences de la morale, de l'ordre public et du bien-être général dans une société démocratique.

Ce principe voulant que toute limitation imposée doit nécessairement être établie par une loi visant exclusivement à assurer la reconnaissance d'autres principes démocratiques fondamentaux, anticipe sur les normes et les procédures qui permettent à la communauté internationale de concilier, comme elle s'y est engagée, la protection de la vie privée et un certain nombre de besoins sociétaux importants. Ces éléments seront repris et précisés dans des textes ultérieurs tels la *Convention européenne des droits de l'homme*.

## C. La *Convention européenne des droits de l'homme* de 1950

Deux ans après la *Déclaration universelle* des Nations Unies, le Conseil de l'Europe (CE) reprit certaines des normes qui y étaient énoncées, afin de faire de la protection de la vie privée un principe fondamental du droit international, dans la *Convention de sauvegarde des droits de l'homme et des libertés fondamentales* (ou, succinctement, Convention européenne des droits de l'homme : *CEDH*)[7]. Fondé par un traité conclu en 1949 à titre d'organisation intra-européenne de défense des droits de la personne, le CE regroupait au départ quelque dix pays. Aujourd'hui, la *CEDH* est en vigueur dans les quelque quarante États membres du CE qui l'ont adoptée[8]. Ces États se trouvent tenus de veiller à ce que leur droit interne se conforme aux principes de la *CEDH.*

S'inspirant de la *Déclaration universelle,* l'article 8 de la *CEDH* reconnaît le droit au respect de la vie privée et prévoit les limites pouvant y être apportées :

> Toute personne a droit au respect de sa vie privée et familiale (…) Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

---

7 Conseil de l'Europe. *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*. Rome, 4 novembre 1950. S.T.E. nº 5, 213 R.T.N.U. 222. Site Web : http://conventions.coe.int/Treaty/fr/cadreprincipal.htm

8 États membres : l'Albanie, l'Allemagne, Andorre, l'Arménie, l'Autriche, la Belgique, la Bulgarie, Chypre, la Croatie, le Danemark, l'Espagne, l'Estonie, la Fédération de Russie, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Islande, l'Italie, la Lettonie, le Liechtenstein, la Lituanie, le Luxembourg, l'ex-République yougoslave de Macédoine, Malte, la Moldavie, la Norvège, les Pays-Bas, la Pologne, le Portugal, la République tchèque, la Roumanie, le Royaume-Uni, la Russie, Saint-Marin, la Slovaquie, la Slovénie, la Suède, la Suisse, la Turquie et l'Ukraine.

Si l'article 8 de la *CEDH* reprend l'essentiel des articles 12 et 29 de la *Déclaration universelle*, et même plusieurs de leurs termes, il y apporte certaines précisions importantes. Il prévoit notamment que toute ingérence doit être à la fois prévue par la loi et « nécessaire » dans une société démocratique. La *CEDH* prévoit en outre, comme motifs d'ingérence explicites, la « protection de la santé ou de la morale », motifs qui viennent s'ajouter aux autres limitations de la vie privée qui peuvent se révéler nécessaires dans une société démocratique. Nous verrons, dans la Troisième partie, que, des dizaines d'années plus tard, les textes et les principes internationaux de protection des données reprendront ces deux critères de la nécessité et de la protection de la santé.

La *CEDH* a également contribué à faire de la protection de la vie privée un droit international de la personne effectif. Aux termes du traité, l'individu habitant un des États membres du CE peut, s'il estime qu'une loi ou pratique nationale est contraire au droit à la vie privée de l'article 8, en appeler au CE. Après avoir épuisé les voies de recours judiciaires ouvertes dans son pays, il peut porter plainte pour violation des droits de la personne et saisir la Cour européenne des droits de la personne du CE. De litiges en litiges sur la communication irrégulière de données personnelles sur la santé, la Cour a dégagé un commencement d'interprétation de cet aspect du droit à la vie privée. Elle a rappelé que « la protection des données à caractère personnel (…) revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale (…); par conséquent, 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 seraient pas conformes aux garanties prévues à l'article 8 de la *CEDH* »[9]. Les arrêts judiciaires de ce genre montrent bien quel rôle jouent les tribunaux dans l'effort sociétal de définition de normes de collecte, d'utilisation et de communication des données personnelles sur la santé respectueuses de l'intimité des êtres.

## D. Les Pactes internationaux (1966 et 1976)

### Le *Pacte international relatif aux droits civils et politiques* et le *Pacte international relatif aux droits économiques, sociaux et culturels* de 1966 (entrés en vigueur en 1976)

C'est en 1966 que l'ensemble de la communauté internationale a officiellement intégré au droit international, à titre de principe fondamental, le respect de la vie privée. L'Assemblée générale des Nations Unies adopta et ouvrit à la signature le *Pacte international relatif aux droits civils et politiques* (*PIDCP*)[10]. La même année, l'ONU adoptait un texte lui faisant pendant : le *Pacte international relatif aux droits économiques, sociaux et culturels* (*PIDESC*)[11]. Ces deux pactes, qui sont des traités internationaux liant les États qui y sont parties, entendaient donner juridiquement effet aux principes proclamés dans la *Déclaration universelle*, les développer et les mettre en oeuvre. Ils sont entrés en vigueur en 1976. Ils ont été signés et ratifiés par plus de cent quarante pays.

---

9 Cour européenne des droits de l'homme, Recueil des arrêts et décisions, Affaire *M.S. c. Suède*, 27 août 1997, par. 41. Voir également l'affaire *Z. v. Finland*, 25 février 1997, 45 B.M.L.R.107.

10 Nations Unies, Assemblée générale, résolution 2200A, en date du 16 septembre 1966 : *Pacte international relatif aux droits civils et politiques*, adopté et ouvert à la signature, à la ratification et à l'adhésion. R.T.C. 1976 nº 47, 999 R.T.N.U. 171. Site Web : http://www.unhchr.ch/french/html/menu3/b/a_ccpr_fr.htm

11 Nations Unies, Assemblée générale, résolution 2200A (XXI), en date du 16 décembre 1966 : *Pacte international relatif aux droits économiques, sociaux et culturels*, adopté et ouvert à la signature, à la ratification et à l'adhésion.

Au moins trois des articles des Pactes devaient revêtir une importance directe pour les règles et les principes de protection internationale des données ultérieurs. Ces trois articles ont trait à la vie privée, au consentement, à la recherche et à la santé.

D'abord l'article 17 du *PIDCP* décrit le droit à la vie privée : « Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée (…). Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ». L'article reprend donc mot pour mot l'article 12 de la *Déclaration universelle.* Par contre, à l'inverse de l'article 29 de la *Déclaration universelle* et de l'article 8 de la *CEDH*, le *PIDCP* ne prévoit aucune norme régissant les limitations susceptibles d'être apportées au droit à la protection de la vie privée.

Ensuite, à l'inverse aussi bien de la *Déclaration universelle* que de la *CEDH*, le *PIDCP* rend juridiquement effectif le *Code de Nuremberg*. Ainsi l'article 7 prévoit qu' « il est interdit de soumettre une personne sans son libre consentement à une expérience médicale ou scientifique ».

Enfin les articles 15 et 12 du *PIDESC* incluent respectivement, dans l'énumération des droits sociaux, le droit que toute personne a « de bénéficier du progrès scientifique et de ses applications » et « du meilleur état de santé physique et mentale qu'elle soit capable d'atteindre ». Tout cela est tiré de la *Déclaration universelle.* L'article 15 prévoit, en outre, que les États qui adhèrent au *PIDESC* « s'engagent à respecter la liberté indispensable à la recherche scientifique ».

Qu'il convienne ou non d'accorder à ces deux dispositions du *PIDESC* concernant la santé et la recherche scientifique, une importance égale à celle des droits au respect de la vie privée et au consentement reconnus par le *PIDCP*, la reprise de ces quatre principes, dans les années 70, par divers traités internationaux atteste la pertinence et l'importance accordées à la protection et à la défense de la dignité de l'être humain. À partir des années 70, ce sera aux règles applicables en matière de vie privée et aux principes de protection des données qu'il reviendra de préciser les normes, les définitions, les structures et les procédures permettant d'établir un juste équilibre entre la protection de la vie privée et un usage légitime des données personnelles aux fins de la recherche en santé.

## E. La *Déclaration de Genève* de 1948 et la *Déclaration d'Helsinki* de 1964 (révisée en 1975 et en 2000)

L'Association médicale mondiale (AMM), fondée en 1947, est une association internationale qui s'est donné pour mission de promouvoir, auprès des médecins, le respect de normes internationales élevées de comportement professionnel. Au cours des années, l'Association s'est acquittée de cette tâche par l'adoption de déclarations et de résolutions officielles. Trois revêtent une importance particulière en ce qui a trait aux normes internationales régissant la vie privée et la recherche.

D'abord, en 1948, six mois environ après l'achèvement des procès de Nuremberg, l'AMM a adopté la *Déclaration de Genève*[12]. La *Déclaration de Genève* est un serment que prête le médecin; ultérieurement l'AMM l'a repris dans son *Code de déontologie médicale*. La *Déclaration de Genève* commence par un engagement solennel, celui de se mettre au service de l'humanité. Elle articule ensuite plusieurs responsabilités, y compris l'obligation de « respecter les secrets qui me sont

[12] Association médicale mondiale. *Déclaration de Genève : Le serment médical*, modifié, Genève, 1948.

confiés, au-delà même du décès du patient ». Cette obligation posthume de confidentialité allait d'ailleurs être reprise dans les directives adoptées en 1990 par les Nations Unies sur la protection des données.

La seconde déclaration de l'AMM qui nous concerne en l'occurrence est venue plus d'un quart de siècle après la *Déclaration de Genève* de 1948. En 1964, en effet, l'AMM a adopté une déclaration détaillée de principes éthiques pour la recherche médicale, texte qui se fit connaître sous le nom de *Déclaration d'Helsinki*[13]. Faisant écho aux principes dégagés par le Code de Nuremberg, la *Déclaration d'Helsinki* insistait largement sur les protocoles de recherches médicales, sur l'obligation d'évaluer correctement les risques et sur la question du consentement éclairé des sujets humains faisant l'objet des recherches. La Déclaration de 1964 ne disait rien, en effet, sur les questions de vie privée ou de confidentialité. Mais, lorsqu'en 1975, la *Déclaration d'Helsinki* fut amendée, on ajouta une disposition prévoyant expressément que : « Le droit du sujet à la protection de son intégrité doit toujours être respecté. Toutes précautions doivent être prises pour respecter la vie privée du sujet (…) ». La révision de cette déclaration, en 2000, conserve cette disposition mais y ajoute une obligation plus générale : « Dans la recherche médicale, le devoir du médecin est de protéger la vie, la santé, la dignité et l'intimité de la personne ».[14] La *Déclaration d'Helsinki*, du moins depuis le milieu des années 70, montre bien que la protection de la vie privée et le principe du consentement éclairé revêtent une importance essentielle lorsqu'il s'agit de préserver l'intégrité et la dignité des sujets humains. Ce sont dorénavant des principes internationaux d'éthique médicale reconnus régissant toute recherche. Cette reprise de l'obligation de protection de la vie privée et du consentement dans les documents internationaux ayant trait à l'éthique de la recherche effectuée sur des sujets humains fait pendant à la reconnaissance officielle de ces normes dans le *PIDCP*, qui d'ailleurs date de la même époque.

Rétrospectivement, une troisième déclaration de l'AMM permet peut-être d'expliquer l'amendement apporté en 1975 à la *Déclaration d'Helsinki* afin d'inclure expressément le respect de la vie privée dans le contexte de la recherche médicale. Cet amendement faisait suite aux résolutions adoptées par l'AMM en 1973 sur la protection de la vie privée. Après avoir réfléchi aux avantages et aux inconvénients de l'utilisation des ordinateurs en médecine lors de son assemblée de 1973, l'AMM avait adopté des résolutions affirmant à nouveau, entre autres, l'« importance essentielle de respecter le secret professionnel du médecin (…) afin de garantir la protection de la vie privée de l'individu, cela étant à la base même de cette relation de confiance existant entre le patient et son médecin »[15]. Cette résolution établissait un lien direct entre l'obligation de protection de la vie privée et l'obligation professionnelle de confidentialité. Aujourd'hui, dans sa version amendée, cette *Déclaration sur l'utilisation des ordinateurs en médecine*[16] tente de concilier le respect de la confidentialité, proclamé nécessaire dans la *Déclaration de Genève* de l'AMM, et les exigences de la recherche en santé, à laquelle peut contribuer le traitement électronique des données. Selon cette déclaration : « Il n'y a pas de violation du secret professionnel lorsque des informations confidentielles concernant

---

13 Association médicale mondiale. *Déclaration d'Helsinki : Recommandations à l'adresse des médecins dans le domaine de la recherche médicale sur des sujets humains.* Helsinki, 1964; art. III.4a. Site Web : http://www.wma.net

14 Association médicale mondiale. *Déclaration d'Helsinki : Principes éthiques applicables aux recherches médicales sur des sujets humains.* Édimbourg, 2000; articles B.10 et B.21. Site Web : http://www.wma.net/f/policy/17-c_f.html

15 The 27th World Medical Assembly: Munich, October 14–20, 1973, 2 *World Med. J.*, 1974, pp.4-10.

16 Association médicale mondiale. *Déclaration sur l'utilisation des ordinateurs en médecine*, fondée sur la résolution adoptée par la 27e assemblée médicale mondiale, Munich (Allemagne), octobre 1973, amendée par la 35e assemblée médicale mondiale, Venise (Italie), octobre 1983.

les soins de santé sont diffusées ou transmises dans le but de servir à la recherche scientifique (…) pour autant que l'information diffusée ne révèle pas directement ou indirectement, l'identité du patient dans aucun des rapports sur ladite recherche (…) ni ne dévoile l'identité des patients de quelque façon que ce soit (…) ». Les détails et définitions contenus dans cette *Déclaration sur l'utilisation des ordinateurs en médecine* sont la caractéristique des premiers principes et règles de protection des données adoptés au cours des années 70 et 80.

# III. Les règles et principes internationaux contemporains de protection des données (de 1980 à aujourd'hui).

Dans cette partie, un aperçu des règles et des principes internationaux de protection des données développés à partir des années 80 est donné. Par ces règles et ces principes, fondés sur les normes internationales initialement définies entre 1945 et les années 70 pour assurer le respect de la vie privée, on a recherché, par l'établissement de normes spécifiques et détaillées, un juste équilibre entre divers usages sociétaux légitimes des renseignements personnels et le respect du droit à la vie privée. Plusieurs de ces normes de protection des données s'inspirent des principes généraux dégagés au début des années 80. Depuis, divers pays ont voulu les préciser et les appliquer à des domaines particuliers, dont la recherche utilisant des renseignements. Parmi les normes dont il est fait état dans les pages qui suivent, l'on compte celles de l'Organisation de coopération et de développement économiques, du Conseil de l'Europe, de l'Union européenne et des Nations Unies.

## A. L'Organisation internationale de coopération et de développement économiques (l'OCDE)

### 1. Les principes de 1980 de l'OCDE régissant la protection des données de caractère personnel

Créée en 1960 par un traité international, l'Organisation internationale de coopération et de développement économiques (l'OCDE) dégagea, en 1980, une série de principes de protection des données qui devaient avoir une influence considérable. Parmi ces principes, que l'on retrouve dans les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (*les *Lignes directrices de l'OCDE)*[17] de l'Organisation, l'on compte les suivants :

- Le principe de limitation en matière de collecte;
- Le principe de qualité des données;
- Le principe de spécification des finalités;
- Le principe de limitation de l'utilisation;
- Le principe des garanties de sécurité;
- Le principe de transparence;
- Le principe de participation individuelle;
- Le principe de responsabilité.

Ces principes ont exercé une influence certaine sur les textes internationaux et nationaux ultérieurs de protection des données, ainsi que sur les délibérations, les politiques publiques et les lois des quelque trente pays membres de l'OCDE[18]. Selon la préface des *Lignes directrices*

[17] OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, (Paris : OCDE, 1981). Site Web : http://www1.oecd.org/dsti/sti/it/secur/prod/priv-fr.html

[18] Sont membres : l'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, la Corée, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Islande, l'Italie, le Japon, le Luxembourg, le Mexique, la Norvège, la Nouvelle-Zélande, les Pays-Bas, la Pologne, le Portugal, la République slovaque, la République tchèque, le Royaume-Uni, la Suède, la Suisse, la Turquie. Site Web : www.oecd.org

*de l'OCDE*, environ la moitié des États membres de l'Organisation avaient adopté ou étaient sur le point d'adopter, lorsque parurent les *Lignes directrices de l'OCDE*, des lois de protection de la vie privée. Les *Lignes directrices de l'OCDE* ne lient pas juridiquement. Elles cherchent plutôt à préciser quel est le consensus international sur les principes de protection des données tel que permet de le constater la législation des États membres. En cherchant à élaborer des lignes directrices en vue de l'harmonisation des lois nationales de protection de la vie privée et des données en pleine évolution, les *Lignes directrices de l'OCDE*, selon la préface, relevaient un défi : prévenir les violations des droits fondamentaux de la personne pouvant résulter de l'archivage illicite ou de l'utilisation ou de la communication non autorisées de données personnelles sans, toutefois, faire obstacle au libre mouvement, légitime, des données personnelles à travers les frontières internationales et entre des économies nationales qui, de plus en plus, dépendent de la technologie de l'information et des communications. Voici un aperçu des *Lignes directrices de l'OCDE.*

### a. Champ d'application

Les normes des *Lignes directrices de l'OCDE* s'appliquent aux données personnelles dans les secteurs public et privé. Selon l'article 2, ces normes s'appliquent uniquement aux données qui, compte tenu de leur nature, du contexte dans lequel elles sont utilisées ou de leur mode de traitement, « comportent un danger pour la vie privée et les libertés individuelles ».

### b. Définitions

Selon la définition donnée à l'article premier des *Lignes directrices de l'OCDE*, on entend par « données de caractère personnel (…) toute information relative à une personne physique identifiée ou identifiable ». Ce qu'on entend par « personne identifiable » n'est toutefois pas précisé. Cependant, le paragraphe 43 de l'exposé des motifs précise bien que sont exclues les données qui ne permettent pas d'identifier, notamment les données statistiques ou anonymes.

### c. Protections spéciales : données sensibles

Contrairement aux normes internationales de protection des données personnelles en vigueur à l'époque et adoptées depuis, les *Lignes directrices de l'OCDE* ne prévoient aucune mesure de protection spécifique pour les diverses catégories de données, tels les renseignements personnels sur la santé. L'article 3 des *Lignes directrices de l'OCDE* précise qu'elles ne doivent pas être interprétées comme interdisant l'élaboration de « mesures de protection différentes ». Dans l'Exposé des motifs accompagnant les *Lignes directrices de l'OCDE*, on relève que leurs auteurs se sont penchés sur la question des données sensibles. On y doute cependant qu'il y ait unanimité au sujet du caractère sensible de certaines catégories de données, et l'on se demande si les individus appartenant à certaines catégories (par exemple, les personnes affectées d'un handicap mental) et les données sensibles exigent effectivement des mesures de protection supplémentaires (voir les paragraphes 19 à 32). Dans les vingt années suivantes, par contre, d'autres organisations internationales ont eu tendance à adopter des normes qui levaient de tels doutes en privilégiant une protection renforcée des données sensibles.

### d. Consentement : collecte, utilisation et communication des données

Les *Lignes directrices de l'OCDE* exigent le consentement, considéré comme un élément de base de toute collecte de données personnelles. Énonçant le principe de limitation de collecte de données, l'article 7 prévoit que la collecte des données personnelles doit s'effectuer par des moyens licites et loyaux « et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement ». Le principe de limitation de collecte des données fonctionne de concert avec d'autres principes proches. Les articles 8 à 10 des *Lignes directrices de l'OCDE*

posent également les principes de « spécification des finalités», de « qualité des données » et de « limitation de l'utilisation ». Ces normes, prises dans leur ensemble, veulent donc dire que seules des données pertinentes et exactes doivent être recueillies, à des fins précises et limitées, et que leur communication et utilisation doivent se limiter aux objectifs initiaux, si ce n'est avec le consentement de la personne concernée ou en vertu de quelque autorisation légale. La nécessité du consentement ou de l'autorisation légale permet donc de protéger la vie privée tout en autorisant la collecte, l'utilisation et la communication légitimes des renseignements personnels.

### e. Exceptions et recherche

L'article 4 des *Lignes directrices de l'OCDE* éclaire sur les exceptions qui peuvent être faites aux obligations générales de protection des données. Aux termes de cet article, les exceptions à ces obligations générales pour des raisons de sécurité nationale ou d'ordre public devraient être « aussi peu nombreuses que possible » et « portées à la connaissance du public ». Ces dispositions semblent traduire une double intention : d'abord, donner une large étendue à la protection de la vie privée tout en évitant des exceptions nombreuses et injustifiées contraires aux fins mêmes pour lesquelles une telle protection est recherchée et aux valeurs qui les sous-tendent; ensuite, assurer la transparence et la publicité de ces exceptions de manière à ce qu'elles puissent faire l'objet des examens, des débats et des demandes que l'on rende compte qui sont de règle dans une société démocratique.

Quoiqu'il n'en soit pas question expressément dans les principes eux-mêmes, le paragraphe 47 de l'Exposé des motifs des *Lignes directrices de l'OCDE* précise qu'elles ont été rédigées en présumant que « les exceptions se limiteront à celles qui s'imposent dans une société démocratique ». Les *Lignes directrices de l'OCDE* ne portent pas sur la recherche en santé ni sur la recherche scientifique, et elles ne prévoient aucune exception particulière pour la recherche en santé.

### f. Conservation et sécurité des données

Selon l'article 11 des *Lignes directrices de l'OCDE*, il faut comprendre par principe des garanties de sécurité le fait que les données personnelles doivent être protégées « grâce à des garanties de sécurité raisonnables » contre les risques de destruction ou de perte accidentelle ou contre l'accès, la modification ou la communication non autorisés. Ainsi que l'explique le paragraphe 56 de l'Exposé des motifs, on entend notamment par garanties raisonnables de sécurité les mesures d'ordre matériel de contrôle d'accès, les mesures structurelles telles que les codes de conduite s'adressant des institutions recueillant de telles données, et des mesures de la technologie informationnelle telles que le chiffrement. Les *Lignes directrices de l'OCDE* ne fixent aucun délai pour la conservation des données. Le principe de limitation, qui confine la collecte des données à des fins spécifiques et limitées, semble impliquer que la durée de conservation des données dépendra de la question de savoir si cette conservation continue à être justifiée par rapport aux finalités spécifiées[19].

### g. Autres dispositions intéressantes

Les *Lignes directrices de l'OCDE* encouragent les États à prendre des initiatives, tant au niveau national qu'international, afin d'assurer la confidentialité des données personnelles.

---

[19] Organisation de coopération et de développement économiques (OCDE). *Exposé des motifs, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, par. 54 et 55. Paris : OCDE, 1981. Site Web : http://www1.oecd.org/dsti/sti/it/secur/prod/priv-fr.html

Dans les limites de leur territoire respectif, les États sont encouragés à instaurer des procédures ou à établir des institutions juridiques ou administratives. Cela veut notamment dire que l'on devrait s'efforcer de mettre en place une législation adaptée, de favoriser l'autodiscipline et de fournir aux individus les moyens raisonnables de faire valoir leurs droits, en prévoyant en outre les sanctions et les voies de recours appropriées et veillant à ce que ne se produise aucune discrimination injuste.

Pour favoriser la mise en oeuvre internationale, les États membres sont priés de coopérer les uns avec les autres afin de faciliter le libre mouvement des données personnelles et de définir les restrictions légitimes possibles. Ce défi exige effectivement de parvenir à un certain équilibre. D'une part, l'article 18 prie instamment les États membres de ne pas restreindre de manière indue la circulation transfrontalière des données par la création de normes de protection de la vie privée excessives. Par ailleurs, l'article 17 donne aux États membres la faculté de limiter les flux transfrontaliers entre leur territoire et celui d'un autre pays en raison de la nature des données et du manque de « protection équivalente » dans l'autre pays. Comme beaucoup de concepts et de principes des *Lignes directrices de l'OCDE*, l'idée de protection équivalente est devenue, une vingtaine d'années plus tard, la norme juridique de base en matière de législation et de politique de protection internationale des données.

## B. Le Conseil de l'Europe (CE)

Tel qu'indiqué en C de la deuxième partie, le Conseil de l'Europe a été fondé vers la fin des années 40 en tant qu'organisation intra-européenne de défense des droits de la personne[20]. Venant compléter les dispositions de la *CEDH* sur la protection de la vie privée, au moins trois documents du CE précisent les normes retenues en matière de protection des données personnelles en santé à l'époque actuelle. Il s'agit de la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* de 1981 (la *Convention 108/1981 du CE*), de la *Recommandation concernant la protection des données médicales* de1997 *(la Recommandation R(97)5 du CE)* et de la *Convention 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* de 1997 *(la Convention du CE sur les droits de l'homme et la biomédecine).*

### 1. La *Convention de 1981 du CE pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*

En 1981, après de premiers efforts, au début des années 70, de protection de la vie privée dans le contexte des banques de données électroniques, le CE a ouvert à la signature la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (la *Convention 108/1981 du CE*)[21]. À l'instar des *Lignes directrices de l'OCDE*, ce document s'attaque à un problème sociétal fondamental. Selon les termes de son préambule, il

[20] États membres : l'Albanie, l'Allemagne, Andorre, l'Arménie, l'Autriche, la Belgique, la Bulgarie, Chypre, la Croatie, le Danemark, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Islande, la Lettonie, le Liechtenstein, la Lituanie, le Luxembourg, l'ex-République yougoslave de Macédoine, Malte, la Moldavie, la Norvège, les Pays-Bas, la Pologne, le Portugal, la Roumanie, le Royaume-Uni, la Fédération de Russie, Saint-Marin, la Slovaquie, la Slovénie, la Suède, la Suisse, la République tchèque, la Turquie et l'Ukraine.

[21] Conseil de l'Europe. *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, R.T.E. nº 108. Strasbourg, 28 janvier 1991. Site Web : http://conventions.coe.int/Treaty/FR/Treaties/Html/108.htm

s'agit de concilier les « valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples ». À l'inverse des *Lignes directrices de l'OCDE*, par contre, la *Convention 108/1981 du CE* constitue un traité international liant les États qui y sont parties. Les vingt pays européens qui l'ont adoptée sont tenus d'harmoniser leurs lois afin de donner effet aux principes qui y sont énoncés. Les pays qui ne sont pas membres du CE peuvent également adhérer à la *Convention 108/1981 du CE*, dont nous allons maintenant exposer les grands traits.

### a. Champ d'application

En vertu de l'article 3 de la *Convention 108/1981 du CE*, celle-ci s'applique aux fichiers et aux traitements automatisés des données personnelles. L'article laisse aux États membres la faculté d'en étendre les principes aux fichiers de données personnelles ne faisant pas l'objet de traitements automatisés. Dans la mesure, cependant, où elle ne s'applique strictement qu'aux traitements automatisés des données, cette convention a un champ d'application plus restreint que celui des *Lignes directrices de l'OCDE*. Par contre, comme celles-ci, elle s'applique à la fois au secteur public et au secteur privé.

### b. Définitions

À l'instar des *Lignes directrices de l'OCDE*, la *Convention 108/1981 du CE*, à son article premier, définit « données à caractère personnel » comme étant « toute information concernant une personne physique identifiée ou identifiable ». La notion de personne physique identifiable n'est cependant pas définie. Et il faut entendre par « traitement automatisé » les opérations suivantes, effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion.

### c. Protections spéciales : données sensibles

La *Convention 108 /1981 du CE*, à son article 6, prévoit des mesures de protection supplémentaires pour les « catégories particulières de données ». Elle s'éloigne en cela des *Lignes directrices de l'OCDE*. En effet, la *Convention 108/1981 du CE* prévoit que les données personnelles révélant l'origine raciale, les convictions religieuses et celles 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 ». Il n'est pas élaboré et aucun exemple n'est donné pour illustrer ce qu'il conviendrait d'entendre par « garanties appropriées ». En ce qui concerne le traitement des données sensibles, le texte n'exige pas de manière explicite que l'on obtienne le consentement de l'intéressé avant de traiter la donnée sensible. La *Convention 108/1981 du CE* exige, cependant, qu'une protection spéciale soit apportée aux données personnelles sensibles. En cela, elle fixe une norme qui sera reprise par la suite par d'autres organisations dans leur élaboration de règles internationales de protection des données.

### d. Consentement : collecte, utilisation et communication des données

En ce qui concerne les données personnelles générales ou non sensibles, l'article 5 prévoit que ces données personnelles doivent en général être obtenues loyalement et traitées licitement, enregistrées pour des finalités déterminées et légitimes et être à la fois exactes, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées. À l'inverse des *Lignes directrices de l'OCDE*, ces dispositions générales ne prévoient expressément aucune obligation d'obtenir le consentement éclairé des personnes dont l'information personnelle est traitée. Une obligation expresse d'obtention du consentement peut cependant être prévue par le droit interne.

### e. Exceptions et recherche

L'article 9 de la *Convention 108/1981 du CE* prévoit certaines exceptions aux obligations générales de protection des données. Alors que les *Lignes directrices de l'OCDE* portaient que les exceptions devaient être « aussi peu nombreuses que possible », la *Convention 108/1981 du CE* dit, elle, que les exceptions doivent être « nécessaires », et être à des fins sociétales démocratiques aussi impératives que la protection de la sécurité de l'État, de la sûreté publique ou de la répression de l'activité criminelle. La *Convention 108/1981 du CE* ne dit rien sur le traitement des données effectué à des fins de recherche. Notons cependant que, selon l'article 9.3, la loi d'un pays membre peut restreindre l'exercice des droits que peut avoir une personne, de consultation ou de correction des données personnelles des fichiers automatisés utilisées à des fins d'analyse statistique ou de recherche scientifique lorsqu' « il n'existe manifestement pas de risques d'atteinte à la vie privée des personnes concernées ».

### f. Conservation et sécurité des données

Selon l'article 7 de la *Convention 108/1981 du CE*, des « mesures de sécurité appropriées » doivent être prises pour la protection des données personnelles contre la destruction ou la perte accidentelles et contre la consultation, la modification ou la communication non autorisées. Cela fait penser aux *Lignes directrices de l'OCDE*. L'article 5 e) porte que des données qui permettent d'identifier le sujet ne doivent pas être conservées plus longtemps qu'il n'est nécessaire pour les fins pour lesquelles elles sont enregistrées. Cette disposition rappelle la motivation qui sous-tend tacitement les *Lignes directrices de l'OCDE* au regard de la durée de conservation des données personnelles.

### g. Autres dispositions intéressantes

La *Convention 108/1981 du CE* contient en outre d'importantes dispositions en vue de sa mise en oeuvre nationale et internationale. L'article 12 contient des dispositions analogues à celles des *Lignes directrices de l'OCDE*; il autorise les restrictions applicables aux transferts internationaux de données à des pays dont les normes de protection de la vie privée n'accordent pas de « protection équivalente ». En ce qui concerne la mise en oeuvre interne, l'article 10 impose aux États de prévoir des « sanctions et recours appropriés » pour les violations des lois nationales de réception des principes de la *Convention 108/1981 du CE*. À l'inverse, cependant, des principes plus récemment adoptés de protection des données personnes par les Nations Unies et l'Union européenne (voir en C et D de la Troisième partie, plus bas), la *Convention 108/1981 du CE* ne comportait au départ aucune exigence précise concernant l'instauration d'autorités de contrôle de la protection des données. C'est pourquoi il a récemment été proposé d'amender la *Convention 108/1981 du CE*[22]. L'amendement exigerait des États parties qu'ils constituent des autorités indépendantes de contrôles qui seraient chargées de veiller au respect de la législation ou de la réglementation qu'ils auraient adoptées en exécution de la *Convention 108/1981 du CE*. Enfin les articles 18 et 19 de la *Convention 108/1981 du CE* prévoient la création d'un comité consultatif chargé, entre autres choses, de proposer des réformes et de répondre aux demandes écrites faites au sujet de la *Convention 108/1981 du CE*. Le projet d'amendement concernant l'établissement d'autorités nationales de contrôle est en partie dû aux délibérations de ce comité consultatif.

[22] Conseil de l'Europe. *Projet de protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (RTE nº 108) concernant les autorités de contrôle et les flux transfrontières de données*. Strasbourg, 2000. Site Web : http://stars.coe.fr/ta/TA00/fopi217.htm

## 2. La *Recommandation de 1997 du CE relative aux données médicales*

Dans le but de préciser les principes généraux inscrits dans la *Convention 108/1981 du CE* et de les adapter aux besoins particuliers de divers secteurs de la société, le CE a, au cours des ans, proposé un certain nombre de recommandations. Celles-ci visaient par exemple les banques de données médicales (1981), les recherches statistiques et scientifiques (1983), les transferts de données effectuées par des organismes publics (1991) et les données traitées à des fins statistiques (1997). Ces recommandations n'avaient aucune force obligatoire en droit. Il s'agissait simplement, de la part du CE, de demander aux États membres d'envisager, de bonne foi, de mettre en oeuvre une législation conforme aux applications et aux interprétations de la Convention qu'il recommandait. À ce titre, ces recommandations établissent des normes de référence détaillées concernant des aspects particuliers de la protection des données au profit de la communauté des États membres du CE. En 1997, le CE a ainsi adopté la *Recommandation R(97)5 relative à la protection des données médicales (la Recommandation R(97)5 du CE)*[23] qui porte de façon assez détaillée sur la recherche médicale. Plusieurs de ses dispositions s'inspirent des *Lignes directrices de l'OCDE*, de la *Convention 108/1981 du CE* et de la *Directive 95/46/CE 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* (la *Directive de l'UE relative aux données à caractère personnel).*

### a. Champ d'application

Selon l'article 2 de la *Recommandation R(97)5 du CE*, ce texte s'applique à la collecte et au traitement automatisé des données médicales. Son champ d'application, ainsi limité, est donc encore plus étroit que celui des *Lignes directrices de l'OCDE* et de la *Convention 108/1981 du CE*. Cet article offre aux États membres la faculté d'en étendre ses principes au traitement non automatisé. À l'instar des *Lignes directrices de l'OCDE* et de la *Convention 108/1981 du CE*, cette recommandation s'applique au secteur public et au secteur privé.

### b. Définitions

La *Recommandation R(97)5 du CE* contient notamment des définitions de ce qu'il faut entendre par données personnelles, personnes physiques identifiables et données médicales. À l'instar de la *Convention 108/1981 du CE* et des *Lignes directrices de l'OCDE*, on entend par (à l'article premier) « données à caractère personnel (…) toute information concernant une personne physique identifiée ou identifiable ». Contrairement à la *Convention 108/1981 du CE* et aux *Lignes directrices de l'OCDE*, la *Recommandation R(97)5 du CE* donne également, encore à son article premier, la définition de ce qu'on doit entendre par une personne identifiable, c'est-à-dire que : « une personne physique n'est pas considérée comme identifiable si cette identification nécessite des délais et des activités déraisonnables ». Et, toujours aux termes de l'article premier, on entend par données médicales les « données à caractère personnel relatives à la santé d'une personne ». Il s'agit de données ayant un lien manifeste et étroit avec la santé et des données génétiques.

### c. Protections spéciales : données sensibles

La *Recommandation R(97)5 du CE* s'inspire explicitement de l'article 6 de la *Convention 108/1981 du CE*. L'article 6 prévoit des mesures de protection spéciales pour les données personnelles sur la santé. La *Recommandation R(97)5 du CE* part des raisons qui sont à la base

[23] Conseil de l'Europe. *Recommandation nº R(97)5 du Comité des ministres aux États membres relative à la protection des données médicales*. Strasbourg, 1997. Site Web : http://cm.coe.int/ta/rec/1997/f97r5.html

de cet article et en tire un exposé détaillé de normes particulières. La *Recommandation R(97)5 du CE* établit même certaines normes pour des sous-ensembles de données médicales telles que les données génétiques.

### d. Consentement : collecte, utilisation et communication des données

À l'instar de la *Convention 108/1981 du CE* et des *Lignes directrices de l'OCDE*, l'article 4 prévoit que le traitement des données médicales doit, en général, être effectué de manière loyale et licite, et uniquement pour des finalités déterminées. À l'inverse de la *Convention 108/1981 du CE*, cependant, la *Recommandation R(97)5 du CE* fait du consentement une condition explicite du traitement des données médicales, comme les *Lignes directrices de l'OCDE* et la *Directive de l'UE relative aux données à caractère personnel*. Selon l'article 4.3 de la *Recommandation R(97)5 du CE*, les données médicales peuvent être recueillies et traitées s'il y a eu consentement ou, en l'absence de consentement, si la loi l'autorise. Le consentement peut être donné : a) soit par la personne concernée; b) soit par son représentant légal; c) soit par quelque autre autorité légalement reconnue. D'après l'article 6, pour être valable, le consentement doit être « libre, exprès et éclairé ». L'article 5 énumère les éléments d'information minimaux qui doivent être communiqués à la personne concernée pour qu'elle puisse plus facilement donner un consentement éclairé. L'article 8 établit des normes analogues de communication et de divulgation.

### e. Exceptions et recherche

La *Recommandation R(97)5 du CE* établit également des normes applicables à l'utilisation sans consentement des données médicales, y compris en matière de recherche. À l'instar d'autres textes, les dérogations prévues sont généralement conçues et définies de manière restrictive, et fondées sur un critère de nécessité qui rend compte de divers intérêts sociétaux opposés, parfois supérieurs. Les articles 4 et 7 définissent des normes spécifiquement applicables à la « collecte » sans consentement et à la « communication » des données médicales. Bien que ce qu'il convient d'entendre par « communication » ne soit pas défini, ce sont la communication ou le partage des données médicales qui sont visés. Les articles 4 et 7 prévoient tous les deux que les données médicales peuvent être recueillies et communiquées sans consentement lorsque « la loi le prévoit » aux fins de la santé publique, de la prévention de dangers réels ou d'autres intérêts d'ordre public importants semblables. Les données peuvent également être recueillies ou communiquées « si la loi le prévoit » notamment aux fins du respect d'une obligation contractuelle, de la constatation, de l'exercice ou de la défense d'un droit en justice, pour la sauvegarde des intérêts vitaux d'une personne ou à des fins thérapeutiques, au profit de la personne qui fait l'objet des données ou d'un parent de la lignée génétique. Ces dispositions énoncent des normes analogues à celles de la *Directive de l'UE relative aux données à caractère personnel*.

Outre ces dernières dispositions, la *Recommandation R(97)5 du CE* détaille également certains devoirs et dérogations particuliers applicables à l'utilisation de données médicales à des fins de recherche. Ainsi, l'article 12 prescrit un devoir général obligeant de s'assurer de l'anonymat des données médicales utilisées. L'utilisation de données médicales non anonymes est autorisée à certaines conditions. Il faut démontrer que le projet de recherche s'impose « dans un but légitime » et que l'anonymisation rendrait « impossible » le projet. Une fois démontrées la légitimité des buts et l'impossibilité de procéder avec des données anonymes, les données peuvent être utilisées : a) avec le consentement de la personne concernée ou de son représentant légal; b) avec l'autorisation d'une autorité ou instance régulièrement désignée par la loi en vertu de certains critères; c) lorsque la recherche s'impose pour des raisons de santé publique

et qu'elle est autorisée par la loi. En accord avec la *Convention 108/1981 du CE*, l'article 8.2 de la *Recommandation R(97)5 du CE* limite le droit général d'accès d'une personne aux données médicales la concernant qui sont utilisées à des fins de recherche scientifique ou statistique « lorsqu'il n'existe manifestement pas de risques d'atteinte » à la vie privée.

### f. Conservation et sécurité des données

L'article 9 de la *Recommandation R(97)5 du CE* reprend, d'une manière générale, les normes de sécurité élémentaires prévues par la *Convention 108/1981 du CE* et les *Lignes directrices de l'OCDE*. De plus, l'article 9 prévoit une série de « mesures appropriées » qui doivent faire l'objet d'un réexamen périodique pour l'assurance de la confidentialité et de l'exactitude des données traitées. Il s'agit notamment de mesures de contrôles de mémoire, de communication, de transport, de saisie et d'utilisation des données, ainsi que du traitement de séparation des identifiants des données administratives, sociales et médicales.

En accord avec la *Convention 108/1981 du CE* et les *Lignes directrices de l'OCDE*, l'article 10 de la *Recommandation R(97)5 du CE* crée une obligation générale en vertu de laquelle les données médicales ne doivent être conservées que pendant la durée nécessaire pour atteindre le but pour lequel elles ont été recueillies. Cette obligation générale souffre deux dérogations : d'abord, s'il se révèle « nécessaire » de conserver des données notamment dans l'intérêt légitime de la santé publique, de la science médicale ou à des fins historiques ou statistiques, « en tenant compte de la vie privée du patient »; ensuite, les demandes d'effacement de données médicales identifiant les auteurs de ces demandes doivent en général être honorées, à moins que « des intérêts supérieurs et légitimes » ne s'y opposent et justifient leur conservation. Les données rendues anonymes n'ont pas à être détruites.

### g. Autres dispositions intéressantes

À part le traitement automatisé des données médicales, qui représente son principal centre d'intérêt, la *Recommandation R(97)5 du CE* contient quelques autres dispositions dignes de mention. D'abord, elle doit remplacer la *Convention 108/1981 du CE* relative aux banques de données médicales automatisées, et traduire une pensée davantage proche des évolutions récentes, notamment des initiatives analogues prises par l'UE, telle qu'en témoigne la *Directive de l'UE relative aux données à caractère personnel* (voir en C.1 plus bas). Ensuite, selon la *Recommandation R(97)5 du CE*, en règle générale, les flux transfrontières de données médicales entre les États membres du CE doivent dépendre de l'assurance, par l'État de destination, d'une « protection équivalente » aux dispositions et principes de la *Recommandation R(97)5 du CE*. Il reste à savoir si cette norme de la « protection équivalente » aux dispositions de la *Recommandation R(97)5 du CE* sera pour l'essentiel analogue, ou si au contraire, elle s'écartera de la norme de la « protection équivalente » également prévue par les *Lignes directrices de l'OCDE* et la *Directive de l'UE relative aux données à caractère personnel* (voir en C.1 plus bas).

## 3. La *Convention de 1997 du CE 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*

Dans les années 90, le CE a été parmi les premières organisations internationales à tenter d'élaborer un traité en bonne et due forme sur la protection des droits de la personne face aux « rapides développements de la biologie et de la médecine ». Cette initiative s'inspirait des principes hérités de la *Déclaration universelle* et de la *CEDH* et voulait élever les structures conceptuelles juridiques qui permettraient de promouvoir la dignité de la personne humaine dans la société contemporaine. En 1997, la *Convention de 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 (*la *Convention du CE sur les droits de l'homme et la biomédecine)*[24] a été ouverte à la signature. Plus de la moitié des quarante et un États membres du Conseil ont signé cette Convention. Elle est également ouverte aux États non membres, tels l'Australie, le Canada, le Japon et les États-Unis qui ont, au Comité directeur sur la bioéthique du CE, le statut d'observateurs.

Au moins quatre de ces dispositions portent d'une manière générale sur la recherche en santé et la protection de la vie privée. En premier lieu, l'article 15 énonce pour principe que la recherche scientifique dans le domaine de la biologie et de la médecine s'exercera librement sous réserve des dispositions de la *Convention du CE sur les droits de l'homme et la biomédecine* et des autres instruments juridiques qui « assurent la protection de l'être humain ». En second lieu, l'article 16 énonce un certain nombre de normes générales qui régiront la recherche sur l'être humain. Il s'agit notamment de l'approbation des travaux, sur le plan de la pertinence scientifique et sur le plan éthique, par une instance indépendante, de l'exigence du consentement libre et éclairé des personnes concernées, de la procédure d'obtention du consentement, de la nécessité d'informer la personne se prêtant à une recherche de ses droits et des garanties prévues par la loi pour sa protection. Ces droits et mesures de protection sont ensuite exposés plus en détail dans des dispositions particulières sur le consentement libre et éclairé et la protection de la vie privée. En troisième lieu, un article de la *Convention du CE sur les droits de l'homme et la biomédecine* vise expressément la protection de la vie privée. L'article 10 porte que « toute personne a droit au respect de sa vie privée s'agissant des informations relatives à sa santé ». En quatrième lieu enfin, ce même article précise que le droit à la protection de la vie privée comprend le droit de choisir soit d'être informé de toute information recueillie sur sa santé, soit au contraire, de ne pas l'être. La *Convention du CE sur les droits de l'homme et la biomédecine* ne contient aucune disposition explicite concernant la protection des données, mais elle renvoie à la *Convention 108/1981 du CE*. Davantage de précision pourrait ressortir d'amendements apportés à la *Convention du CE sur les droits de l'homme et la biomédecine* sous forme de protocoles additionnels. Des protocoles portant généralement sur des questions plus précises ont déjà été élaborés au sujet du clonage et des greffes d'organes. D'autres sont en cours d'élaboration pour la recherche médicale et la génétique.

## C. L'Union européenne (UE)

Créée par un traité international dans les années 50, la Communauté économique européenne (la CEE) a dès le départ favorisé et harmonisé les lois et les politiques régissant les relations économiques, le commerce et le développement en Europe. Certaines de ses politiques d'harmonisation ont exercé une influence directe sur le développement des sciences ainsi que sur la recherche et la santé publique. Relevons à titre d'exemple les initiatives poursuivies pendant des années par la CEE pour parfaire l'harmonisation du droit des brevets, notamment en matière pharmaceutique. Avec la conclusion d'un nouveau traité en 1990, la CEE a changé de nom, elle est devenue l'Union européenne et a vu sa mission s'élargir. Celle-ci s'étendra dorénavant explicitement au domaine de

[24] Conseil de l'Europe. *Convention 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,* R.T.E. nº 164. Oviedo, 1997. Site Web : http://conventions.coe.int/Treaty/FR/CadreListeTraites.htm

la santé. L'UE réunit quelque quinze pays européens[25]. Les États membres sont tenus d'harmoniser leur législation avec les directives de l'UE et divers autres textes juridiques qui les lient. À l'égard d'une grande partie de l'Europe, l'UE s'est donc vu reconnaître des pouvoirs, des rôles et des responsabilités analogues à ceux d'un gouvernement fédéral. Les rôles qui lui incombent en matière intereuropéenne sont pour la plupart exercés par l'intermédiaire du Parlement européen, de la Cour européenne de justice, du Conseil européen et de la Commission européenne.

Dans ce contexte, entre 1995 et 2000, l'UE a adopté trois grands instruments fixant les principes de la protection des données personnelles en santé. Il s'agit de : 1) la *Directive de l'UE relative aux données à caractère personnel* de 1995; 2) l'*Avis sur l'utilisation des données personnelles de santé dans la société de l'information* de 1999; 3) la *Charte des droits fondamentaux de l'Union européenne* de 2000.

## 1. La *Directive de l'Union européenne de 1995 relative aux données à caractère personnel*

La *Directive 95/46/CE 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* (la *Directive de l'UE relative aux données à caractère personnel)* est entrée en vigueur en 1998[26]. Les États membres sont tenus de mettre leur droit interne en conformité avec les principes énoncés dans la *Directive de l'UE relative aux données à caractère personnel* dans les trois ans suivant l'adoption de cette directive. Pour ce faire, ils peuvent utiliser tout moyen qui leur semble adapté, lois, règlements, décrets, etc. La *Directive de l'UE relative aux données à caractère personnel* a entraîné, dans de nombreux pays européens, y compris la Grèce, l'Italie, le Portugal, la Suisse, le Royaume-Uni, l'Allemagne, l'Autriche, la Belgique, l'Espagne, le Danemark, la Finlande et les Pays-Bas, l'adoption de nouvelles lois sur la protection des données, ou la révision des législations déjà en place. La *Directive de l'UE relative aux données à caractère personnel* vise le même double objectif que les *Lignes directrices de l'OCDE* et la *Convention 108/1981 du CE* : 1) protéger le droit fondamental à la vie privée lors du traitement des données personnelles; 2) et faciliter, par l'harmonisation, la libre circulation de ces données entre les États membres.

### a. Champ d'application

Selon son article 3, la *Directive de l'UE relative aux données à caractère personnel* s'applique au traitement des données personnelles, automatisé ou non. Elle a ainsi le même champ d'application que les *Lignes directrices de l'OCDE* et donc une portée plus large que la *Convention 108/1981 du CE*. À l'instar des *Lignes directrices de l'OCDE* et de la *Convention 108/1981 du CE*, la *Directive de l'UE relative aux données à caractère personnel* s'applique aux données détenues aussi bien par le secteur public que par le secteur privé.

---

[25] Les États membres de l'Union européenne étaient, au printemps 2001 : l'Allemagne, l'Autriche, la Belgique, le Danemark, l'Espagne, la Finlande, la France, la Grèce, l'Irlande, l'Italie, le Luxembourg, les Pays-Bas, le Portugal, le Royaume-Uni et la Suède. L'élargissement de l'Union est en cours.

[26] *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, Journal officiel* n° L 281 , 23/11/1995, p. 0031 - 0050. Site Web : http://europa.eu.int/eur-lex/fr/lif/dat/1995/fr_395L0046.html

### b. Définitions

En son article 2, la *Directive de l'UE relative aux données à caractère personnel*, tout comme les *Lignes directrices de l'OCDE*, définit l'expression « données à caractère personnel » comme étant « toute information concernant une personne physique identifiée ou identifiable ». À l'inverse, cependant, des *Lignes directrices de l'OCDE* et de la *Convention 108/1981 du CE*, la *Directive de l'UE relative aux données à caractère personnel* raffine la définition des termes « personne qui peut être identifiée » en précisant que cette identification peut se faire « 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 ». Selon l'article 2 de la *Directive de l'UE relative aux données à caractère personnel*, le « traitement » comprend notamment la collecte, l'enregistrement, la consultation, l'utilisation, la diffusion, la modification ou la destruction de données personnelles.

### c. Protections spéciales : données sensibles

À l'instar de la *Convention 108/1981 du CE* et à l'inverse des *Lignes directrices de l'OCDE*, la *Directive de l'UE relative aux données à caractère personnel* prévoit explicitement des normes plus exigeantes pour le traitement de « catégories particulières de données », notamment en ce qui concerne les renseignements sur la santé de personnes identifiables. Cela est en partie assuré par l'imposition d'une interdiction générale de toute collecte de données sur la santé, sous réserve de certaines dérogations strictement définies. L'article 8 dispose expressément que les États membres de l'UE « interdisent le traitement des données à caractère personnel relatives à la santé et à la vie sexuelle » à moins que la personne concernée n'ait librement donné son consentement explicite et informé. Nous verrons, plus loin, en e. de la section 1, les dérogations très précises à cette obligation générale d'obtention du consentement.

### d. Consentement : collecte, utilisation et communication des données

En ce qui concerne le traitement des données personnelles d'ordre général, la *Directive de l'UE relative aux données à caractère personnel* fixe des principes régissant la qualité des données et des normes relatives au consentement. L'article 6 prévoit notamment que les données personnelles doivent de manière générale être : a) traitées loyalement et licitement; b) recueillies pour des finalités déterminées, explicites et légitimes; c) adéquates et pertinentes. Ces dispositions concordent avec les principes adoptés à l'origine par l'OCDE en matière de contrôle de la qualité, mais comportent quelques innovations, certaines mineures et d'autres plus importantes.

Par exemple, la *Directive de l'UE relative aux données à caractère personnel* renforce le principe de finalité des *Lignes directrices de l'OCDE*, qui exige un objectif déterminé et légitime, en ajoutant l'obligation que cet objectif soit en outre « explicite ». Cette exigence permet du moins théoriquement aux personnes concernées de donner, en ce qui concerne la collecte et l'utilisation des données personnelles les concernant, un consentement plus détaillé, plus précis et plus éclairé. Cette exigence est complétée par les articles 11 à 13, qui prévoient que la personne dont on recueille les données doit recevoir davantage d'information au sujet de son droit d'accès et de rectification des données et de celui d'être informée des types de données recueillies. La *Directive de l'UE relative aux données à caractère personnel* aussi renforce la norme de consentement applicable à la collecte des données personnelles. Alors que, selon les *Lignes directrices de l'OCDE*, la collecte des données exige la connaissance et le consentement de la personne concernée « le cas échéant », la *Directive de l'UE relative aux données à caractère personnel* pose, en matière de consentement, des exigences de base plus claires. Plus précisément, l'article 7 prévoit que les données personnelles ne peuvent être traitées que si « la personne concernée a indubitablement donné son consentement », sous réserve des cas de nécessité, définis explicitement

(voir à la section e. qui suit). Selon la définition qu'en donne l'article 2 de la *Directive de l'UE relative aux données à caractère personnel*, il faut entendre par consentement « toute manifestation de volonté, libre, spécifique et informée » visant le traitement de données personnelles.

### e. Exceptions et recherche

La *Directive de l'UE relative aux données à caractère personnel* prévoit trois catégories de dérogations fondées sur le critère de la nécessité — c'est-à-dire qu'il faut que les dérogations soient manifestement nécessaires à la réalisation d'un intérêt sociétal concurrent supérieur. Ce critère reprend en fait la norme de nécessité de la *Convention 108/1981 du CE* et des *Lignes directrices de l'OCDE*.

En premier lieu, l'article 7 pose qu'en l'absence du consentement de la personne concernée, lorsqu'il s'agit de données personnelles d'ordre général, il faut démontrer qu'il est nécessaire de les traiter, notamment pour respecter une obligation légale au titre du droit interne, ou pour sauvegarder les intérêts de la personne concernée, ou afin d'exécuter une mission d'intérêt public.

En second lieu, l'article 8 prévoit, en matière de consentement, des règles précises ainsi que des dérogations pour le traitement des données sensibles telles que les renseignements personnels sur la santé.

Selon l'article 8, outre les conditions générales qui doivent être respectées lors du traitement des données personnelles d'ordre général, il existe des conditions particulières applicables au traitement exceptionnel non consenti des données sur la santé, conditions qui exigent que l'on démontre la nécessité, en avançant un « motif d'intérêt public important », tel que l'exercice ou la défense d'un droit en justice, ou les fins thérapeutiques, notamment les fins de diagnostics, ou l'administration de soins ou de traitements, ou la gestion de services de santé. Les avantages que la recherche scientifique peut apporter à la société persuaderont peut-être certains États européens d'appliquer à la recherche en santé la dérogation prévue pour les missions d'intérêt public en raison de sa nécessité pour l'avancement des recherches biomédicales, épidémiologiques, génomiques et, en général, de tout ce qui concerne la santé publique. Il conviendrait, malgré tout, en l'absence de consentement, que le traitement de données sur la santé de personnes identifiables respecte, même dans le cadre de la recherche, la norme renforcée de protection de la vie privée prévue à l'article 8 de la *Directive de l'UE relative aux données à caractère personnel* et que les données sur la santé ne soient traitées que par des personnes contraintes au secret médical, ou plus généralement, à un devoir de confidentialité.

En troisième lieu enfin, l'article 13 prévoit que les États peuvent assortir d'un certain nombre d'exceptions leurs mesures législatives sur les normes de qualité des données, l'information qui doit être donnée aux personnes dont les données sont recueillies et les droits de consultation et de rectification de ces personnes, mais seulement lorsque cela s'avère nécessaire aux fins de sauvegarder la défense, l'administration de la justice pénale, ou un intérêt économique ou financier important d'un État membre. Bien qu'en ce qui a trait à la recherche scientifique, la *Directive de l'UE relative aux données à caractère personnel* ne prévoit aucune exception expresse pour le traitement non consenti de données personnelles d'ordre général ou de données sur la santé, l'article 13 dispose que des lois internes comportant des protections adéquates peuvent restreindre les droits d'accès et de rectification des données personnelles de la personne concernée, et ce uniquement à des fins de recherche scientifique, s'il « n'existe manifestement

aucun risque d'atteinte à la vie privée de la personne concernée ». Ceci correspond à l'exception prévue par la *Convention 108/1981 du CE*.

### f. Conservation et sécurité des données

Selon l'article 17 de la *Directive de l'UE relative aux données à caractère personnel*, les États doivent prendre des « mesures techniques et d'organisation appropriées » afin de protéger les données contre toute destruction ou perte accidentelles, ainsi que contre tout accès, modification ou communication non autorisés. Il s'agit de normes analogues à celles retenues par l'OCDE. Cet article demande de mettre en balance diverses considérations, de tenir compte même des facteurs coût et des facteurs technologiques, estimant que le niveau de sécurité devrait être proportionné aux risques causés par la nature des données et par leur traitement. Comme la *Convention 108/1981 du CE*, l'article 6 e) de la *Directive de l'UE relative aux données à caractère personnel* prévoit que les données sur des personnes identifiables ne doivent être conservées que pendant la durée nécessaire à la réalisation des finalités pour lesquelles elles sont recueillies. Selon l'article 6 e) également, les États membres sont en outre priés de prévoir des garanties appropriées pour les données personnelles conservées, à des fins statistiques ou scientifiques, pour des périodes plus longues.

### g. Autres dispositions intéressantes

La *Directive de l'UE relative aux données à caractère personnel* contient en outre plusieurs dispositions touchant la mise en oeuvre au niveau national, au niveau de l'UE et au niveau international. Ainsi, les États membres sont tenus de faire en sorte que leur législation nationale comporte des mécanismes de surveillance et de répression des infractions. Selon l'article 22, les États membres de l'UE sont tenus de garantir aux individus un recours juridictionnel en cas de violation des droits de protection des données. L'article 28, en outre, impose aux États membres l'obligation d'instaurer des autorités publiques indépendantes de contrôle de l'application des lois nationales de protection des données. Afin de faciliter la mise en oeuvre des normes de la *Directive de l'UE relative aux données à caractère personnel*, l'article 27 impose aux États membres l'obligation d'encourager l'élaboration de codes de conduite de protection des données. Pour veiller à la mise en œuvre de la *Directive de l'UE relative aux données à caractère personnel* et jouer un rôle consultatif à son sujet, en assurant notamment l'évolution, au sein de l'UE, de la protection des données, l'article 29, enfin, institue un Groupe de protection indépendant.

La *Directive de l'UE relative aux données à caractère personnel* traite également des échanges internationaux de données avec des pays qui ne sont pas membres de l'UE. Ainsi, selon l'article 25, les États membres doivent prévoir que le transfert à un pays tiers ne peut avoir lieu que si le pays tiers destinataire assure un « niveau de protection adéquat ». Le caractère adéquat de ce niveau de protection dépendra de facteurs tels que la nature des données, les lois nationales pertinentes, les règles professionnelles et les mesures de sécurité. La décision à cet égard sera prise par le Groupe de protection indépendant créé par l'article 29. Les documents et les rapports sur l'évaluation des normes de protection des renseignements personnels adoptés par des pays comme le Canada et les États-Unis aux fins de la communication de données avec les États membres de l'UE viennent d'être rendus publics[27]. L'article 26 de la *Directive de l'UE relative aux données à caractère personnel* autorise, dans certaines circonstances limitées, les transferts de données

[27] Site Web : http://europa.eu.int/comm/internal_market/fr/dataprot/wpdocs/index.htm**.** Les rapports et décisions concernant des pays tels que les États-Unis sont achevés, mais le rapport définitif sur le Canada, et la décision qui doit l'accompagner, est attendu pour le début de 2002.

aux États n'assurant pas un niveau de protection adéquat. Il s'agit notamment de cas où le transfert est « nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important ». Enfin l'article 33 prévoit que le premier rapport sur la mise en oeuvre de la *Directive de l'UE relative aux données à caractère personnel*, devant être rendu à l'issue d'une période de trois ans et proposant éventuellement des amendements au texte, devait être remis à l'automne 2001.

## 2. Le *Groupe européen d'éthique des sciences et des nouvelles technologies : l'Avis nº 13 sur les aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information*

Initialement établi en 1991 sous une appellation différente, le Groupe européen d'éthique des sciences et des nouvelles technologies a pour mission d'offrir à la Commission européenne des avis d'ordre éthique de nature interdisciplinaire sur les questions soulevées par les avancées de la science et de la technologie. Le Groupe européen d'éthique des sciences et des nouvelles technologies a rendu quelque 15 avis, dont de nombreux portant sur les problèmes d'éthique des biotechnologies. Dans un avis remis en 1999 sur les *Aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information* (l'*Avis du Groupe européen d'éthique*)[28] le Groupe se penche sur les principales questions soulevées par la collecte et l'utilisation à des fins de recherche des données personnelles sur la santé.

L'*Avis du Groupe européen d'éthique* reprend les huit principes énoncés initialement par l'OCDE en matière de données personnelles et y ajoute la participation des citoyens et l'effort de pédagogie. Il évoque la tension entre, d'une part, la protection de la vie privée, et d'autre part, les besoins de la recherche, et il y voit un des nombreux conflits de valeur auxquels donne lieu la prestation des soins de santé. Cette tension avait été relevée dans les *Lignes directrices de l'OCDE*, ainsi que dans la *Convention 108/1981 du CE*, quelque vingt ans plus tôt. D'après *l'Avis du Groupe européen d'éthique*, il peut parfois falloir échanger une partie de la protection de la vie privée contre certains biens tels que la recherche, sous réserve du respect de certaines normes et conditions. Voici les principaux aspects de l'*Avis du Groupe européen d'éthique*.

### a. Champ d'application

L'*Avis du Groupe européen d'éthique*, consultatif, se penche sur les aspects éthiques que soulèvent les soins de santé dans la société de l'information. Ces questions relèvent en effet de la mission récemment élargie de l'UE, qui comprend maintenant expressément les domaines de la santé et des droits de l'homme. L'*Avis du Groupe européen d'éthique* porte plus particulièrement sur l'utilisation, aux fins générales de la santé, y compris à celles de la recherche, des données sur la santé fournies par des personnes identifiables.

### b. Définitions

L'*Avis du Groupe européen d'éthique* reprend la définition de l'expression « données sur la santé de personnes identifiables » retenue par la *Directive de l'UE relative aux données à caractère personnel*.

[28] Groupe européen d'éthique des sciences et des nouvelles technologies. *Aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information, Avis nº 13*, Bruxelles, 1999. Site Web : http://europa.eu.int/comm/european_group_ethics/docs/avis13_fr.pdf

### c. Protections spéciales : données sensibles

L'*Avis du Groupe européen d'éthique* note que les données personnelles sur la santé englobent un éventail très large de renseignements, y compris les données médicales de base, telles que les antécédents médicaux de l'intéressé, des données sensibles concernant la santé mentale ou des données de nature administrative telles les conditions d'assurance. L'*Avis du Groupe européen d'éthique* précise que « les données personnelles de santé, en tant qu'elles touchent à l'identité et à la vie privée de l'individu, doivent être considérées comme particulièrement sensibles … Les données personnelles de santé sont partie intégrante de la personnalité de l'individu qu'elles concernent. Elles ne sauraient donc être exclusivement considérées comme des marchandises ».

L'*Avis du Groupe européen d'éthique* n'examine que les données de santé, et c'est peut-être pour cela qu'il ne cherche pas à comparer les mesures de protection des données personnelles sur la santé à celles qui s'appliquent aux données personnelles n'ayant pas trait à la santé. L'*Avis du Groupe européen d'éthique* ne précise pas non plus que certaines données personnelles sur la santé, telles les données à caractère génétique, revêtent un caractère plus sensible que d'autres.

### d. Consentement : collecte, utilisation et communication des données

Les vues et les normes du Groupe sur le consentement sont exprimées par ses principes d'autodétermination et de confidentialité. À l'instar des *Lignes directrices de l'OCDE*, l'article 2.3 de l'*Avis du Groupe européen d'éthique* interprète le principe d'autodétermination comme comprenant, pour le citoyen, « le droit de connaître et de déterminer les données personnelles de santé collectées et enregistrées sur son compte et de savoir qui les utilise et à quelles fins. Ce principe suppose également que le citoyen a le droit de rectifier ces données si besoin est ». Le citoyen a en outre le droit de s'opposer à toute utilisation des données personnelles sur la santé le concernant dans un autre but que la prestation de soins, non prévu par la loi.

L'article 2.2 dessine les contours du droit au respect de la vie privée et à la confidentialité, estimant que cela est généralement lié au consentement éclairé de la personne concernée.

Le droit au respect de la vie privée suppose de garantir en permanence la confidentialité des données personnelles de santé. Il impose, par ailleurs, de subordonner en principe la collecte et la transmission de ces données au consentement informé de la personne concernée.

En accord avec la *Directive de l'UE relative aux données à caractère personnel*, cette disposition prévoit que tous les usagers légitimes de données personnelles sont tenus à un devoir de confidentialité *équivalant* à l'obligation professionnelle du secret médical. Le secret médical est considéré comme essentiel à la confiance accordée au système de santé. L'*Avis du Groupe européen d'éthique* reprend en outre la position énoncée par l'Association médicale mondiale en 1948 dans la *Déclaration de Genève* : le respect de la confidentialité continue de s'imposer même après le décès de la personne concernée. (Voir à la Deuxième partie, en E, plus haut.)

### e. Exceptions et recherche

L'*Avis du Groupe européen d'éthique* ne prévoit expressément aucune exception pour la recherche, mais il précise que les exceptions éventuelles à l'obligation de respect de la vie privée et de la confidentialité « doivent être strictement limitées et prévues par la loi ». Cette approche est analogue à celle des *Lignes directrices de l'OCDE*. L'utilisation de données personnelles dans l'intérêt collectif de la société doit se justifier au regard du principe d'autodétermination de

l'individu. En accord avec ces principes, les articles 2.2 et 2.3 impliquent que l'utilisation des données à d'autres fins que celles initialement prévues doit être limitée et autorisée par un texte de loi.

### f. Conservation et sécurité des données

Selon l'article 2.6, la sécurité des technologies de l'information et des communications est « un impératif éthique ». Cet impératif exige donc le recours au cryptage, à l'utilisation de réseaux fermés pour la transmission données à caractère personnel et à d'autres mesures de sécurité appropriées d'ordre organisationnel. L'*Avis du Groupe européen d'éthique* ne fixe aucun délai pour la conservation des données.

### g. Autres dispositions intéressantes

L'*Avis du Groupe européen d'éthique* invite à élaborer, dans le cadre de la *Directive de l'UE relative aux données à caractère personnel*, une directive particulière pour la protection des données médicales.

## 3. La *Charte des droits fondamentaux de l'Union européenne de 2000*

En vertu de traités conclus dans les années 90, les États membres de l'UE sont juridiquement tenus au respect des droits fondamentaux de la personne. Ces traités renvoient aux droits énoncés dans la *CEDH* dont il a été fait état à la Deuxième partie, en C, plus haut. En 2000, l'UE a adopté un nouvel instrument sur les droits de la personne : la *Charte des droits fondamentaux de l'Union européenne* (*Charte de l'UE*)[29]. Ce texte est le résultat d'une initiative commune de ces dernières années visant à réunir dans un texte unique les divers droits civils, politiques, économiques et sociaux énoncés dans divers instruments juridiques ou ayant leur origine dans les divers pays de l'Union européenne élargie. La *Charte de l'UE* est un document qui englobe davantage d'éléments que la *CEDH*. Elle n'offre cependant aucune voie de recours. Elle n'a pas directement force obligatoire. À l'instar de la *Déclaration universelle*, il s'agit d'une proclamation solennelle de droits fondamentaux, attestant et énonçant les principes généraux du droit de l'UE. En théorie, donc, la *Charte de l'UE* pourrait être invoquée devant les tribunaux, judiciaires ou administratifs, en tant que source d'interprétation des droits de la personne de l'UE. L'étude et l'affinement de son statut officiel, et les possibilités, par exemple, de l'intégrer aux traités instituant l'UE, seront étudiés au cours des prochaines années.

L'article 7 de la *Charte de l'UE* rappelle l'appel classique lancé au cours de la période d'après-guerre invitant à l'incorporation, dans les droits de la personne, du droit au respect de la vie privée; il prévoit en effet que toute personne « a droit au respect de sa vie privée et familiale ». Il s'inspire donc largement des textes de la *Déclaration universelle* , de la *CEDH*, du *PIDCP* et du *PIDESC*. Bien qu'il ne cherche pas à définir ce qu'il convient d'entendre par vie privée, comme le préambule de la *Charte de l'UE* renvoie à certains de ces autres documents internationaux et à la jurisprudence européenne sur les droits de l'homme, il y a lieu d'interpréter la notion de « vie privée » d'une manière compatible avec les normes énoncées dans ces instruments.

Au droit au respect de la vie privée vient s'ajouter, par une phrase brève et précise, le principe de protection des données personnelles. L'article 8 prévoit que « toute personne a droit à la

[29] Parlement européen et Conseil de l'Europe, *Charte des droits fondamentaux de l'Union européenne*, Nice, 2000. Site Web : www.europarl.eu.int/charter/default_fr.htm

protection des données à caractère personnel ». Ces données, selon le même article, « doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi ». Cela implique qu'en matière de collecte de données, les exceptions au principe du consentement doivent être explicitement prévues par la loi. Le même article invite en outre à reconnaître le droit pour toute personne d'accéder aux données recueillies la concernant et au contrôle du respect de ces règles par une autorité indépendante. La *Charte de l'UE* reprend donc les principaux éléments constitutifs des principes de protection des données initialement adoptés par l'OCDE et les codifie dans un instrument international régional sur les droits de de la personne.

## D. Les Nations Unies

Dans la Deuxième partie, plus haut, il a été montré qu'au cours des dernières décennies, la protection de la vie privée avait été un des principaux soucis de la communauté internationale en matière de protection des droits de la personne; ce n'est cependant qu'au cours des années 90 que l'ONU a commencé à se pencher sérieusement sur la protection des données entendue comme un aspect de celle de la vie privée. Depuis lors, au moins deux initiatives d'instances des Nations Unies ont abouti à l'élaboration de textes officiels concernant la protection des données : une résolution de l'Assemblée générale de l'ONU, de 1990, et une déclaration, de 1994, découlant d'un effort de coopération d'un des bureaux régionaux de l'Organisation mondiale de la santé.

### 1. Les *Principes directeurs de 1990 pour la réglementation des fichiers informatisés contenant des données à caractère personnel*

En 1990, l'Assemblée générale des Nations Unies a adopté les *Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel (les Principes directeurs de l'ONU)*[30]. Les *Principes directeurs de l'ONU* reprennent, parfois en les modifiant, les normes initialement adoptées par l'OCDE en intégrant, en matière de traitement électronique de données, les principes suivants : le principe de licéité et de loyauté, le principe d'exactitude, le principe de finalité, le principe de l'accès par les personnes concernées, le principe de non-discrimination et le principe de sécurité. Les *Principes directeurs de l'ONU* ne revêtent aucune force obligatoire, cela dit, ils constituent une déclaration officielle de la part de quelque cent quatre-vingt États membres de l'Assemblée générale de l'ONU. C'est dire qu'ils témoignent d'un consensus très poussé sur les principes fondamentaux des règles et des politiques internationales de protection des données.

#### a. Champ d'application

L'ONU invite les organisations internationales, gouvernementales et non gouvernementales, ainsi que les États, à recevoir les *Principes directeurs de l'ONU*, en tant que mesures de protection minimum, dans leur législation nationale. Les *Principes directeurs de l'ONU* s'appliquent aux dossiers informatisés contenant des renseignements personnels et du secteur public et du secteur

[30] Nations Unies, Assemblée générale. *Résolution 45/95 du 14 décembre 1990* : *Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel,* New York, 1990. Site Web : http://www.unhchr.ch/french/html/menu3/b/71_fr.htm

privé. Il y est précisé que les gouvernements et les organisations sont libres également de les appliquer aussi aux dossiers non informatisés.

### b. Définitions

Les *Principes directeurs de l'ONU* ne définissent pas les principaux termes qu'ils utilisent.

### c. Protections spéciales : données sensibles

À l'inverse des *Lignes directrices de l'OCDE*, mais en accord avec la *Convention 108/1981 du CE* et la *Directive de l'UE relative aux données à caractère personnel*, les *Principes directeurs de l'ONU* prévoient une protection particulière pour les données sensibles. Sous réserve d'exceptions strictement définies, la collecte de « données pouvant engendrer une discrimination illégitime ou arbitraire » est interdite globalement. Les données concernant la vie sexuelle d'un individu, ou son origine ethnique ou raciale, sont citées comme exemple de données sensibles, mais les *Principes directeurs de l'ONU* ne comportent aucune mesure particulière pour les données sur la santé. Une telle désignation est laissée à l'appréciation des États membres.

### d. Consentement : collecte, utilisation et communication des données

En vertu des *Principes directeurs de l'ONU*, les données doivent être recueillies ou traitées de manière licite, loyale, exacte et avoir une finalité spécifiée et légitime. La cueillette de toute donnée recueillie à des fins incompatibles avec les finalités spécifiées, ou entraînant l'utilisation ou la communication de renseignements personnel exige, de manière générale, le consentement de la personne concernée.

### e. Exceptions et recherche

Les *Principes directeurs de l'ONU* prévoient des dérogations étroites à l'obligation générale de collecte, d'utilisation et de communication licites, loyales et consenties des données personnelles. Toute exception doit remplir plusieurs conditions. Il faut d'abord que l'exception soit fondée sur la nécessité de protéger, notamment, l'ordre public, la santé ou la moralité publique, la sécurité nationale, ou les droits et libertés d'autrui. Ensuite, il faut que cette exception soit « prévue par la loi », ou par une réglementation équivalente, et soumise à des limites expressément définies et à des « garanties appropriées ». Le critère d'appréciation de la nécessité correspond aux critères retenus dans d'autres documents internationaux tels les *Lignes directrices de l'OCDE*, la *Convention 108/1981 du CE* et la *Directive de l'UE relative aux données à caractère personnel*. En ce qui concerne les données sensibles, les *Principes directeurs de l'ONU* exigent en outre que toute exception dont la nécessité est avérée respecte les limites prescrites par les traités et les instruments internationaux des droits de la personne applicables.

### f. Conservation et sécurité des données

Les *Principes directeurs de l'ONU* contiennent, en matière de conservation et de sécurité des données, des dispositions analogues aux *Lignes directrices de l'OCDE*. Ainsi, les données personnelles ne doivent pas être conservées plus longtemps qu'il n'est nécessaire au regard des finalités spécifiées et légitimes ayant justifié leur collecte. Il convient en outre qu'elles soient protégées par des mesures de sécurité « appropriées » contre, notamment, la perte ou la destruction accidentelle ou l'accès non autorisé.

### g. Autres dispositions intéressantes

Les *Principes directeurs de l'ONU* traitent expressément aussi des questions de transferts internationaux de données et de mise en oeuvre nationale des mesures de protection.

À l'instar des *Lignes directrices de l'OCDE* et de la *Convention 108/1981 du CE*, il est recommandé, dans les *Principes directeurs de l'ONU*, que les échanges internationaux de données puissent s'effectuer librement entre pays accordant des « garanties comparables » à la protection de la vie privée. Même en l'absence de garanties comparables, les restrictions aux flux transfrontaliers de données « ne peuvent être imposées indûment et seulement dans la stricte mesure où la protection de la vie privée l'exige ».

En ce qui concerne la mise en oeuvre nationale, les *Principes directeurs de l'ONU* vont au-delà des dispositions des *Lignes directrices de l'OCDE* et de la *Convention 108/1981 du CE* et proposent des normes qui ont depuis été reprises par la *Directive de l'UE relative aux données à caractère personnel*. (Voir plus haut, dans la Troisième partie, en C, à 1). Il est recommandé dans les *Principes directeurs de l'ONU* que les lois nationales désignent des autorités nationales impartiales et techniquement compétentes pour veiller au respect des principes que devraient sanctionner des dispositions notamment pénales, et qu'elles ouvrent aux particuliers les voies de recours appropriées. Dans de nombreux pays, ces responsabilités sont de nos jours celles de commissaires à la protection de la vie privée indépendants.

## 2. La *Déclaration de 1994 de l'OMS sur la promotion des droits des patients en Europe*

En 1994, l'Organisation mondiale de la santé (l'OMS) a organisé une consultation en vue de l'institution d'une structure commune de principes au regard des malades en Europe. Cette consultation s'est terminée par l'endossement d'une grande déclaration régionale, la *Déclaration sur la promotion des droits des patients en Europe (la Déclaration de l'OMS)*[31]. Il y était notamment prévu que les principes ayant trait à la vie privée, à la confidentialité et à la protection des données qui y étaient inscrits pourraient aider les gouvernements européens à mieux régir le secteur de la santé, et qu'ils pourraient être mis de l'avant et en oeuvre par des lois et des codes de conduite professionnelle ainsi que par la formation professionnelle et l'éducation.

La *Déclaration de l'OMS* fait de la protection de la vie privée une valeur humaine et un droit de la personne de base en matière de soins de santé. Selon l'article premier, toute personne possède le droit à l'autodétermination, à l'intégrité physique et mentale et au respect de sa vie privée. Conformément à ce droit au respect de la vie privée dans le secteur de la santé, l'article 4.1 de la *Déclaration de l'OMS* rappelle l'obligation générale de confidentialité au sujet de la situation de santé du malade, de sa situation médicale et que : « toutes les données identifiables concernant le patient doivent être protégées » — même après son décès. Ce devoir de confidentialité posthume fait écho à la *Déclaration de Genève* de 1948 de l'Association médicale mondiale. L'article 4.2 indique en outre que l'information confidentielle ne peut être divulguée que s'il y a eu obtention d'un consentement explicite ou que la loi l'autorise expressément. La *Déclaration de l'OMS* précise ensuite, à son article 4.3, que toute donnée relative à un patient identifiable doit être protégée et que « cette protection doit correspondre à leur forme de stockage ». Relevons également parmi les dispositions pertinentes, l'article 3.10 qui, à l'instar de la *Déclaration d'Helsinki* de l'AMM, fixe comme condition préalable à la conduite de la recherche scientifique, l'obtention du consentement et un contrôle éthique suffisant.

---

[31] Consultation européenne sur le droit des patients de l'Organisation mondiale de la santé. *Déclaration sur la promotion des droits des patients en Europe*. Amsterdam, mars 1994. Réimpression (en anglais) dans *European J. Health L.*, nº 1, 1994, pp. 279-291. Site Web : http://www.who.int/library/reference/information/declarations/index.fr.shtml

## 3. La *Déclaration universelle de 1997 sur le génome humain et les droits de l'homme de l'UNESCO*

Fondée en 1945, l'Organisation des Nations Unies pour l'éducation, la science et la culture (l'UNESCO) est une institution spécialisée des Nations Unies. Cette organisation a notamment pour mission de resserrer par l'éducation, la science et la culture, les rapports entre les peuples du monde dans le cadre de la vocation générale des Nations Unies de défense de la dignité de la personne humaine. Au cours de la dernière décennie, l'impact sur la culture, sur l'évolution de l'idée de bien-être humain en particulier, de l'accélération des progrès scientifiques et technologiques n'a pas échappé à l'UNESCO. Tout au long des années 90, l'UNESCO a consacré toujours davantage attention, analyses et débats interdisciplinaires à une série de questions dans divers domaines, telles la génétique et la société. Les délibérations menées dans le domaine de la génétique ont abouti, en 1997, à la *Déclaration universelle sur le génome humain et les droits de l'homme (la Déclaration de l'UNESCO)*[32]. S'inspirant en partie de la *Déclaration universelle*, la *Déclaration de l'UNESCO* offre à la communauté internationale, une série de principes et de normes sur la recherche, le développement et l'application des connaissances modernes en génétique. Certains, dans ce large éventail de principes, traitent de l'importance de la recherche, d'autres insistent plutôt sur la protection adéquate des données à assurer.

L'article 12 de la *Déclaration de l'UNESCO* lance un appel en faveur de l'accès de tous aux bénéfices qui peuvent être tirés des nouvelles connaissances sur le génome humain. Selon cet article, la liberté de la recherche procède de la liberté de pensée. Mais, bien qu'une liberté, la recherche doit tout de même respecter certaines normes de base. Aussi l'article 5 insiste-t-il sur la nécessité d'une évaluation rigoureuse des risques et des avantages, d'un contrôle préalable des protocoles de recherche sur le génome en fonction de normes nationales et internationales, et du consentement préalable, libre et éclairé de l'intéressé, ou de l'autorisation d'une instance de substitution, pour toute participation à une recherche conforme à la loi.

La *Déclaration de l'UNESCO* traite en outre de l'information génétique associée à une personne identifiable. Elle fait d'ailleurs de la confidentialité des données génétiques une obligation générale à laquelle seules des dérogations très précisément encadrées peuvent être admises. L'article 7 prévoit en effet que « la confidentialité des données génétiques associées à une personne identifiable, conservées ou traitées à des fins de recherche ou dans tout autre but, doit être protégée dans les conditions prévues par la loi ». (La *Déclaration de l'UNESCO* ne donne cependant aucune définition de ce qu'il faut entendre par « données génétiques ».) L'article 9 vient préciser que les exceptions au principe général de confidentialité doivent n'être autorisées qu'en cas de « raisons impérieuses et dans les limites du droit international public et du droit international des droits de l'homme ». Cette formule s'aligne sur le critère de nécessité qui conditionne toute limitation au principe de protection de la vie privée prévu en vertu de la *Déclaration universelle* et de la *CEDH*, ainsi que nous l'avons vu plus haut, au B et au C de la Troisième partie. La *Déclaration de l'UNESCO* invite à prendre des mesures pour favoriser la mise en oeuvre de ses principes. C'est ainsi que le Comité international de bioéthique de l'UNESCO a récemment entrepris un examen plus approfondi des principes régissant le respect de la vie privée et de la confidentialité des données génétiques[33].

---

[32] Organisation des Nations Unies pour l'éducation, la science et la culture. *Déclaration universelle sur le génome humain et les droits de l'homme*. Paris, 1997. Site Web : http://www.unesco.org/ibc/fr/genome/projet/

[33] Voir, par exemple, UNESCO, Groupe de travail du Comité international de bioéthique sur la confidentialité et les données génétiques. *Rapport sur la confidentialité et les données génétiques*. Paris, juin 2000.

# IV. Sélection de lois nationales sur la protection des données

Sur la toile de fond internationale qui précède, voici un aperçu des lois de quelques pays sur la protection des données. Nous présenterons les principes généraux des principales lois nationales, puis leurs dispositions particulières sur la recherche dans le domaine de la santé. Les lois sont analysées selon la méthode générale énoncée dans l'introduction.

## A. L'Australie

En Australie, la principale source de protection de la vie privée est une loi fédérale, le *Privacy Act 1988*[34]. Comme ce sont des représentants australiens qui ont présidé le comité de travail chargé d'élaborer les normes de protection des données pour les *Lignes directrices de l'OCDE,* il n'est pas surprenant que la Loi adopte et incorpore toutes les dispositions des *Lignes directrices de l'OCDE*. Le *Privacy Act* s'est appliqué durant des années au secteur public fédéral. Mais, à la suite de la promulgation récente du *Privacy Amendment (Private Sector) Act 2000*[35], la Loi révisée (le *Privacy Act révisé*) a acquis une portée plus large. À compter de décembre 2001, le *Privacy Act révisé* s'appliquera au secteur privé.

Comme d'autres pays qui viennent de moderniser leurs lois nationales sur la protection des données personnelles, l'Australie, par le *Privacy Act révisé,* s'efforce de traduire juridiquement les engagements qu'elle a pris en matière de protection de la vie privée, considérée comme un droit de la personne. L'Australie a manifesté sa disposition à prendre ces engagements en signant et en ratifiant le *PIDCP*, qui reconnaît le droit à la vie privée comme un droit fondamental de la personne du droit international public (voir plus haut, au D de la Seconde partie). En fait, le *PIDCP* est mentionné dans le préambule du *Privacy Act 1988*. Le *Privacy Act révisé* montre bien également comment d'autres intérêts sociétaux, comme la recherche dans le domaine de la santé, peuvent s'opposer au droit à la vie privée, voire justifier des incursions limitées dans la sphère qu'il protège pour l'avancement de l'intérêt public.

Nous allons maintenant : 1) donner un aperçu des dispositions générales du *Privacy Act révisé*; 2) comparer les principes, déjà établis, applicables au secteur public et les nouveaux principes applicables au secteur privé; 3) analyser les directives relatives à la recherche médicale publiées ou approuvées par le Commissaire à la protection de la vie privée en vertu du *Privacy Act révisé*. En fait, l'un des aspects remarquables du *Privacy Act révisé* est la façon dont il autorise le Commissaire à la vie privée de l'Australie à approuver des directives, élaborées par le ministère de la Santé, au sujet de l'utilisation, dans la recherche médicale, de renseignements personnels.

---

34 Commonwealth de l'Australie. *Privacy Act 1988*, loi nº 119 de 1988, modifiée. Site Web : www.austlii.edu.au

35 Commonwealth de l'Australie, *Privacy Amendment (Private Sector) Act 2000*, loi nº 155 de 2000, modifiant le *Privacy Act 1988.* Site Web : www.privacy.gov.au/

## 1. Le *Privacy Act 1988* [Loi sur la vie privée]

Le nouveau *Privacy Act révisé* a un champ d'application plus large et un plus grand nombre de ses dispositions portent sur la recherche en santé. C'est le Commissaire à la protection de la vie privée de l'Australie qui en supervise l'application et l'exécution.

Il résulte du *Privacy Act révisé* que le secteur public et le secteur privé sont désormais régis par une série parallèle de principes destinés à instaurer un régime national de protection de la vie privée coréglementé. Ces principes fixent les normes générales de collecte, d'utilisation et de communication des renseignements personnels.

Les normes du secteur public : les *Principes d'information et de protection de la vie privée («Information Privacy Principles »* : IPP*)*, et celles du secteur privé : les *Principes nationaux de protection de la vie Privée (« Information Privacy Principles »* : NPP), sont évoqués dans les paragraphes d. à f. qui suivent. Il est à signaler que chacun de ces éléments est décrit deux fois : une pour les IPP et une autre pour les NPP.

L'article 16 du *Privacy Act révisé* fait obligation aux entreprises du secteur privé de se conformer aux NPP ou aux codes de protection de la vie privée approuvés par le Commissaire à la protection de la vie privée de l'Australie. Au printemps 2001, aucun code de ce genre n'avait encore été approuvé. Le Commissaire n'avait non plus approuvé, en vertu de l'article 95A, aucun *Guidelines for National Privacy Principles on Health Information* (ou *Lignes directrices pour l'application des Principes nationaux de protection de la vie privée à l'information sur la santé*) pour le secteur privé, comme cela est le cas pour le secteur public. Mais, même après l'éventuelle approbation de ces codes ou de ces lignes directrices, les dix NPP, énoncés à l'annexe 3 du *Privacy Act révisé*, continueront de définir les normes générales de protection de la vie privée du secteur privé. Ils font écho aux principes fondamentaux adoptés par l'OCDE en 1981 et sont analogues aux IPP appliqués depuis longtemps au secteur public.

### a. Champ d'application

Le *Privacy Act révisé* de 1988 s'applique aux renseignements personnels recueillis et sur papier et sur support électronique dans le secteur public fédéral et dans le secteur privé. Ses dispositions et ses normes sont applicables depuis longtemps aux « institutions » fédérales : en général, les ministères, les départements, les tribunaux et les organes spéciaux du Commonwealth d'Australie. La plupart de ces dispositions sont axées sur une série de normes de base de protection de la vie privée dans le secteur public : les IPP.

À compter de décembre 2001, une série parallèle de normes entrera en vigueur pour les « organismes » du secteur privé. Aux termes de l'article 6 D) du *Privacy Act révisé*, il s'agit notamment des personnes physiques et morales, des sociétés de personnes, des associations non constituées en personnes morales et des fiducies, des entreprises dont le chiffre d'affaires est de trois millions de dollars ou plus, des organismes sans but lucratif (associations caritatives, clubs sportifs et syndicats), des cocontractants des marchés du gouvernement fédéral, des fournisseurs des services de santé qui détiennent des renseignements personnels sur la santé, des entreprises de collecte ou de communication de renseignements personnels contre rémunération, service ou avantage quelconque et des organisations désignées par la réglementation. Les petites entreprises ne sont généralement pas visées par la définition. Les nouvelles normes parallèlement applicables au secteur privé sont les NPP. Les principes qui s'appliquent au secteur public et ceux qui s'appliquent au secteur privé sont décrits plus loin.

### b. Définitions

Le *Privacy Act révisé* définit divers termes de la recherche en santé lorsque des renseignements personnels sont en cause. À l'article 6, on trouve les définitions qui sont communes au secteur public et au secteur privé : renseignements personnels, renseignements sensibles, renseignements sur la santé et recherche médicale notamment.

Les « renseignements personnels », ce sont « des renseignements ou une opinion (…) sur un particulier dont l'identité est reconnaissable ou peut vraisemblablement être établie à partir de ces renseignements ou opinion ». Aux termes de sa définition, tout « particulier » doit être une personne physique. Par suite de la révision de la Loi en l'an 2000, les « renseignements sur la santé » sont définis comme incluant tous les renseignements concernant la santé ou une invalidité d'un particulier, un service de santé dispensé ou à dispenser, ainsi que tous les renseignements personnels recueillis en rapport avec la fourniture d'un service de santé ou d'un don d'organes, de parties du corps ou de substances corporelles. Le *Privacy Act révisé* donne également une définition large de l'expression « service de santé », mais il n'y fait pas référence à la recherche, pas plus qu'il ne définit l'expression « recherche en santé »; il précise plutôt que la « recherche médicale (…) comprend la recherche épidémiologique ».

Il est à noter que, comme nous le verrons plus loin, d'autres termes ayant rapport à la recherche en santé sont définis dans les lignes directrices applicables au secteur public qui sont adoptées sous le régime du *Privacy Act révisé*. Il s'agit de termes comme « données de personnes identifiées », données de personnes « potentiellement identifiables » et données « dépersonnalisées ».

### c. Protections spéciales : données sensibles

Le *Privacy Act révisé* reprend la notion de données sensibles. Il s'écarte donc des *Lignes directrices de l'OCDE* et s'aligne sur la plupart des autres normes internationales de protection des données mentionnées plus haut, dans la Troisième partie. L'expression « renseignements sensibles » est définie largement à l'article 6 de la Loi : y sont inclus les renseignements concernant la race ou l'origine ethnique, les opinions politiques, les convictions religieuses, les préférences ou les pratiques sexuelles et les renseignements sur la santé. Ainsi, les « renseignements sur la santé », selon la définition ci-dessus, sont considérés comme des données sensibles. Les données sensibles sont assujetties à des normes spéciales de protection de la vie privée en vertu des NPP, qui ont été récemment intégrées à la Loi pour qu'elles puissent s'appliquer au secteur privé. Les NPP interdisent toute collecte de renseignements sensibles, à moins que le consentement du particulier concerné ne soit obtenu ou à moins d'autres exceptions particulières. Il n'existe pas de dispositions explicites concernant les données sensibles pour le secteur public, mais les lignes directrices du secteur public sur la recherche font état de données sur la santé qui sont considérées comme sensibles.

### d.1. Consentement : collecte, utilisation et communication des données (IPP)

Les normes applicables à la protection des données du secteur public sont inspirées en partie des *Lignes directrices de l'OCDE*. Entre autres, les IPP prévoient que la collecte de l'information doit être effectuée à des fins licites et qu'elle doit être « nécessaire » pour les atteindre (principe premier). Les données doivent généralement être recueillies directement auprès de l'intéressé, avoir trait aux fins pour lesquelles est faite la collecte et s'inscrire dans un large éventail de renseignements recueillis, selon des méthodes justes et licites ne représentant pas une intrusion déraisonnable dans la vie privée (principes 2 et 3).

Comme les *Lignes directrices de l'OCDE*, les normes ne font pas explicitement état du consentement exigé pour la collecte des renseignements personnels. Mais le principe qui exige que les données soient recueillies directement auprès de l'intéressé (principe 2) l'implique probablement. Le principe 9, lui, exige que les renseignements personnels ne servent qu'aux fins prévues. Ils ne doivent pas servir à d'autres ou être communiqués, à moins que l'individu concerné n'y consente ou que d'autres exceptions soient applicables en vertu de quelque norme sur la nécessité comme, par exemple, lorsque l'usage ou la communication s'avère « nécessaire » pour faire respecter la loi ou pour pallier un danger imminent et grave pour la vie ou la santé, ou encore que la loi l'exige ou l'autorise (principes 10 et 11). Voir pour plus de détails la section e. 1 plus bas.

### d.2. Consentement : collecte, utilisation et communication des données (NPP)

Selon les NPP applicables au secteur privé, les renseignements personnels :

- Ne peuvent être recueillis que par des moyens licites, loyaux et respectueux, directement de la personne concernée, et seulement si c'est nécessaire (principe premier);
- Ne peuvent être utilisés et communiqués que pour les fins premières prévues de leur collecte (principe 2);
- Doivent être traités avec exactitude, rapidement et complètement (principe 3);
- Doivent être conservés en sûreté (principe 4);
- Doivent être traités et gérés selon les politiques de protection des renseignements personnels des organisations détentrices (principe 5);
- Doivent pouvoir être consultés et corrigés par la personne concernée (principe 6 );
- Ne doivent être associés à des identificateurs uniques que dans des cas limités (principe 7);
- Doivent être rendus anonymes s'il est possible et licite de le faire, à la demande de la personne concernée (principe 8);
- Ne doivent être communiqués à d'autres pays que dans des cas limités (principe 9);
- Ne doivent être recueillis, s'ils sont considérés comme étant des données sensibles, que dans des conditions strictes et limitées (principe 10).

Une norme générale est imposée par ces principes en matière de consentement à la collecte, à l'utilisation et à la communication des renseignements personnels ayant trait à la santé. Trois de ces principes illustrent comment.

Premièrement, pour les données générales, le principe premier exige entre autres choses que l'information soit recueillie directement de l'intéressé, lequel doit être informé des fins, des besoins, des justifications juridiques et des paramètres du traitement des données. Cela fait écho au principe applicable au secteur public et aux *Lignes directrices de l'OCDE.* Le principe 1.2 exigeant d'informer l'intéressé des conséquences d'un refus de fournir l'information laisse penser qu'on s'attend généralement à ce qu'il accepte.

Deuxièmement, le principe 10 impose une norme stricte pour la collecte des renseignements sur la santé et des autres données sensibles du même genre. Faute de consentement ou d'exceptions particulières, il n'est pas possible de recueillir des renseignements sur la santé. Le deuxième alinéa de ce principe établit également une norme pour le consentement aux utilisations par des tiers. C'est-à-dire que les organisations n'ont pas le droit d'utiliser ou de communiquer ces renseignements à d'autres fins que pour le but premier prévu de la collecte, à moins que l'intéressé n'y consente ou que des exceptions particulières ne s'appliquent.

Troisièmement enfin, le principe 9 prévoit qu'il est possible de transférer des renseignements à d'autres pays n'ayant pas de garanties substantiellement équivalentes en matière de protection de la vie privée si, notamment, l'intéressé y consent. Cela reviendrait à une renonciation aux garanties habituelles.

### e.1. Exceptions et recherche (IPP)

En dehors de ces exceptions, les IPP n'autorisent expressément aucune exception pour la recherche médicale. Mais le *Privacy Act révisé* délègue le pouvoir d'élaborer des normes au *National Health and Medical Research Council of Australia* (le Conseil national de la santé et de la recherche médicale d'Australie, le NHMRC). L'article 95 du *Privacy Act révisé* prévoit qu'une loi promulguée par une institution du Commonwealth qui est contraire à un IPP ne sera pas tenue pour telle si elle est conforme aux lignes directrices du NHMRC sur la recherche médicale approuvées par le Commissaire à la vie privée. Comme nous le montrerons à la section 3 plus bas, ces lignes directrices prévoient des exceptions strictes à l'utilisation ou à la communication non consentie de données médicales de personnes identifiables.

### e.2. Exceptions et recherche (NPP)

Les principes applicables au secteur privé prévoient également d'importantes exceptions à la norme générale selon laquelle les renseignements sur la santé ne peuvent être recueillis et utilisés que si l'intéressé y consent. Ils prévoient même des exceptions particulières pour la recherche.

Les règles relatives aux données sensibles et aux utilisations secondaires, par exemple, autorisent le traitement non consenti des données personnelles en des cas limités de nécessité. Le principe 10.1 autorise une organisation à recueillir des données sensibles, dont des données sur la santé, sans consentement si, par exemple, « la loi l'exige » ou si cela est « nécessaire » aux fins d'une instance judiciaire donnée. La collecte sans consentement est également permise dans les cas d'urgence, lorsqu'elle est « nécessaire pour prévenir ou pallier un grave et imminent danger pour la vie ou la santé humaines et que la personne concernée n'est pas en mesure de donner son consentement ou est physiquement incapable de le communiquer ». De même, le principe 2 autorise les utilisations secondaires de données personnelles sans consentement dans divers cas de nécessité et dans des circonstances limitées. Beaucoup de ces exceptions font écho aux normes énoncées dans la *Directive de l'UE relative aux données à caractère personnel* dont il a été traité plus haut, à la Troisième partie, en C.

Les normes applicables aux données sensibles et aux utilisations secondaires des NPP autorisent également le traitement sans consentement dans le cas précis de la recherche médicale. Il est possible de recueillir sans consentement des renseignements sur la santé à des fins de recherche si quatre conditions sont remplies. Le principe 10.3 prévoit, premièrement, que la collecte de renseignements sur la santé doit être « nécessaire » aux fins limitées de la recherche. Ces fins sont notamment la recherche en santé publique, l'analyse statistique à des fins de sécurité publique et la recherche de supervision d'un service de santé. Deuxièmement, la collecte de données de santé de personnes identifiables doit également être nécessaire à la réalisation de l'objectif de recherche. Troisièmement, il doit être peu réaliste pour l'organisation d'obtenir le consentement de l'intéressé (ce « peu de réalisme » n'est pas défini). Quatrièmement, les renseignements doivent également être recueillis en vertu de pouvoirs spéciaux : a) parce que « la loi l'exige »; b) conformément aux lignes directrices approuvées par le Commissaire à la protection de la vie privée en vertu de l'article 95A du *Privacy Act révisé*; c) ou « conformément aux règles établies par les autorités sanitaires ou médicales compétentes statuant sur les obligations de

l'organisation en matière de secret professionnel ». Avant que les renseignements recueillis en vertu du principe 10.3 puissent être communiqués, le principe 10.4 fait également obligation aux organisations de prendre des mesures raisonnables pour dépersonnaliser définitivement les renseignements.

Dès lors que des renseignements personnels sur la santé sont recueillis, le principe 2 §1 d) en autorise l'utilisation et la communication non consenties si cela est « nécessaire à la recherche ou à la compilation ou à l'analyse de données statistiques aux fins de la santé ou de la sécurité publiques ». Ce genre de recherche est assujettie à trois conditions : a) il serait à peu près impossible de chercher à obtenir le consentement de l'intéressé (ce « à peu près impossible » n'est pas défini); b) « l'utilisation ou la communication de l'information est conforme aux lignes directrices approuvées par le Commissaire à la protection de la vie privée en vertu de l'article 95A »; c) l'organisation, lorsqu'il s'agit de communication, « est raisonnablement convaincue » que les destinataires de l'information ne la divulgueront pas, non plus que les renseignements personnels qui s'y rattachent. Remarquons que l'utilisation et la communication de ces renseignements sont assujetties aux lignes directrices du NHMRC approuvées par le Commissaire à la protection de la vie privée pour le secteur privé. Comme nous le verrons plus loin, ces lignes directrices sont censées entrer en vigueur en 2001-2002.

### f.1. Conservation et sécurité des données (IPP)

Les obligations relatives à la conservation et à la sécurité des données sont énoncées au principe 4 des IPP. Selon ce principe, ceux qui ont la garde des enregistrements de renseignements personnels doivent appliquer des mesures de sécurité suffisantes pour les protéger de tout accès non autorisé et éviter qu'ils soient perdus ou détournés de leur usage. Contrairement aux principes applicables au secteur privé, les IPP ne semblent pas énoncer de règles précises concernant une période ou une norme de conservation des données.

### f.2. Conservation et sécurité des données (NPP)

Le principe 4 des NPP prévoit quelles obligations doivent être associées à la conservation et à la protection des données dans le secteur privé. Il fait obligation aux organisations de prendre des « mesures suffisantes » pour garantir la sécurité des renseignements personnels et éviter qu'ils soient détournés de leur usage, détruits ou perdus. Ce principe est différent de celui qui s'applique au secteur public car il oblige les organisations à détruire ou à dépersonnaliser définitivement les renseignements personnels devenus inutiles soit aux fins pour lesquelles ils avaient été recueillis soit pour d'autres usages autorisés. Ce principe de conservation des données est complété par les normes des lignes directrices applicables à la recherche médicale publiées par le NHMRC et approuvées par le Commissaire à la protection de la vie privée.

## 2. Les Lignes directrices applicables à la recherche médicale et à la recherche en santé adoptées en vertu du *Privacy Act*

Les articles 95 et 95A du *Privacy Act révisé* prévoient que le NHMRC d'Australie peut, si le Commissaire à la protection de la vie privée accorde son approbation, publier des lignes directrices concernant la protection de la vie privée dans la conduite de la « recherche médicale » lorsqu'il est nécessaire d'y utiliser des renseignements personnels.

Ces lignes directrices ne seront approuvées que si « l'intérêt public qu'il peut y avoir à favoriser la recherche dans le domaine touché par les lignes directrices l'emporte dans une mesure substantielle sur un autre, celui de continuer à « adhérer » aux garanties de protection des

renseignements personnels. Les lignes directrices applicables à la protection de la vie privée au regard de la recherche médicale viennent d'être révisées. Celles qui sont destinées au secteur privé sont en cours d'élaboration; elles sont attendues pour la fin de 2001 ou pour 2002.

## 2A. Lignes directrices approuvées pour le secteur public

Le NHMRC vient de produire de nouvelles lignes directrices, approuvées récemment par le Commissaire à la protection de la vie privée, pour la recherche médicale qui se fait dans le secteur public fédéral. Il s'agit des *Guidelines Under Section 95 of the Privacy Act 1988 (les Lignes directrices applicables au secteur public de l'article 95)*[36].

### a. Champ d'application

Les *Lignes directrices applicables au secteur public de l'article 95* sont applicables directement et indirectement. Lorsque la recherche médicale suppose l'usage de renseignements personnels par le secteur public fédéral, les lignes directrices s'appliquent directement et doivent être respectées pour que l'information puisse être licitement utilisée ou communiquée. Les lignes directrices « instaurent une structure d'encadrement de la conduite de la recherche médicale lorsqu'elle fait appel à des renseignements détenus par les institutions du Commonwealth [d'Australie] et que des renseignements de personnes identifiables doivent être utilisés sans le consentement de ces personnes ». Le champ d'application des lignes directrices est cependant élargi par l'intégration de certaines normes et procédures tirées d'autres documents fédéraux sur la recherche en santé dont, par exemple, le *National Statement on Ethical Conduct in Research Involving Humans*[37] (Énoncé national d'éthique de comportement en matière de recherche sur les êtres humains) du NHMRC (1999). Ce dernier document renvoie à son tour aux *Lignes directrices applicables au secteur public de l'article 95* et les incorpore à ses normes. Par conséquent, les Lignes directrices ont une large application indirecte. En fait, comme cet Énoncé national d'éthique du NHMRC exige des bénéficiaires des subventions fédérales à la recherche en santé qu'ils respectent les Lignes directrices à titre de normes nationales de l'éthique de la recherche en santé[37], les Lignes directrices touchent un large éventail de spécialistes et d'établissements non gouvernementaux qui font de la recherche en santé.

### b. Définitions

Outre les définitions tirées du *Privacy Act révisé, les Lignes directrices applicables au secteur public de l'article 95* comportent un glossaire d'autres définitions intéressant directement la recherche en santé. Par exemple, elles incorporent la définition de « renseignements personnels » du *Privacy Act révisé,* or cette expression englobe les données d'identification autant des groupes que des particuliers. La référence explicite aux groupes peut s'avérer directement applicable à la santé publique, à la génétique et à la recherche démographique.

Les *Lignes directrices applicables au secteur public de l'article 95* définissent d'autres termes et expressions dans ce domaine, dont : « données de personnes identifiées », données de personnes « potentiellement identifiables » et « données dépersonnalisées ». Les données « permettant l'identification d'une personne » sont des « données de personnes identifiées ». Les renseignements personnels sur la santé qui ont été codés ont été « dépersonnalisés », mais, dans la mesure où

---

36 Australie, National Health and Medical Research Council, *Guidelines Under Section 95 of the Privacy Act 1988*, Canberra, 2000. Site Web : http://www.health.gov.au/nhmrc/issues/researchethics.htm

37 National Health and Medical Research Council of Australia, *National Statement on Ethical Conduct in Research Involving Humans*, Canberra, 1999 (préambule et art. 18).

ils peuvent être « personnalisables » par décodage, ils restent des données de personnes « potentiellement identifiables ».

Les *Lignes directrices applicables au secteur public de l'article 95* font la même référence à la « recherche médicale »[38] que le *Privacy Act révisé*, mais elles définissent plus précisément la « recherche » comme supposant « une investigation systématique dans le but d'établir des faits, des principes et un savoir ».

### c. Protections spéciales : données sensibles

*Les Lignes directrices applicables au secteur public de l'article 95* ne font pas elles-mêmes explicitement état des données sensibles, mais le *Privacy Act révisé* définit les « renseignements sensibles » comme englobant les renseignements de santé et les renseignements médicaux. Par conséquent, au sens du *Privacy Act révisé*, les Lignes directrices portent sur le traitement d'une catégorie de données sensibles du secteur public fédéral.

### d. Consentement : collecte, utilisation et communication des données

L*es Lignes directrices applicables au secteur public de l'article 95* visent de façon générale l'utilisation non consentie de renseignements personnels aux fins de la recherche médicale. Lorsque les exceptions prévues ne s'appliquent pas, les normes de base générales régissant la collecte, l'utilisation et la communication des données personnelles des IPP de l'article 14 du *Privacy Act révisé* sont applicables.

### e. Exceptions et recherche

Pour justifier une communication de renseignements personnels contraire aux IPP du *Privacy Act révisé*, une organisation doit s'assurer que « la recherche dans le cadre de laquelle ces renseignements doivent être utilisés a été approuvée par un Human Research Ethics Committee [ou Comité d'éthique pour la recherche sur l'être humain] (HREC) à ces fins particulières, conformément aux Lignes directrices ». *Les Lignes directrices applicables au secteur public de l'article 95* indiquent donc en général suivant quelle procédure et quelles normes les comités d'éthique des institutions peuvent accorder des exemptions et donc lever l'obligation générale du consentement à l'utilisation et à la communication de données de personnes identifiables qui est applicable en matière de recherche médicale dans le secteur public. Les lignes directrices font cela en imposant aux chercheurs une procédure à suivre et aux HREC des normes d'évaluation correspondantes. La norme matérielle d'évaluation de la demande d'un chercheur découle de l'article 95 du *Privacy Act révisé*; il faut répondre à la question suivante : l'intérêt public que revêt la recherche l'emporte-t-il « dans une grande mesure » sur l'intérêt public qu'il y a à protéger la vie privée en adhérant aux conditions posées par les principes?

Les obligations des chercheurs sont donc fonction des renseignements recherchés et elles déterminent quelle forme prendra la demande adressée au HREC. L'article 2 des Lignes directrices exige que le chercheur adresse une proposition écrite à un HREC en indiquant l'objet de la recherche, les emplois précis qu'il prévoit faire des renseignements personnels, les raisons pour lesquelles il a besoin de données de personnes identifiables ou potentiellement identifiables plutôt que de données dépersonnalisées, la raison pour laquelle le consentement des intéressés ne peut être obtenu, la durée estimée de conservation des renseignements et les normes de sécurité qui assureront l'intégrité de cette conservation. Si le projet de recherche suppose la contravention des principes, le chercheur doit faire référence aux dispositions particulières auxquelles il sera

[38] La « recherche médicale » englobe la recherche épidémiologique.

contrevenu et dire pour quelles raisons l'intérêt public que revêt la recherche l'emporte sur celui de la protection de la vie privée.

Lorsqu'il évalue une demande de recherche médicale à effectuer sans consentement, le HREC doit se conformer à certaines exigences de base, tant de fond que de procédure. L'article 3.1 des Lignes directrices exige du HREC qu'il s'assure qu'il possède suffisamment d'informations, d'expertise et de compréhension au regard des questions de protection de la vie privée. L'article 3.2 fait obligation au HREC qui se prépare à approuver un projet de recherche de tenir compte, entre autres, du nombre de IPP auxquels il sera contrevenu et de se demander s'il est vraiment « nécessaire » d'utiliser des données de personnes identifiables ou potentiellement identifiables et d'effectuer la recherche sans le consentement des intéressés, et si, enfin, l'intérêt public que revêt la recherche l'emporte « dans une grande mesure » sur la protection des renseignements personnels. L'article 3.3 donne toute une série de facteurs à évaluer pour peser ces « intérêts publics », dont les progrès de la recherche médicale, les avantages pour les particuliers et le degré, minime ou non, de tort qui risque d'être causé aux intérêts du droit individuel à la vie privée.

### f. Conservation et sécurité des données

*Les Lignes directrices applicables au secteur public de l'article 95* demandent l'observation de normes de base de conservation et de protection des renseignements personnels. Les lignes directrices exigent par exemple que les données soient conservées « avec au moins le même degré de sécurité » que celui exigé par les normes énoncées dans le *Joint National Health and Medical Research Council/Australian Vice-Chancellors' Committee Statement and Guidelines on Research Practice* (l'Exposé conjoint et les Lignes directrices de pratique pour la recherche du NHMRC et de l'Australian Vice-Chancellors' Committee, ci-après dénommés le *Joint NHMRC/AVCC Statement)*. Entre autres, selon ce document, la gestion des données doit être généralement conforme aux normes applicables à la protection de la vie privée, le ministère ou les services de recherche doivent établir une procédure de conservation, d'accès et de sécurité pour les données; les données doivent être enregistrées sous une forme durable, correctement référencée, et elles doivent être conservées « suffisamment longtemps » pour qu'on puisse, par exemple, s'y reporter après la publication des résultats de la recherche. Dans ce dernier cas, le document recommande un délai de cinq à quinze ans de conservation après la publication selon le type de recherche. Le *Joint NHMRC/AVCC Statement* impute également une responsabilité professionnelle générale aux enquêteurs, afin de garantir une « sécurité suffisante » au traitement des données.

(Il n'y a pas de rubrique « Autres dispositions intéressantes » concernant les Lignes directrices adoptées en vertu de l'article 95 du *Privacy Act 1988*.)

## 2B. L'élaboration de lignes directrices sur la protection de la vie privée à l'intention du secteur privé

Le *Privacy Act révisé* comporte deux articles autorisant le Commissaire fédéral à la protection de la vie privée de l'Australie à publier ou à approuver des lignes directrices pour la recherche effectuée dans le secteur privé. Semblable à l'article 95, l'article 95A de la Loi autorise le Commissaire à approuver les lignes directrices publiées par le NMHRC pour la recherche en santé. Le NMHRC n'en a pas adoptées jusqu'à maintenant mais, en attendant, le Commissaire à la protection de la vie privée se fonde sur un autre article du *Privacy Act révisé*, l'article 27, qui lui permet de publier des lignes directrices au sujet des NPP. C'est ainsi que, au printemps 2001,

le Commissaire a rendu public un document de consultation sur d'éventuelles lignes directrices pour la recherche en santé dans le secteur privé en se fondant sur l'article 27. Ce document, intitulé *Draft Health Privacy Guidelines*[39] (Projet de Lignes directrices pour la protection des renseignements personnels de la recherche en santé), est destiné à susciter un débat public aux fins d'arrêter des lignes directrices définitives en 2001-2002. Une fois arrêtées, ces lignes directrices faciliteront l'interprétation des règles générales applicables à la recherche en santé dans le secteur privé et viendront s'ajouter aux normes régissant la collecte, l'utilisation et la communication non consenties de données de personnes identifiables en vertu des principes 2 et 10 des NPP (voir plus haut).

## B. La France

Les tendances et nationales et internationales ont eu des répercussions sur l'évolution de la protection de la vie privée et de la législation française concernant la protection des données. La France a signé la *CEDH* dans les années 50. Comme il a été dit plus haut, dans la Deuxième partie, en B, l'article 8 de la *CEDH* oblige ses membres à respecter la vie privée et la vie familiale. La France fait aussi partie de l'Organisation de coopération et de développement économiques depuis le début des années 60 et elle a adopté les *Lignes directrices de l'OCDE*. Membre du Conseil de l'Europe, la France a signé et ratifié la *Convention 108/1981 du CE* au début des années 80. Membre de l'Union européenne, elle doit rendre ses lois conformes à la *Directive de l'UE relative aux données à caractère personnel*.

En raison de ces obligations internationales, le gouvernement français a pris toutes sortes de mesures législatives au cours des ans pour mettre en œuvre diverses normes destinées à assurer le respect de la vie privée et la protection des données. Par exemple, l'article 9 du *Code civil français*[40] proclame que toute personne a droit au respect de sa vie privée. Le Conseil Constitutionnel a jugé que le droit à la vie privée est protégé de façon implicite par la *Constitution* française[41]. De récentes modifications aux codes de déontologie ont accru les obligations, morales et légales, applicables en matière de confidentialité. Par exemple, les articles 4 et 72 du *Code de Déontologie médicale*[42] obligent les médecins à s'assurer que les personnes qui les assistent se conforment à une obligation professionnelle de confidentialité dont le *Code pénal*[43] punit la transgression. En outre, au cours des deux dernières décennies, la France a adopté des lois sur la protection des données et sur la recherche biomédicale qui régissent l'utilisation des renseignements personnels. Voici un aperçu de la législation française sur la protection des données.

---

39 Australia, Privacy Commissioner. *Draft Health Privacy Guidelines*. Canberra, 14 may 2001. Site Web : www.privacy.gov.au

40 *Code Civil*. Site Web: www.legifrance.gouv.fr/citoyen/new_code.ow

41 Décision 94-352 du Conseil Constitutionnel du 18 janvier 1995.

42 *Code de Déontologie médicale*. Site Web : http : //www.legifrance.gouv.fr/citoyen/new_code.ow

43 *Code pénal*. Site Web : www.legifrance.gouv.fr/citoyen/new_code.ow

## 1. La *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

La législation française sur la protection des données remonte à la fin des années 70 à tout le moins, lorsque l'Assemblée nationale adopta la *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (la Loi 78-17)*[44]. La *Loi 78-17* est entrée en vigueur avant la plupart des normes internationales sur la protection des données mentionnées plus haut, dans la Troisième partie. Elle a été modifiée à plusieurs reprises. Même si d'autres lois contiennent des normes qui ont trait aux renseignements personnels, c'est la *Loi 78-17* qui demeure la plus importante en France pour la protection de ces renseignements. Les normes de protection des données qu'elle contient et le contrôle exercé par la Commission nationale de l'informatique et des libertés (la CNIL)[45] expliquent ce rôle important. Comme on le verra, de récentes modifications apportées à cette loi ont ajouté des normes de protection pour les données particulières de la recherche en santé.

### a. Champ d'application

La *Loi 78-17* porte de façon générale sur la collecte, l'enregistrement et la conservation des renseignements personnels. Au départ, elle s'appliquait aux données traitées par des systèmes automatisés et informatiques, mais des modifications subséquentes ont étendu son champ d'application ces dernières années. Les articles 45 et 46 étendent désormais l'application des dispositions clés de la loi aux « fichiers non automatisés ou mécanographiques ». Ces dispositions permettent aussi au gouvernement d'appliquer la *Loi 78-17* à des secteurs particuliers par décrets. L'article 4 prévoit que la *Loi 78-17* s'applique aux personnes morales et physiques. Malgré cette portée élargie, il faut noter qu'en vertu de l'article 40-1, la *Loi 78-17* ne s'applique pas aux données traitées aux fins d'un traitement médical. Le traitement des données ayant pour fin la recherche effectuée dans le cadre du suivi thérapeutique ou médical des patients n'est pas régi non plus par cette loi.

### b. Définitions

La *Loi 78-17* définit quelques termes importants. Par exemple, l'article 4 dit que les « informations nominatives » sont des informations qui « permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent ». De plus, il est mentionné à l'article 5 que les termes « traitement automatisé » désignent « des moyens automatiques relatifs à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ». La *Loi 78-17* a été modifiée pour y ajouter des dispositions sur la recherche dans le domaine de la santé, mais les terme « recherche » n'y est pas défini explicitement.

### c. Protections spéciales : données sensibles

La *Loi 78-17* protège davantage certaines données sensibles. L'article 31 interdit de façon générale la collecte ou la conservation de données sensibles nominatives sans l'accord exprès de la personne concernée. Il y est fait référence à l'information sur l'origine raciale, sur les opinions politiques, philosophiques ou religieuses ou sur les appartenances syndicales. Contrairement à la *Directive de l'UE relative aux données à caractère personnel* et à la *Convention 108/1981 du CE* (voir plus haut, dans la Troisième partie), la liste ne renvoie pas aux renseignements sur

---

[44] Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés; *Journal Officiel*, 7 janvier 1978, modifiée. Site Web : www.legifrance.gouv.fr/

[45] La Commission nationale de l'informatique et des libertés de France. Site Web : www.cnil.fr

la santé de l'individu. Cette omission est importante, car les données sensibles sont protégées de manière accrue par l'article 29 qui interdit en général leur usage par des tiers, tandis que leur conservation en mémoire informatisée sans l'accord exprès de l'intéressé est interdite par l'article 31. Il n'en reste pas moins, comme il est indiqué plus bas, que la révision de 1994 a introduit dans la *Loi 78-17* des dispositions particulières visant la recherche en santé faite à l'aide d'informations nominatives concernant la santé.

### d. Consentement : collecte, utilisation et communication des données

Certaines des dispositions de la *Loi 78-17* concernant le traitement des données ressemblent à celles de la *Directive de l'UE relative aux données à caractère personnel*, alors que d'autres s'en éloignent. Cela est peut-être dû au fait que la *Loi 78-17* fut adoptée avant la *Directive de l'UE relative aux données à caractère personnel*. En 1994, toutefois, la *Loi 78-17* a été révisée en profondeur pour la rendre applicable à la recherche dans le domaine de la santé[46.]. Le *Décret 95-682 du 9 mai 1995* est venu compléter cette modification[47]. L'Assemblée nationale française s'est servie de cette révision pour promulguer, dans le cadre de la protection des données de la *Loi 78-17*, des dispositions particulières visant le traitement des renseignements personnels aux fins de la recherche médicale. Les normes et la procédure modifiées établissent une approche qui a des effets pour les chercheurs, pour les personnes qui font l'objet de recherche, pour la supervision administrative et pour les destinataires des données de la recherche effectuée dans le domaine de la santé.

L'article 40-1 autorise les chercheurs à traiter, dans la plupart des cas, des informations nominatives ayant pour fin la recherche en santé, mais ils doivent respecter certaines conditions. Aux termes de l'article 40-2, les chercheurs doivent présenter leur plan de recherche à un comité consultatif responsable du traitement des informations en recherche et en soins médicaux. La décision de ce comité doit être prise en tenant compte de la méthode de recherche et de la pertinence des informations nominatives requises pour atteindre les objectifs scientifiques. Les chercheurs doivent ensuite obtenir l'autorisation de la Commission nationale de l'informatique et des libertés (CNIL), un organisme indépendant composé de 17 membres chargés de mettre en œuvre les normes de protection des données, de les appliquer et d'en superviser l'application. La CNIL est chargée de veiller à ce que le traitement des informations nominatives conservées en mémoire informatisée soit adéquat et conforme à la *Loi 78-17*. Aux étapes de la conception et de la mise en œuvre de la recherche, l'article 40-3 impose, à moins d'exceptions prévues par la loi, une obligation générale de codification des données de santé nominatives avant leur transmission (voir plus bas, à la section e.). On ne doit communiquer ou publier les résultats de la recherche qu'après les avoir rendus anonymes. Les destinataires de ces données sont, en vertu de l'article 40-3, assujettis au secret professionnel dont la violation est passible de sanctions pénales. La CNIL, dans ses recommandations, a repris, en les élaborant, les obligations et les normes applicables en matière de confidentialité, de codage, de transmission et d'utilisation secondaire des données personnelles[48].

---

46 *Loi n° 94-548* du 1er juillet relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la *Loi n° 78-17 du 6 janvier relative à l'informatique, aux fichiers et aux libertés*. *Journal officiel* du 2 juillet 1994.

47 *Décret 95-682* du 9 mai 1995, *Journal officiel* du 11 mai 1995.

48 Voir, p.ex., la Commission nationale de l'informatique et des libertés. *Délibérations n° 97-008* du 4 février portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel. *Journal officiel* du 12 avril 1997.

La *Loi 78-17* révisée indique au moins trois cas où les normes régissant le consentement sont applicables. Dans un premier, comme il est dit à la section b, il doit y avoir consentement lorsqu'il y a conservation de données sensibles. Ensuite, deuxième cas, les normes et les droits au refus éclairé applicables au traitement des données dont fait usage la recherche effectuée dans le domaine de la santé sont spécifiés depuis la révision de 1994. L'article 40-4 accorde à l'individu un droit d'opposition générale au traitement des données nominatives recueillies pour la recherche en santé. L'article 40-5 accorde le droit d'être informé, avant le début du traitement des données, à des fins de recherche en santé, notamment de la finalité du traitement des données, de la nature des informations communiquées, des destinataires probables, etc. Dans le cas où la recherche nécessite des prélèvements biologiques identifiants, l'article 40-4 exige l'accord éclairé et exprès des personnes concernées. Il autorise même le traitement d'informations concernant des morts, sauf si l'intéressé a, de son vivant, exprimé son opposition par écrit. Enfin, troisième cas, les normes régissant le consentement sont également applicables à l'utilisation secondaire des données. L'article 28 interdit de façon générale l'usage non consensuel des données à d'autres fins que l'objectif initial pour lequel elles ont été recueillies. Cependant, cette règle est assujettie à certaines exceptions (voir plus loin, à la section e).

### e. Exceptions et recherche

Les normes actuelles sur le traitement des données personnelles nominatives comportent au moins trois exceptions importantes au sujet de la recherche en santé. En premier lieu, l'article 40-3 autorise une dérogation à l'obligation générale de codage, avant leur communication, des données permettant l'identification dans les cas suivants : lorsque cette identification est requise pour réaliser des études pharmacologiques, lorsque les protocoles de recherche l'exigent et lorsque les données doivent servir à un effort de recherche national ou international spécial, fait en collaboration. En second lieu, l'article 40-5 peut être invoqué pour autoriser l'utilisation secondaire de données sans le consentement de la personne concernée lorsqu'il est difficile de communiquer avec cette dernière. Enfin, en troisième lieu, l'article 28 permet la conservation non consensuelle des informations à des « fins historiques, statistiques ou scientifiques »[49]. Cette conservation doit être conforme à la *Loi relative aux archives*[50].

### f. Conservation et sécurité des données

Les articles 28 et 29 traitent des exigences minimales en matière de mesures de sécurité et de durée de conservation des données. L'article 28 prévoit qu'on ne peut pas, en général, conserver des informations sous une forme nominative au-delà de la durée nécessaire à la réalisation des objectifs pour lesquels elles ont été recueillies ou traitées. Comme il a été mentionné, l'article 28 prévoit une exception à cette règle pour les informations conservées à des « fins historiques, statistiques ou scientifiques ». L'article 29 impose un devoir général de prudence, de prendre toute précaution utile afin de prévenir l'accès non autorisé, la communication ou la déformation des données. En complément, la CNIL a recommandé que l'on chiffre ou mélange les informations lorsque les systèmes de données requièrent des mises à jour et des suivis réguliers[51]. Les

---

[49] Comparez avec l'article 8 de la *Directive de l'UE relative aux données à caractère personnel* et avec l'article 9 de la *Convention n° 108/1981 du CE* traitées plus haut, dans la Troisième partie.

[50] *Loi n° 79-18 du 3 janvier 1979 relative aux archives*, art. 4-1. *Journal officiel* du 5 janvier 1979 : 49; corrigé dans le *Journal officiel* du 6 janvier 1979 : 55. Site Web : www.cnil.fr/textes/text052.htm

[51] La Commission nationale de l'informatique et des libertés. *Délibérations n° 97-008* du 4 février 1997 portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel. *Journal officiel* du 12 avril 1997.

mesures de sécurité accrues mises en place pour les données médicales sont également assujetties aux contrôles de la CNIL.

### g. Autres dispositions intéressantes

Il y a aussi, dans *Loi 78-17*, des dispositions destinées à assurer la mise en œuvre des mesures de protection de la vie privée. Les trois exemples suivants décrivent la nature de ces dispositions.

D'abord l'article 40-9 prévoit que les données nominatives sur la santé ne peuvent être transmises, dans le cadre de la collaboration à la recherche internationale, à un État destinataire dont la législation n'accorde pas une protection équivalente à la loi française en matière de protection des données personnelles. Cet article est conforme à la *Directive de l'UE relative à la protection des données à caractère personnel*.

Ensuite, les articles 6 à 33 traitent de la création et des fonctions de la CNIL. Certaines de ses responsabilités ont déjà été mentionnées. Ses fonctions principales, d'ordre réglementaire, consistent, notamment : à autoriser les institutions publiques à traiter diverses données particulières, à enregistrer et à surveiller le traitement des données fait dans le secteur privé, à indiquer des normes simplifiées, à donner des avis sur le traitement des données, à ouvrir des enquêtes au sujet des plaintes écrites d'atteintes à la vie privée éventuellement portées, et à donner des avis au gouvernement[52] sur la réforme du droit de la protection des données.

Enfin, la société française a eu recours au droit pénal pour faire avancer la cause de la protection de la vie privée en ce qui avait trait au traitement automatisé des informations nominatives. Les dispositions servant à atteindre cet objectif se retrouvent dans la *Loi 78-17* elle-même et au *Code pénal*, qui a été révisé le 16 décembre 1992. Des sanctions pénales peuvent être infligées pour le traitement frauduleux ou illégal de données, l'atteinte à leur sécurité, leur conservation sans consentement, leur conservation au-delà du délai réglementaire, ainsi que leur usage non autorisé et leur communication illicite. Ces dispositions peuvent nous aider à comprendre pourquoi certains considèrent le droit français[53] comme un bel exemple de protection stricte de la vie privée et du secret médical.

## 2. *La mise en œuvre de la Directive de l'UE relative à la protection des données à caractère personnel : la Loi sur la société de l'information*

À l'instar de nombreux autres membres de l'Union européenne, la France a récemment pris des mesures législatives pour recevoir la *Directive de l'UE relative à la protection des données à caractère personnel* dans son droit national[54]. Pour parvenir à cet objectif, l'Assemblée nationale française étudie présentement un projet de loi qui, une fois adopté, s'intitulera *Loi sur la société de l'information*. On propose par cette loi de modifier la *Loi 78-17*, la loi actuelle sur la protection des données. Ce projet de loi prévoit entre autre : a) un élargissement de la portée de certains droits; b) la simplification des normes; c) le renforcement des pouvoirs et des ressources de la CNIL; d) l'harmonisation enfin des normes de traitement des données applicables au secteur

---

52 Décret n° 78-774, du 17 juillet 1977. Journal officiel *du 23 juillet 1997, art. 20, 3E$^0$*

53 J.K. Mason & R.A. McCall Smith, *Law and Medical Ethics*, 4e éd., Butterworth's, Londres, 1994 : p.169. *Journal Officiel* du 11 mai 1995.

54 Guy Braibant, *Données personnelles et société de l'information: Rapport au Premier Ministre sur la transposition en droit français de la directive n° 95/46.* Paris, 1998.

public et de celles applicables au secteur privé[55]. On s'attend à ce que la loi soit adoptée en 2001–2002.

## C. Les Pays-Bas

L'évolution des règles de protection des données aux Pays-Bas est le reflet des obligations internationales contractées par ce pays et des engagements qu'il a pris sur le plan intérieur pour protéger la vie privée de l'individu. Au cours des années 50, les Pays-Bas ont signé et ratifié la *CEDH*. Comme il a été dit plus haut, dans la Troisième partie, il est reconnu dans la *CEDH* que le respect de la vie privée est un droit fondamental, qui ne peut faire l'objet d'ingérence qu'aux fins des nécessités raisonnables de la démocratie. Membre de l'Organisation de coopération et de développement économiques (OCDE) dès le début des années 60, les Pays-Bas ont ainsi eu formellement la possibilité d'examiner et de mettre en œuvre les *Lignes directrices de l'OCDE*. En tant que membre de l'Union européenne, les Pays-Bas sont également tenus d'harmoniser leur législation nationale avec la *Directive de l'UE relative aux données à caractère personnel*.

Les obligations juridiques qui découlent de ces relations internationales semblent s'être concrétisées sous la forme d'au moins deux initiatives juridiques officielles prises par les Pays-Bas au cours des quinze dernières années. Les Pays-Bas sont par exemple l'un des rares pays étudiés dont la constitution protège expressément le droit à la vie privée. De plus, la disposition accordant la protection constitutionnelle au droit à la vie privée exige expressément l'adoption de « règles de protection de la vie privée » sous forme de loi « concernant la saisie et la communication des données personnelles »[56]. Le Parlement des Pays-Bas a mis en œuvre cette exigence constitutionnelle en adoptant une loi omnibus sur la protection des données en 1988[57]. Plus de dix ans plus tard, une autre loi sur la protection des données a été adoptée. En voici les principales dispositions.

### 1. *Wet bescherming persoonsgegevens (la Loi de l'an 2000 sur la protection des données personnelles)*

En juillet 2000, la *Wet bescherming persoonsgegevens (*la *Loi sur la protection des données personnelles)* (la LPDP)[58] a été adoptée par le Parlement. Cette loi met à jour et remplace la loi initiale de 1988 sur la protection des données mettant en œuvre la *Directive de l'UE relative aux données à caractère personnel*. L'application de cette loi est surveillée par la Commission de protection des données.

---

55 Site Web : www.internet.gouv.fr/

56 Art. 10 de la *Constitution du Royaume des Pays-Bas* de 1989.

57 *Wet persoonsregistraties (Loi sur l'enregistrement des données personnelles)*. 28 décembre 1988. Loi hollandaise de 1988 sur l'enregistrement des données. Site Web: http://home.planet.nl/~privacy1 Voir également Ploem M.C. Medical Research and Informational Privacy, *Medicine and Law* 1998,17, pp. 287-297.

58 *Wet bescherming persoonsgegevens (Loi sur la protection des données personnelles)*. 6 juillet 2000. Staatsblad 2000 302. Sites Web: http://www.registratiekamer.nl; http://home.planet.nl/~privacy1. *Wet geneeskundige behandelingsovereenkomst* (*Loi sur le contrat médical,* Loi du 17 novembre 1994, modifiant le Code civil et d'autres lois relativement à l'incorporation de dispositions concernant le contrat de traitement médical). Stp 1994, p. 837. *Wet geneeskundige behandelingsovereenkomst* (*Loi sur le contrat médical*), 17 novembre 1994, Stb 1994. L'article 458 autorise l'accès aux données, notamment, si : a) le consentement ne peut raisonnablement être demandé et que des garanties sont données pour circonscrire l'atteinte à la vie privée; b) la recherche s'effectue dans l'intérêt public et ne peut être effectuée sans ces renseignements; c) le malade ne s'est pas expressément opposé à ce que ces renseignements soient fournis.

### a. Champ d'application

L'article 2 de la *LPDP* en définit le champ d'application. La *LPDP* s'applique aux données personnelles saisies par les systèmes de traitement automatisés, automatisés en partie, ou non automatisés, ou saisis en vue de constituer un fichier. Elle s'applique au traitement des données dans les deux secteurs, public et privé, des Pays-Bas, ainsi qu'aux personnes se trouvant à l'extérieur de l'UE qui utilisent des moyens de traitement de données situés aux Pays-Bas.

### b. Définitions

La *LPDP* définit plusieurs termes, notamment « données personnelles », « traitement » et « consentement ». Constituent des « données personnelles » les renseignements « relatifs à une personne physique identifiée ou susceptible de l'être ». La définition ne précise pas ce qu'il faut entendre par « identifiée ». La *LPDP* définit largement le « traitement »; ce terme comprend la collecte, l'enregistrement, la structuration, l'entreposage, la mise à jour, la modification, l'extraction, la consultation, l'utilisation, la diffusion, la fusion, l'enchaînement, l'effacement ou la destruction de données.

### c. Protections spéciales : données sensibles

La LPDP prévoit des mesures de protection renforcées pour diverses catégories particulières de données personnelles, notamment les renseignements relatifs à la santé. L'article 16 crée une interdiction générale à l'encontre du traitement des données personnelles relatives, notamment, à la religion, à la race, aux convictions politiques, au comportement criminel, illégal ou répréhensible, à la santé et à la vie sexuelle. L'article 23 prévoit des exceptions à cette interdiction, fondées sur divers motifs dont le consentement exprès de la personne concernée, ou lorsque cela est « nécessaire » aux fins d'instances judiciaires ou pour protéger des « d'importants intérêts publics ». Ces exceptions s'accompagnent de mesures de protection de la vie privée appropriées ou encore par une exemption accordée par la Commission de protection des données qui doit en être assortie. Les autres exceptions pertinentes en ce qui a trait à la recherche en santé sont décrites ci-dessous.

### d. Consentement : collecte, utilisation et communication des données

La LPDP reprend la plupart des normes générales de traitement des données prévues par les *Lignes directrices de l'OCDE*, modifiées par la *Directive de l'UE relative aux données à caractère personnel*. L'article 7 s'inspire de l'alinéa 6b) de la *Directive de l'UE relative aux données à caractère personnel* en prévoyant que les données personnelles doivent être « recueillies pour des fins déterminées, explicitement définies et légitimes ». L'article 9 vient compléter cette obligation générale et interdire tout traitement « qui serait incompatible avec les fins pour lesquelles elles [les données] ont été obtenues ». Sont ensuite énumérés une série de facteurs permettant de déterminer si un traitement subséquent est « incompatible ». Comme nous l'avons noté ci-dessous, le traitement à des « fins scientifiques » n'est pas considéré comme étant incompatible s'il y est procédé dans certaines conditions particulières.

L'article 8 indique quelle est la norme de base qui régit le traitement des données : l'exigence générale est le consentement « non ambigu » de la personne concernée. Le consentement est défini à l'article 1er comme étant un « accord précis et informé, donné librement » au traitement des données personnelles. L'article 23, comme cela a été dit plus haut, prévoit une exception à l'interdiction du traitement des données personnelles lorsqu'il s'effectue avec le « consentement exprès » de la personne concernée.

### e. Exceptions et recherche

La LPDP prévoit également qu'il peut y avoir traitement non consensuel de données, à des fins de recherche en sciences et en santé. En voici quatre exemples.

L'article 21, premier exemple, porte que l'interdiction générale de traitement non consensuel des données personnelles sur la santé ne s'applique pas lorsque le traitement est effectué par des professionnels de la médecine ou par des institutions hospitalières lorsque cela est « nécessaire » à la dispensation de soins à la personne concernée, aux fins de l'administration de l'institution ou à celles de l'exécution des tâches professionnelles en cause.

Le paragraphe 34(4), second exemple, relève les institutions de leur obligation de renseigner les personnes concernées par les données lorsque cela « semble être impossible ou exigerait un effort disproportionné ». Dans de tels cas, l'article 44 indique que le traitement des données n'est assujetti à aucune obligation particulière de communication d'information.

Troisième exemple : l'article 9 de la LPDP prévoit une exception expresse à l'interdiction générale de toute « utilisation incompatible » non autorisée ou non consensuelle des données personnelles. Le traitement ultérieur des données personnelles est toutefois réputé ne pas constituer un « but incompatible », s'il est fait à des « fins historiques, statistiques ou scientifiques ». Des arrangements particuliers doivent être pris pour limiter le traitement ultérieur aux fins énumérées. L'exception de l'article 9 comporte d'autres conditions. Aux termes de l'article 9, le traitement « ne peut s'effectuer lorsqu'il est interdit par une obligation de confidentialité découlant d'une disposition juridique ou d'une règle professionnelle ». Or, comme le *Wet geneeskundige behandelingsovereenkomst* (la *Loi sur le contrat médical*) impose aux médecins qui donnent un traitement médical des obligations particulières de confidentialité, ses dispositions peuvent s'appliquer également à certaines utilisations en recherche des données concernant les malades. Par exemple, cette dernière loi autorise, dans des cas strictement limités, l'accès non consensuel à des renseignements sur la santé à des fins de recherches statistiques et scientifiques reliées à l'hygiène publique.

Quatrième et dernier exemple, l'article 23 prévoit une exception étroite à l'exigence générale du consentement au traitement des données personnelles relatives à la santé, à des fins de « statistique ou de recherche scientifique ». Les conditions suivantes doivent être remplies : a) la recherche doit être effectuée dans l'intérêt public; b) le traitement doit être « nécessaire » pour effectuer la recherche ou pour recueillir des données statistiques; c) le consentement exprès de la personne concernée doit être soit « impossible » à obtenir, soit exiger un « effort disproportionné »; d) des garanties suffisantes permettant de s'assurer que le traitement « ne porte pas atteinte de façon disproportionnée à la vie privée de la personne concernée » doivent être prévues. Le paragraphe 21(4) impose des critères tout aussi restrictifs pour la recherche statistique et scientifique concernant les données génétiques personnelles pour lesquelles le chercheur ne possède pas le consentement exprès de la personne concernée.

### f. Conservation et sécurité des données

La LPDP impose également certaines obligations générales en matière de conservation et de mise en sécurité des données. L'article 10 prévoit, conformément aux *Lignes directrices de l'OCDE*, qu'en général les données personnelles ne doivent pas être conservées pour une période plus longue que celle qui est nécessaire pour réaliser le but pour lequel elles ont été recueillies puis traitées. Comme il a été dit plus haut, cette norme est assujettie à une exception : les « fins historiques, statistiques ou scientifiques », lorsque la partie responsable a pris les

dispositions nécessaires pour que les données soient utilisées uniquement à ces fins. Les articles 12 à 14 imposent un devoir général de confidentialité aux personnes qui traitent des données personnelles et ils exigent en outre que des mesures de sécurité et d'ordre technique « appropriées » soient prises pour éviter la perte, la destruction et le traitement inutile ou illicite des données.

### g. Autres dispositions intéressantes

Plusieurs dispositions de la LPDP ont pour but d'en assurer la mise en œuvre en conformité avec la *Directive de l'UE relative aux données à caractère personnel* et à répondre aux besoins sociétaux des Pays-Bas. La *LPDP* a, par exemple, créé la Commission de protection des données, laquelle est chargée de l'appliquer et d'en surveiller la mise en œuvre. La Commission est notamment autorisée à donner des avis sur la réforme des lois de protection des données, à ouvrir des enquêtes au sujet des plaintes d'atteinte à la vie privée qui sont portées, et à s'assurer que l'on se conforme à la LPDP. L'attribution de ces responsabilités répond à une exigence de la *Directive de l'UE relative aux données à caractère personnel*, qui demande de confier à un organisme indépendant de surveillance la supervision de l'application des principes nationaux de protection des données.

Deux autres dispositions concernant les attributions générales de la Commission sont intéressantes. La première : l'article 25 de la *LPDP*. Aux termes de cet article, la Commission a le pouvoir d'approuver les codes de déontologie qu'elle estime conformes aux principes et aux obligations juridiques de la LPDP. Ces codes de déontologie peuvent être adoptés par les institutions de différents secteurs de la société et soumis à la Commission. La deuxième : les articles 51 et 52. Ils attribuent à la Commission un rôle de surveillance du traitement des données personnelles lorsque le traitement est effectué en conformité avec la loi d'un autre pays de l'Union européenne. L'article 76 interdit de façon générale le transfert de données personnelles à l'extérieur de l'Union européenne à moins que le pays destinataire ne garantisse un niveau « suffisant » de protection. L'appréciation du niveau de protection doit tenir compte des circonstances entourant l'opération de transfert des données ou de la catégorie de données. Il y a lieu de tenir compte en particulier du type de données transférées, du ou des objectifs recherchés, de la durée du traitement ou des opérations de traitement prévus, du pays d'origine et du pays de destination ultime, des dispositions juridiques générales et sectorielles applicables dans le pays extérieur à l'UE concerné, ainsi que des règles régissant le secteur commercial, et la sécurité, en vigueur dans ces pays.

## D. La Nouvelle-Zélande

Membre de l'Organisation de coopération et de développement économiques depuis les années 70, la Nouvelle-Zélande a ainsi eu formellement la possibilité d'examiner les *Lignes directrices de l'OCDE* et d'en envisager l'adoption. C'est l'un des nombreux pays qui ont signé et ratifié le *PIDCP*; la Nouvelle-Zélande a donc pris l'engagement international formel de respecter les droits de la personne, y compris le droit à la vie privée. Fidèle à ces deux traditions et à leur conception de la recherche en santé, la Nouvelle-Zélande a pris d'importantes mesures pour la protection des données au cours des années 90.

En 1993, elle a promulgué une loi nationale de protection des données : le *Privacy Act 1993*. Un an plus tard, elle adoptait le *Health Information Privacy Code* (le HIPC). Un aperçu du contenu de ces

textes est donné ci-après. Comme les deux documents établissent de nombreuses normes parallèles, voire identiques, l'analyse plus étendue des normes identiques est parfois reportée à l'analyse du *Health Information Privacy Code*.

## 1. Le *Privacy Act 1993* [Loi sur la vie privée]

Le *Privacy Act 1993*[59] de Nouvelle-Zélande, dont l'application est surveillée par un commissaire à la vie privée indépendant, est une loi générale de protection des données ayant comme objet principal l'institution, de par la loi, de contrôles de la façon dont les organismes publics et privés recueillent, utilisent et communiquent les renseignements personnels. Le *Privacy Act 1993* s'inspire des *Lignes directrices de l'OCDE* de 1980 et des IPP du *Privacy Act 1988* de l'Australie[60]. En raison, d'une part, du réexamen systématique qui doit être fait des lois nationales et, d'autre part, de la nécessité d'adapter la nouvelle Loi à des normes internationales plus récentes (par exemple celles de la *Directive de l'UE relative aux données à caractère personnel*), on a discuté longuement, au cours des dernières années, de l'opportunité de modifier certaines des dispositions de la Loi.

### a. Champ d'application

Le *Privacy Act 1993* régit tous les « renseignements personnels » tels qu'ils sont définis plus bas. Cela englobe les données automatisées et du secteur public et du secteur privé.

### b. Définitions

L'article 2 définit plusieurs concepts essentiels au fonctionnement de la Loi. Par exemple, les « renseignements personnels »[61] sont définis comme étant des renseignements concernant une personne identifiable, et ils englobent les renseignements contenus dans les registres de décès. Une « personne » est définie comme étant toute personne physique vivante, ce qui signifie que la Loi s'applique en général à tous les renseignements personnels concernant des personnes vivantes. Il y a des exceptions à cette règle. Selon le paragraphe 46(6), aux fins d'un code de pratique relatif aux renseignements sur la santé, les renseignements personnels englobent ceux qui ont trait aux vivants et aux morts. Ce que sont ces codes de pratique est expliqué plus loin. Le *Privacy Act 1993* ne définit pas directement ce qu'il faut entendre par « renseignements sur la santé », mais elle renvoie indirectement à la définition énoncée dans une autre loi néo-zélandaise[62]. On y précise par ailleurs qu'elle s'applique aux « organisations », qui sont généralement définies comme étant une personne ou un ensemble de personnes, constituées ou non en société, dans le secteur public ou le secteur privé.

### c. Protections spéciales : données sensibles

Le *Privacy Act 1993* ne comporte pas de dispositions expresses concernant les « données sensibles ». Elle fait donc comme les *Lignes directrices de l'OCDE* originelles. Mais dans le HIPC adopté en vertu du *Privacy Act 1993*, certaines dispositions portent sur le traitement de

---

59 *Privacy Act 1993* de la Nouvelle-Zélande. Site Web : http://www.privacy.org.nz/recept/rectop.html

60 Basinar D., *Privacy and Human Rights : An International Survey of Privacy Laws and Developments*, Epic, 2000, p. 162.

61 Dans *Re Application by L* (1997), 3 HNRX 716, le tribunal d'examen des plaintes a jugé que peut être considérée comme des renseignements personnels l'information traitée mentalement.

62 Paragraphe 22B de la *Health Act 1956.*

renseignements sur la santé de personnes identifiables (voir plus loin). De plus, l'opportunité d'inclure une protection expresse pour les données sensibles a récemment fait l'objet d'analyses et de discussions publiques dans le cadre de propositions de révision du *Privacy Act 1993*[63].

### d. Consentement : collecte, utilisation et communication des données

L'article 6 du *Privacy Act 1993* énonce 12 principes (les *Privacy Information Principles*) définissant les normes fondamentales de la Loi. Ces principes font écho à ceux que l'OCDE a adoptés en 1981 (voir plut haut dans la Troisième partie). Selon ces principes, les renseignements personnels doivent être :

- Recueillis à des fins licites et nécessaires seulement (principe 1);
- Recueillis directement auprès de la personne concernée (principe 2);
- Recueillis de façon que la personne concernée soit informée du traitement des données (principe 3);
- Recueillis selon des moyens licites, loyaux et raisonnables (principe 4);
- Conservés en sécurité (principe 5);
- Accessibles à la personne concernée (principe 6);
- Susceptibles de corrections par la personne concernée (principe 7);
- Vérifiés, pour s'assurer de leur exactitude, avant usage (principe 8);
- Conservés durant une période raisonnable (principe 9);
- Utilisés à des fins limitées (principe 10);
- Communiqués dans certains cas seulement (principe 11);
- Associés à des identificateurs uniques dans certains cas seulement (principe 12).

Les dispositions du *Privacy Act 1993* relatives au consentement ou à « l'autorisation » sont généralement identiques à celles du HIPC (voir l'analyse du Code plus loin).

### e. Exceptions et recherche

Les conditions générales régissant la collecte, l'utilisation et la communication des renseignements personnels sont, par exception, levées lorsqu'il s'agit de renseignements publics, ou que se conformer aux exigences du *Privacy Act 1993* est jugé à peu près impossible, que les données ne permettent pas d'identifier la personne concernée ou que leur utilisation est jugée « nécessaire » aux fins de la justice ou de la répression pénale ou pour éviter qu'un tort ou un préjudice imminents ne soient causé à la santé physique ou mentale d'une personne.

Il y a aussi certaines dispositions particulières qui sont applicables à la recherche. Comme elles sont pour l'essentiel identiques à celles du HIPC, elles sont analysées avec celles du Code plus bas.

Par ailleurs et plus généralement, l'article 54 du *Privacy Act 1993* prévoit que les organisations peuvent être autorisées par le Commissaire à la protection de la vie privée à recueillir ou à utiliser des renseignements personnels dans des conditions qui enfreignent parfois les principes applicables à la collecte (le principe 2), à l'utilisation (le principe 10) et à la communication (le principe 11). Pour obtenir ce genre d'autorisation, il faut que le Commissaire juge que toute ingérence dans la vie privée de l'intéressé est justifiée et compensée par un intérêt public substantiel ou par un avantage manifeste pour l'intéressé lui-même.

---

[63] Commissaire à la vie privée de Nouvelle-Zélande, *Discussion Paper nº 12 : New Privacy Protections*, Auckland, 1998. Site Web : http://www.privacy.org.nz/slegisf.html

### f. Conservation et sécurité des données

Les principes 5 et 9 sont, pour l'essentiel, repris des *Lignes directrices de l'OCDE* sur la conservation et la sécurité des données (voir plus haut dans la Troisième partie). Ils sont également pour la plus grande partie identiques aux conditions de sécurité et de conservation exigées par le HIPC (voir l'analyse du Code plus loin).

### g. Autres dispositions intéressantes

Le *Privacy Act 1993* comporte un certain nombre de dispositions applicables à la mise en œuvre concrète des principes et des normes de protection de la vie privée. Deux au moins sont particulièrement importants pour la recherche en santé.

L'une d'elles a trait à la mise en œuvre et à la surveillance par une instance de supervision indépendante : le Commissaire à la vie privée de Nouvelle-Zélande. Les principales fonctions du Commissaire sont : promouvoir les principes édictés par le *Privacy Act 1993* et examiner les projets de loi et les politiques gouvernementales pouvant avoir un effet sur la vie privée des particuliers; examiner le fonctionnement de la Loi; surveiller l'usage qui est fait des identificateurs uniques; approuver les exemptions aux principes; recevoir les plaintes, ouvrir les enquêtes pertinentes et faire office de conciliateur. Une deuxième disposition digne de mention a trait aux pouvoirs de réglementation spéciaux attribués au Commissaire. Il peut en effet publier des codes de pratique développant les normes que fixe la Loi ou les modifiant. Comme on le verra plus loin, c'est ce qu'il a fait au sujet des renseignements sur la santé.

## 2. Le *Health Information Privacy Code (HIPC) 1994* [Code de protection des renseignements personnels sur la santé]

L'article 46 du *Privacy Act 1993* donne au Commissaire à la vie privée de ce pays le pouvoir de publier des codes de pratique tenant compte des caractéristiques particulières de certains secteurs d'activité, de certaines organisations ou de certains types de renseignements personnels. Il prévoit expressément que ces codes peuvent modifier l'application des principes (les *Privacy Information Principles*) du *Privacy Act 1993*. Les codes peuvent prescrire des normes plus strictes, et même moins strictes, que les principes. Pour publier un code de pratique, le Commissaire doit d'abord faire paraître un avis public général de son intention, consulter ceux et celles dont les intérêts sont en cause et soumettre le code au Parlement de Nouvelle-Zélande, qui doit tenir un débat à son sujet avant qu'il ne puisse entrer en vigueur. Une fois entrée en vigueur, un code a force de loi. C'est en vertu de ce pouvoir et suivant cette procédure que le Commissaire à la vie privée a publié le *Health Information Privacy Code* (HIPC) de Nouvelle-Zélande en 1994[64]. Le Code a été révisé récemment, en l'an 2000. Comme on le verra, le vocabulaire du Code, ses normes et ses exceptions sont conçus spécifiquement pour le secteur de la santé.

### a. Champ d'application

Le HIPC réglemente la collecte, l'utilisation et la communication de renseignements de personnes identifiables sur la santé par les organismes publics et privés. Il s'applique donc aux fournisseurs des services de santé, aux écoles des métiers et des professions de la santé, à certaines institutions gouvernementales de la santé particulières, aux associations professionnelles de la santé et aux fabricants et distributeurs de médicaments et d'appareils médicaux.

---

[64] Commissaire à la vie privée de Nouvelle-Zélande, *Health Information Privacy Code*, modifié, Auckland, 1994; édition révisée, 2000. Site Web : http://www.privacy.org.nz/recept/rectop.html

### b. Définitions

L'article 4 du HIPC donne une définition large de l'expression « renseignements sur la santé » de personnes identifiables : elle englobe les renseignements concernant la santé, les antécédents médicaux, les handicaps et les tests de substances corporelles d'un particulier ainsi que les services médicaux qu'il a reçu.

### c. Protections spéciales : données sensibles

Comme le *Privacy Act 1993*, le HIPC ne considère pas explicitement que les renseignements de personnes identifiables sur la santé sont des « données sensibles » justifiant des protections particulières.

### d. Consentement : collecte, utilisation et communication des données

Le HIPC exige que la collecte de renseignements soit entreprise à des fins licites et qu'elle soit « nécessaire » à la réalisation de ces fins. La règle 2 prévoit de façon générale que les renseignements sur la santé doivent être recueillis « directement auprès de la personne concernée ». Selon la règle 3, les organisations qui recueillent des données doivent prendre des mesures suffisantes pour s'assurer que la personne concernée « sait », entre autres, à quoi et à qui vont servir les renseignements et si elle est obligée ou non de les donner. Le HIPC impose également une norme générale en faveur de la protection de la vie privée de l'individu eu égard aux identificateurs uniques. La règle 12 prévoit qu'il ne faut pas affecter à des particuliers des identificateurs uniques, à moins qu'il ne soient « nécessaires pour permettre à l'organisation de santé d'exercer » ses fonctions avec efficacité.

Rappelons que le HIPC n'emploie pas le terme « consentement » en tant que norme applicable à la collecte, à l'utilisation ou à la communication de renseignements personnels sur la santé. Il emploie plutôt le terme « autorisation ». C'est ainsi que les règles 10 et 11 assujettissent la « communication » et « l'utilisation » des renseignements sur la santé de personnes identifiables à une condition générale d'obtention de « l'autorisation » de la personne concernée ou de son représentant. Le terme « autorisation » n'est pas défini.

### e. Exceptions et recherche

Le HIPC prévoit un certain nombre d'exceptions aux conditions générales de traitement des renseignements personnels sur la santé de personnes identifiables. Elles concernent les normes de collecte, d'utilisation et de communication. Par exemple, le paragraphe 4 de la règle 3 prévoit que l'obligation générale de recueillir directement les renseignements sur la santé auprès de la personne concernée ne s'applique pas si l'organisation « a de bonnes raisons de croire » que cela « porterait atteinte à l'objet de la collecte » ou que ce n'est pas « raisonnable ». Le terme « raisonnable » n'est pas défini.

Les règles 10 et 11 prévoient des exceptions applicables spécifiquement à la recherche en santé. Elles permettent l'utilisation et la communication non consensuelles à certaines conditions. Par exemple, selon l'alinéa (1) e) de la règle 10, ni le consentement ni la nécessité ne sont des conditions requises pour l'utilisation des renseignements de personnes identifiables si l'organisation a « de bonnes raisons de croire » que ces renseignements ne permettent pas d'identifier les personnes concernées, si les données servent à des fins statistiques sans possibilité d'identification des personnes concernées ou si l'on s'en sert dans des conditions particulières « à des fins de recherche ». Ces conditions particulières supposent généralement qu'un comité d'éthique approuve l'utilisation en question et que les données « ne sont pas publiées sous une

forme qui, pourrait-on raisonnablement s'attendre, risquerait de permettre d'identifier les personnes concernées ».

L'alinéa (2)c) de la règle 11 prévoit des critères semblables pour la communication non consensuelle de données sur la santé « à des fins de recherche ». Cette règle s'applique s'il existe des raisons valables de croire qu'il n'est « ni souhaitable ni raisonnable d'obtenir l'autorisation » de la personne concernée. Lorsque ce genre de communication non consensuelle se justifie, la règle 11 impose cependant des restrictions : elle prévoit que la communication n'est permise « que dans la mesure nécessaire à la réalisation des fins en question ». Cette limitation est conforme à la conception étroite des exceptions, prévue à l'origine par les *Lignes directrices de l'OCDE*, puis reprise par des instruments comme la *Directive de l'UE relative aux données à caractère personnel.*

### f. Conservation et sécurité des données

Les règles 5 et 9 du HIPC établissent les conditions de conservation et de sécurité des données. La règle 5 impose l'obligation de protéger les renseignements sur la santé par « les sauvegardes de sécurité considérées comme raisonnables compte tenu des circonstances », afin de prévenir, par exemple, les pertes, les utilisations abusives ou les communications non autorisées. Elle impose également l'obligation de disposer des documents suivant des modes respectueux du droit à la vie privée de la personne concernée. La règle 9 exige que l'information soit conservée pour une période ne dépassant pas ce qui est nécessaire à l'objet de son usage licite. Les deux règles sont conformes aux principes de sécurité et de conservation des données des *Lignes directrices de l'OCDE* (voir plus haut à la Troisième partie). Rappelons également que si des renseignements sur la santé concernant une personne identifiable sont conservés par un professionnel de la santé, les normes de conservation des données énoncées dans d'autres lois de la Nouvelle-Zélande peuvent être applicables. La réglementation adoptée en vertu de certaines de ces lois, par exemple, peut exiger que les organisations de santé conservent les renseignements sur la santé durant dix ans au moins[65].

(Il n'y a pas de rubrique « Autres dispositions intéressantes » concernant le HIPC.)

## E. Le Royaume-Uni

Au cours des dernières années tout particulièrement, les relations officielles qu'entretient le Royaume-Uni (R.-U.) au sein de la communauté internationale ont favorisé une évolution du droit qui a fini par influer sur la recherche en santé. En fait, certaines de ces relations internationales et les obligations juridiques qu'elles supposent en Europe ont exercé une influence directe et importante sur les lois récentes de protection de la vie privée et des données au Royaume-Uni. Il en est ainsi à trois égards au moins.

Tout d'abord, à titre d'État membre du Conseil de l'Europe depuis des décennies, le Royaume-Uni a signé et ratifié la *CEDH* dans les années 1950, et la *Convention 108/1981 du CE* dans les années 1980. Les deux traités ont été analysés précédement (dans la Deuxième partie).

---

65 Voir le *Health (Retention of Health Information) Regulations 1996*, adopté en vertu du *Health Act 1956*.

Les obligations contractées par le R.-U. aux termes de la *CEDH* ont récemment contribué à faire adopter le *Human Rights Act*[66]. Cette Loi reproduit textuellement l'article 8 de la *CEDH* qui, ainsi, est reçue dans le droit du R.-U, ce qui rend davantage explicite dans la société britannique le « droit au respect de la vie privée », sous réserve de certaines limitations prévues par la loi et jugées « nécessaires dans une société démocratique (…) »

Ensuite, l'adhésion du R.-U., depuis les années 60, à l'Organisation de coopération et de développement économiques lui a donné officiellement la possibilité d'envisager la mise en oeuvre des *Lignes directrices de l'OCDE* et de s'y préparer. Comme on le verra, le R.-U. a procédé à cette mise en oeuvre en partie par le truchement d'initiatives nationales de protection des données dont, par exemple, la première loi sur la protection des données de 1984.

Enfin, le R.-U. est, depuis des décennies, membre de la Communauté économique européenne, devenue l'Union européenne, ce qui signifie qu'il a l'obligation d'intégrer les principes de la *Directive de l'UE relative aux données à caractère personnel* à ses pratiques nationales de protection des données. C'est ce qu'il a fait en partie en révisant sa loi initiale de protection des données et en promulguant un nouveau *Data Protection Act* (DPA) en 1998. Cette initiative a permis à son tour d'inciter des institutions de recherche du gouvernement et des associations professionnelles du secteur de la santé à actualiser et à publier de nouvelles lignes directrices d'éthique pour la recherche en santé. Voici quelques-uns des points saillants de la nouvelle DPA et des lignes directrices révisées du Medical Research Council et de la British Medical Association.

## 1. Le *Data Protection Act* (DPA) de 1998 *[*la *Loi sur la protection des données]*

Promulgué en juillet 1998 et entré en vigueur en mars 2000, le *Data Protection Act*[67] (DPA) est une mise à jour de l'ancienne loi britannique sur la protection des données qui aligna cette dernière sur les dispositions de la *Directive de l'UE relative aux données à caractère personnel*. L'application du DPA est surveillée par le Commissaire à la protection des données.

### a. Champ d'application

Le DPA s'applique aux renseignements personnels, c'est-à-dire aux données concernant des personnes identifiables traitées par les organisations du secteur public ou du secteur privé britanniques. À ce titre (et contrairement aux normes des Nations Unies), la Loi ne couvre pas les renseignements sur les morts. Selon la définition des termes renseignements personnels énoncée plus loin, les données rendues anonymes antérieurement ne font pas non plus partie du champ d'application du DPA.

### b. Définitions

Le DPA définit plusieurs termes et expressions, dont « données personnelles », « traitement » et « données sensibles ». Les « données personnelles » (article 1er), ce sont les renseignements identifiant une personne vivante. Ces renseignements peuvent être issus directement des données en question ou obtenus indirectement, c'est-à-dire lorsque les données sont, ou sont

66 Royaume-Uni, *Human Rights Act* 1998, ch. 42.

67 Royaume-Uni, *Data Protection Act 1998, ch.* 29, remplaçant la *Data Protection Act* de 1984. Site Web : www.dataprotection.gov.uk

susceptibles d'être combinées à d'autres informations. Il s'agit d'une définition large du terme « identifiable ».

L'article 1er définit également en termes larges le mot « traitement » (de données) : il s'agit de « l'obtention, de l'enregistrement ou de la détention de renseignements ou de données, ou de la mise en œuvre d'une opération, ou d'un ensemble d'opérations, concernant ces renseignements ou données, y compris (…) de l'adaptation , de l'altération (…), du repérage, de la consultation ou de l'utilisation (…), de la communication (…), (…) de l'effacement ou de la destruction de renseignements ou de données (…) ». Quant aux « données sensibles », selon leur définition, elles « englobent tous les renseignements concernant la santé, l'état physique ou mental ou la vie sexuelle ».

### c. Protections spéciales : données sensibles

Le DPA comporte des dispositions particulières au sujet de données sensibles comme les renseignements sur la santé de personnes identifiables.

Selon l'article 2, les « données sensibles » sont des renseignements ayant trait à « la santé ou à l'état physique ou mental ».

L'annexe 3 du DPA prévoit que les données sensibles doivent être traitées dans des conditions particulières. Ces conditions supposent généralement que la personne concernée a donné un « consentement explicite » ou que l'on démontre que le traitement non consensuel est « nécessaire », dans le cas par exemple : a) de responsabilités professionnelles, comme l'exige la loi; b) de circonstances particulières, pour protéger les intérêts primordiaux du sujet; c) des exigences de l'administration de la justice ou d'une poursuite judiciaire; d) de « fins médicales », notamment en matière de soins, de prévention, de diagnostic et de recherche médicale. Si le traitement des données est nécessaire à des fins médicales, il doit être effectué par un professionnel de la santé ou par une personne ayant le même genre d'obligations au regard du secret professionnel.

L'annexe 3 offre une certaine souplesse en matière d'adoption de politiques, en permettant expressément au gouvernement d'imposer d'autres conditions que celles énumérées pour la recherche effectuée avec des renseignements personnels sensibles. Le gouvernement a choisi de se prévaloir de cette disposition en 2000, en prenant le *Statutory Instrument 2000 nº 417*. Ce texte concerne le traitement de données à certaines « fins de recherche » lorsqu'il s'agit de faire des statistiques ou des recherches dans des archives[68]. Ce genre de recherches peut être effectué si le traitement est « dans un intérêt du public substantiel », s'il est « nécessaire aux fins de la recherche », s'il ne risque pas de causer « des torts ou des préjudices importants » et s'il ne compromet pas la personne concernée par certaines données, ni ne vient justifier la prise de mesures à son égard. Malgré ces détails, certains analystes demandent que l'on précise davantage les définitions et les normes du DPA, afin de guider plus étroitement la recherche en santé en ce qui a trait aux données consensuelles, non consensuelles et rendues anonymes[69].

Rappelons que, si les dispositions du DPA relatives aux données sensibles font largement écho aux normes de la *Directive de l'UE relative aux données à caractère personnel* (voir plus haut,

---

68 Royaume-Uni, Secrétariat d'État, *The Data Protection (Processing of Sensitive Personal Data) Order 2000 : Statutory Instrument 2000 nº 417,* Londres, février 2000, par. 9.

69 Strobl J, Cave E. et Walley T., « Data Protection Legislation : Interpretation and Barriers to Research », *BMJ*, nº 321, 2000, p. 890-892.

en C de la Troisième partie, au paragraphe 1), il existe cependant certaines différences. Par exemple, la *Directive de l'UE relative aux données à caractère personnel* propose certaines normes pour clarifier ce qu'il faut entendre par « consentement ». Comme on l'a vu, le DPA ne donne de définition précise des termes « consentement explicite » ni ne comporte de normes particulières à leur sujet. Il ne précise non plus ni la portée ni le sens de l'expression « recherche médicale », qu'il faut distinguer de l'expression « recherche en santé ». Il semble pourtant important de savoir si l'expression « recherche médicale » englobe la recherche épidémiologique en santé publique, puisque la recherche médicale constitue une exception à la règle générale du consentement explicite dans les cas de traitement de renseignements personnels sensibles. Par contre, contrairement au DPA, dans la *Directive de l'UE relative aux données à caractère personnel*, la « recherche médicale » n'est pas explicitement énumérée avec les diagnostics et les autres actes médicaux de ce genre qui sont regroupés dans les exceptions dites « à des fins médicales » à la règle générale du consentement explicite au traitement des données sur la santé. Son inclusion dans le DPA semble donc plutôt en accord avec l'exception générale de « l'intérêt public substantiel » prévue à l'article 8 de la *Directive de l'UE relative aux données à caractère personnel*. Comme le montre l'analyse faite plus haut, dans la Troisième partie, en C, point 1, cette exception permet aux États membres de désigner le traitement d'autres catégories de données sensibles comme étant un traitement de données « nécessaire » à la défense d'un « intérêt public substantiel ». Ainsi, comme pour les dispositions de la *Directive de l'UE relative aux données à caractère personnel*, le Parlement du R.-U. semble avoir jugé que la recherche médicale est nécessaire et représente un « intérêt public substantiel ».

### d. Consentement : collecte, utilisation et communication des données

Les normes de collecte des données du DPA sont le reflet, entre autres, des principes initiaux de contrôle de la qualité des données des *Lignes directrices de l'OCDE*, des exigences énoncées dans la *Directive de l'UE relative aux données à caractère personnel* et de diverses normes internationales. Par exemple, on retrouve les *Lignes directrices de l'OCDE*, sous forme modifiée, dans les huit grands principes qui orientent les pratiques de protection des données du DPA. En vertu des principes énoncés à l'annexe 1 du DPA, les renseignements personnels recueillis au R.-U. doivent en général : 1) être traités de façon juste et licite; 2) seulement aux fins prévues et jamais d'une manière incompatible avec ces fins; 3) être suffisants, pertinents et non excessifs; 4) être exacts; 5) être conservés pour une durée ne dépassant pas ce qui est nécessaire aux fins prévues; 6) être traités conformément aux droits de la personne concernée; 7) être protégés; 8) ne pas être transférés à des pays ne disposant pas de mesures de protection suffisantes.

Partant de ces principes, diverses dispositions du DPA les précisent, les explicitent ou les limitent, les transformant en normes. Par exemple, différents articles du DPA indiquent quels sont les droits généraux des personnes concernées par les données. Aux annexes 2 et 3, l'on dit que le traitement doit généralement être effectué avec le consentement de ces personnes, à moins que des exceptions particulières ne soient applicables (ces exceptions sont énumérées plus bas). La *Directive de l'UE relative aux données à caractère personnel* définit le consentement valable comme étant volontaire, précis et éclairé, mais cette norme n'est pas expressément mentionnée dans le DPA. Le DPA ne dit rien non plus sur la question du pouvoir décisionnel de substitution.

### e. Exceptions et recherche

Les articles 28 à 38 du DPA indiquent quelles sont les exceptions aux conditions générales de traitement des données; elles aussi font état de certaines exceptions particulières intéressant la

recherche. Toutes ces exemptions sont le reflet d'un effort sociétal de recherche d'un juste équilibre entre la protection du droit à la vie privée et d'autres nécessités et valeurs sociales qui peuvent de moins en moins être ignorées.

Conforme en général à la *Directive de l'UE relative aux données à caractère personnel*, le DPA s'en écarte par certaines exceptions, exigées, par exemple, pour les besoins des poursuites judiciaires, civiles et pénales, ou requises par d'autres lois, ou jugées par le Secrétaire d'État « nécessaires à la sauvegarde » des intérêts de la personne concernée ou des droits et libertés d'autres personnes.

Le DPA prévoit aussi des exceptions particulières ayant directement trait à la recherche. Voir plus haut les exceptions relatives au traitement non consensuel des renseignements sur la santé de personnes identifiables. Comme on l'a vu, la « recherche médicale » est considérée expressément comme l'une de ces « exceptions nécessaires ». Par ailleurs, en vertu de l'article 33, le « traitement des renseignements personnels à des fins de recherche seulement » n'a pas à être conforme à certains des principes applicables à la collecte des données. Cette exception, appliquée à des « renseignements personnels », amène à se demander si les données personnelles sur la santé traitées « uniquement à des fins de recherche » sont également exemptées ou si elles relèvent des normes du DPA applicables à la protection des données sensibles qui prévoient, par exemple, que le traitement de ce genre de données n'est autorisé que si l'on fait la preuve qu'elles sont nécessaires à la recherche médicale et que la recherche est effectuée par une personne liée par le secret professionnel au même titre qu'un professionnel de la santé. L'article 33 propose une définition des « fins de recherche » lorsqu'il dit que « les fins de recherche englobent les fins statistiques et historiques ». Les données traitées conformes à ces premiers critères ne peuvent être stockées indéfiniment et être traitées une seconde fois qu'à des fins de recherche. De plus, ces données ne sont pas assujetties aux dispositions générales de la Loi en matière d'accès si les données sont traitées de nouveau en fonction d'un ensemble de conditions particulières, notamment que le traitement n'est pas susceptible de causer un tort important à l'intéressé et que les résultats de la recherche seront communiqués sous une forme ne permettant pas d'identifier l'intéressé. Là encore, ces dispositions traduisent les normes énoncées dans la *Directive de l'UE relative aux données à caractère personnel*. Comme on l'a vu, le *Government Statutory Instrument 2000 nº 417*, qui a trait aux renseignements personnels sensibles, établit des normes applicables au traitement des données « nécessaires à des fins de recherche » qui sont « dans l'intérêt public ».

### f. Conservation et sécurité des données

En règle générale, le DPA adopte les normes de sécurité et de conservation des données des *Lignes directrices de l'OCDE*. Selon le principe 5 du DPA, les données personnelles ne doivent être conservées plus longtemps qu'il n'est nécessaire pour les fins particulières pour lesquelles elles ont été recueillies. Cependant, aux termes de l'article 33, les données traitées « uniquement à des fins de recherche » peuvent parfois être conservées pour une durée indéterminée à condition que ce soit conformément à certaines conditions applicables. Il faut par exemple que les données soient traitées de façon à ne pas causer de torts ou de préjudices importants à la personne concernée. Le principe 7 impose également l'obligation générale de prendre les « mesures qui conviennent sur les plans technique et organisationnel » pour éviter le traitement non autorisé ou illicite et la perte ou la destruction accidentelles de données. Le DPA adopte la norme de la *Directive de l'UE relative aux données à caractère personnel* permettant de mesurer ce qui « convient » : compte tenu des coûts et des facteurs technologiques, le degré de sécurité devrait être adapté à la nature des données et aux torts que pourrait causer le traitement abusif ou

négligent des données. Selon ce critère, les protections des données sensibles devraient être plus élevées.

### g. Autres dispositions intéressantes

Plusieurs dispositions du DPA sont destinées à favoriser sa mise en œuvre, conforme à la *Directive de l'UE relative aux données à caractère personnel* et aux politiques publiques dont a besoin la Grande-Bretagne.

Par exemple, en vertu du DPA, c'est le Commissaire à la protection des données qui est chargé d'en faire appliquer, en exerçant une surveillance indépendante, les dispositions. Cette disposition répond à une exigence de la *Directive de l'UE relative aux données à caractère personnel*, qui requiert la création d'un pouvoir de surveillance indépendant chargé de veiller à l'application des principes de protection des données. Les articles 51 à 54 du DPA indiquent que le Commissaire doit exercer ses fonctions en assumant un rôle d'éducateur autant que de policier.

D'autres dispositions sont conçues pour assurer une mise en œuvre effective. L'article 67(2), par exemple, donne au Secrétaire d'État du R.-U. le pouvoir de prendre des arrêtés et des règlements pour assurer la mise en application des principes et des dispositions du DPA, après consultation du Commissaire à la protection des données. C'est ainsi que le Secrétaire d'État a publié des textes réglementaires sur le fondement de ces dispositions, dont un sur la communication internationale de données, ainsi qu'un code de pratique pour les organisations de presse, et un autre texte sur les renseignements personnels sensibles. Certains de ces textes sont mentionnés plus haut.

## 2. Les Lignes directrices sur la confidentialité de la *British Medical Association* (BMA)

En 1999, en réponse au DPA et pour éclairer ses membres, la *British Medical Association* a publié des Lignes directrices (les *Confidentiality and Disclosure of Health Information*)[70]. Ces Lignes directrices portent sur toutes sortes d'aspects de la déontologie du secret professionnel, notamment au regard de la recherche. Elles font partie d'un processus permanent entrepris par la BMA depuis des années pour obtenir une politique gouvernementale et une clarification législative du droit médical de la confidentialité. Les Lignes directrices de la BMA indiquent que, si le DPA représente un progrès à cet égard, la BMA souhaite néanmoins d'autres mesures législatives.

C'est dans ce contexte que les Lignes directrices de la BMA, qui partent du principe que les renseignements sur la santé de personnes identifiables sont des données sensibles d'une catégorie spéciale, définissent plusieurs notions ayant directement trait à la recherche en santé :

- **De confidentialité** : Principe selon lequel les renseignements fournis par une personne donnée ou obtenus sur elle dans le cadre d'un rapport d'ordre professionnel doivent être conservés en sécurité et ne pas être communiqués à d'autres;
- **De communication** : Communication de renseignements sur la santé de personnes identifiables à d'autres qu'à la personne concernée;

[70] British Medical Association, *Confidentiality and Disclosure of Health Information*, Londres, octobre 1999. Site Web : http://www.bma.org.uk (éthique/lignes directrices).

- **De renseignements personnels sur la santé** : Tout renseignement personnel ayant trait à la santé physique ou mentale d'une personne permettant d'identifier cette personne;
- **De renseignements rendus anonymes** : Information qui ne permet pas, directement ou indirectement, d'identifier la personne à laquelle elle se rapporte.

Se fondant sur ces notions, les Lignes directrices de la BMA indiquent quelles sont les conditions d'application de l'obligation générale de confidentialité et ses limites raisonnables. Elles soulignent, par exemple, la nécessité sociétale du secret professionnel traditionnel du médecin, affirmant par exemple qu'il « est manifestement dans l'intérêt public que soit maintenu le principe de confidentialité, de sorte que le malade soit incité à obtenir le traitement dont il a besoin et à donner les renseignements nécessaires à cette fin ». Du point de vue des limitations, les Lignes directrices de la BMA considèrent que la recherche constitue un usage justifiable des renseignements personnels sur la santé à certaines conditions. Compte tenu de la nécessité de la confidentialité et des besoins de la société, il est proposé dans les Lignes directrices de la BMA que les renseignements ne devraient être communiqués que « dans la mesure minimale nécessaire à la réalisation de l'objectif poursuivi ». Cette disposition reprend un thème des *Lignes directrices de l'OCDE* (voir plus haut, dans la Troisième partie, en A). Pour réduire au minimum les risques de contravention aux règles de la confidentialité, les Lignes directrices de la BMA ajoutent que la recherche ne devrait faire usage autant que possible que de données qui auront été rendues anonymes. Lorsqu'elles ne peuvent pas l'être, les Lignes directrices exhortent les usagers à avoir recours à des pseudonymes ou à d'autres mécanismes de traçage susceptibles d'assurer l'exactitude des données tout en réduisant au minimum l'usage des identificateurs uniques.

Les Lignes directrices de la BMA traitent aussi de la question des renseignements et du consentement. Elles invitent les organisations de recherche et les chercheurs à informer les malades et à leur expliquer comment fonctionne la recherche; ceux-ci ne savent peut-être pas comment des données rendues anonymes peuvent contribuer à la recherches en santé et profiter à la société. Les Lignes directrices de la BMA imposent une condition d'ordre général à la communication des renseignements personnels : le malade doit donner son consentement volontairement et précisément, et le faire de façon éclairée. Les Lignes directrices de la BMA prévoient ensuite diverses exceptions possibles dont, par exemple, pour la communication non consensuelle de données nécessaires à des poursuites judiciaires, au traitement de réactions allergiques à des médicaments ou aux fins de la réglementation professionnelle. Selon la BMA, les vraies données ne permettant pas d'identification suscitent moins de problèmes de consentement et de confidentialité. Les Lignes directrices de la BMA rappellent donc qu'il n'est pas éthiquement nécessaire d'obtenir un consentement pour faire usage de données anonymes.

### 3. Les *Medical Research Council Guidelines on Research and Personal Data* [Lignes directrices du *Medical Research Council* sur la recherche et les renseignements personnels]

Un an après la publication, par la *British Medical Association*, de son document, le *Medical Research Council* (ou MRC) [le Conseil de recherches médicales] a publié de nouvelles lignes directrices d'éthique concernant l'utilisation des renseignements personnels dans la recherche médicale[71]. Il s'agissait d'une mise à jour des lignes directrices que le MRC publie périodiquement depuis les années 70.

[71] Medical Research Council (G.-B.), *Personal Information in Medical Research (Ethics Series)*, Londres, 2000. Site Web : http://www.mrc.ac.uk/PDFs/PIMR.pdf

### a. Champ d'application

Contrairement aux Lignes directrices de la BMA, celles du MRC portent exclusivement sur la recherche et sont destinées à guider les chercheurs qu'il finance. Les *Medical Research Council Guidelines on Research and Personal Data (Lignes directrices du MRC)* traitent de tous les renseignements personnels et ont donc un champ d'application plus large que celles de la MBA (voir la section suivante sur les définitions).

### b. Définitions

Les *Lignes directrices du MRC* comportent un glossaire dont les définitions ont directement trait à la recherche contemporaine en santé. On y trouve la définition des expressions « renseignements personnels », « données rendues anonymes »[72] (liées et non liées), « données codées » [73], « données confidentielles »[74] et « données sensibles »[75]. La définition des termes « renseignements personnels » est plus large que celle qu'en donne le DPA. On y englobe « tous les renseignements ayant trait à des personnes, vivantes ou décédées », notamment : « les dossiers écrits et électroniques, les avis, les images, les enregistrements et l'information ». Les Lignes directrices renvoient également à la définition de « données personnelles » du DPA et s'en inspirent : ce sont les renseignements personnels à partir desquels l'on peut être identifié : a) soit directement, par les données mêmes; b) soit par le rapprochement des données et d'autres renseignements que celui ou celle qui contrôle les données possède ou est susceptible d'obtenir ultérieurement.

### c. Protections spéciales : données sensibles

Le glossaire des *Lignes directrices du MRC* définit l'expression « données sensibles » : « Expression rappelant l'importance de la confidentialité lorsqu'il est question de santé mentale, de sexualité ou d'autres domaines au sujet desquels la divulgation de renseignements confidentiels serait particulièrement susceptible de causer de l'embarras ou d'exposer à de la discrimination ». Cette définition reprend des notions définies dans la *Convention 108/1981 du CE* qui, modifiées, ont été incorporées à la *Directive de l'UE relative aux données à caractère personnel* (voir plus haut, dans la Troisième partie).

### d. Consentement : collecte, utilisation et communication des données

À l'article 2 des *Lignes directrices du MRC*, on trouve un ensemble de principes généraux imposant des responsabilités et des obligations aux chercheurs et aux institutions au regard de la collecte, de l'utilisation et de la communication de renseignements personnels sur la santé.

---

[72] Données rendues anonymes : « Données élaborées à partir de renseignements personnels, mais qui ne peuvent permettre l'identification de la personne concernée par le destinataire de l'information. L'expression est employée dans le guide lorsqu'il est question à la fois de données rendues anonymes liées et non liées ».

[73] Données codées : « Renseignements de personnes identifiables où les détails permettant d'identifier les personnes concernées sont dissimulées sous un code, que les usagers peuvent facilement de décoder. Il ne s'agit pas de données rendues anonymes ».

[74] Données confidentielles : « Tout renseignement obtenu d'une personne sur engagement de ne pas le révéler à d'autres ou dans des conditions supposant qu'il ne sera pas communiqué. La loi présume que, lorsqu'on fournit des renseignements personnels aux professionnels de la santé traitants, ces renseignements demeureront confidentiels tant qu'il sera possible d'identifier celle ou celui qui les a fournis ».

[75] Données sensibles : « Expression rappelant l'importance de la confidentialité lorsqu'il est question de santé mentale, de sexualité ou d'autres domaines au sujet desquels la divulgation de renseignements confidentiels serait particulièrement susceptible de causer de l'embarras ou d'exposer à de la discrimination ».

Ces responsabilités sont, notamment :

- D'assurer la confidentialité des renseignements personnels obtenus pour la recherche en santé;
- Informer la personne concernée de l'usage que l'on fera de ses renseignements;
- S'assurer qu'a été obtenu un « consentement explicite » pour la collecte, la conservation et l'utilisation de renseignements personnels;
- Concevoir des modes de recherche respectant les principes de confidentialité et de consentement;
- Obtenir un contrôle éthique indépendant pour la recherche qui fait appel à des données de personnes identifiables ou à des données rendues anonymes;
- Rendre anonymes ou coder les renseignements personnels autant que possible;
- S'assurer que les renseignements personnels ne sont manipulés que par des personnes liées par le secret professionnel au même titre que les professionnels de la santé.

### e. Exceptions et recherche

Les *Lignes directrices du MRC* indiquent qu'il est possible de réaliser la plupart des projets de recherche dans le domaine de la santé en respectant la confidentialité et en s'assurant d'un consentement explicite pour le traitement des renseignements personnels ayant trait à la santé; néanmoins, elles prévoient des normes pour l'utilisation non consensuelle mais justifiée de tels renseignements.

L'article 2.2 dispose que ces cas ne se produisent que dans des conditions bien déterminées et exceptionnelles, c'est-à-dire que : « lorsqu'il est à peu près impossible de chercher à obtenir un consentement, des renseignements personnels peuvent être communiqués sans ce consentement si : les avantages potentiels pour la société l'emportent sur les effets de la perte de confidentialité, de sorte qu'effectuer la recherche s'avère clairement être dans l'intérêt public; et lorsqu'il n'est pas prévu de revenir informer les personnes concernées ni de prendre des décisions à leur sujet et qu'il n'y a pas d'autres moyens aussi efficaces ». Ces conditions réunies, « l'infraction au principe de confidentialité doit demeurer minimale ». Ces critères posent des conditions équivalentes aux normes de la « nécessité » et du juste équilibre de la *Directive de l'UE relative aux données à caractère personnel*, de la *CEDH* et des *Lignes directrices de l'OCDE*.

L'article 5.1 donne les éléments dont il y a lieu de tenir compte lorsqu'on code et rend anonymes les renseignements sur la santé que l'on veut traiter, ce qui peut parfois faire de ces procédés une solution de rechange pratique et efficace au traitement non consensuel. L'article 3.6.6 indique que « l'irréalisme » de l'obtention d'un consentement peut découler de la taille même de la population faisant l'objet d'études épidémiologiques, par exemple, ou dans des cas plus rares, du risque que le consentement des personnes concernées puisse en fait causer du tort, comme cela se présente pour certaines études sur la santé mentale. L'article 4 donne des exemples d'utilisation non consensuelle de renseignements personnels sur la santé. L'article 3.1 laisse entendre cependant qu'en général, il convient de décider du traitement non consensuel de renseignements personnels sur la santé en abordant chaque cas indépendamment, en fonction de principes éthiques et juridiques généraux et, ici encore, de facteurs comme la nécessité, le caractère sensible des données, leur importance, les sauvegardes prévues, les contrôles indépendants et les attentes.

### f. Conservation et sécurité des données

L'article 7 des *Lignes directrices du MRC* indique quelles sont les justifications et les normes applicables au stockage et à la conservation : les dossiers de recherche doivent être conservés à long terme pour des raisons de validation scientifique de la recherche, pour référence ou pour

vérification financières, et parfois à des fins cliniques. L'article 7.12 propose que, pour la recherche clinique et la recherche en santé publique et pour la documentation sur les effets secondaires des médicaments, les dossiers de recherche soient conservés vingt ou trente ans. Les équipes de recherche et les universités ont d'importantes responsabilités à l'égard de ce genre de conservation à long terme, notamment en ce qui concerne la désignation de conservateurs responsables, l'archivage des dossiers dans des endroits sûrs et la confidentialité du traitement des renseignements. L'article 2.1 prévoit, dans ses principes généraux, que les dirigeants de l'équipe de chercheurs ont l'obligation de prendre « la responsabilité personnelle de s'assurer que (…) la formation, les protocoles de conservation, la surveillance et les mesures de protection des données sont suffisantes pour prévenir les infractions à la confidentialité ». L'article 5.3 explicite ce principe général en énumérant les responsabilités qu'entraîne le traitement de données dans un environnement électronique ou physique. Parmi ces responsabilités, il y a celle de rédiger des protocoles de recherche concernant, par exemple, l'équipe de recherche, les contrôles et les révisions périodiques, la gestion des logiciels et les mesures de rétablissement en cas de catastrophe.

(Il n'y a pas de rubrique « Autres dispositions intéressantes » pour les *Medical Research Council Guidelines on Research and Personal Data*.)

# F. Les États-Unis

Les lois et les mesures fédérales américaines qui régissent la protection des renseignements personnels sont différentes de celles des autres pays abordées dans ce rapport tout en étant semblables. Comme tous les autres pays étudiés, les États-Unis ont signé et ratifié le *PIDCP*. Ils ont donc des obligations internationales au regard du droit à la vie privée. Depuis plus d'un quart de siècle, les lois fédérales imposent diverses normes juridiques au gouvernement fédéral pour le traitement des renseignements personnels. De tous les pays étudiés, les lois américaines pertinentes sont les plus anciennes.

Pourtant, contrairement à bon nombre de ces pays, il n'y a pas aux É.-U., une loi d'ensemble, omnibus, régissant la protection des données. On a plutôt tendance à élaborer des normes fédérales détaillées de protection de la vie privée applicables à divers secteurs de la société. Conformément à cette approche sectorielle, le gouvernement américain a récemment arrêté des normes nationales de protection des renseignements personnels sur la santé**.** Il a également mis au point un cadre de référence d'exonération, appelé le *Safe Harbor Framework*, où sont énoncées des règles nationales de protection de la vie privée harmonisant les normes américaines avec celles de l'Union européenne. Le texte qui suit donne un aperçu du *Federal Privacy Act*; il donne ensuite les points saillants de la nouvelle réglementation fédérale concernant la protection des renseignements personnels sur la santé, ainsi que ceux du *Safe Harbor Framework*.

## 1. Le *Federal Privacy Act* de 1974 [Loi fédérale sur la vie privée]

Le *Federal Privacy Act* de 1974[77] régit la collecte, l'utilisation et la dissémination des renseignements personnels par les institutions fédérales. La loi s'applique aux renseignements personnels en général, y compris aux renseignements sur la santé que possèdent les institutions fédérales

[77] 5 *United States Code*, art. 552a, modifié, Site Web : www.usdoj.gov/04foia/04_7_1.html

comme l'*Indian Health Service* et des entités semblables du Ministère fédéral de la Santé. Comme les *Lignes directrices de l'OCDE* qui allaient suivre, la Loi part du principe que les individus ont le droit d'être informés des renseignements personnels que le gouvernement possède à leur sujet et de la façon dont ils seront utilisés, et ils ont le droit de consulter ces renseignements. La Loi oblige les organisations à adopter des pratiques équitables de traitement de l'information, notamment à assurer la protection des dossiers et leur confidentialité. Ces pratiques sont fondées sur le *Code of Fair Information Practice Principles*[76] institué en 1973 par le Ministère américain de la Santé.

La Loi oblige les institutions fédérales à préciser les fins pour lesquelles les renseignements personnels sont recueillis et prévoit des sanctions civiles et pénales en cas d'utilisation abusive. Sauf lorsqu'elle est permise par une de ses exceptions, la Loi interdit la communication de renseignements personnels sans le consentement écrit de la personne concernée. Les exceptions énumérées sont notamment : a) la communication de façon anonyme de renseignements recueillis uniquement à des fins de recherches statistiques; b) la nécessité de protéger la santé et la sécurité d'une personne; c) la communication permise par les règles administratives de l'organisme. Dans ce dernier cas, la communication doit encore être « compatible » avec les fins pour lesquelles le renseignement a été recueilli.

Certains aspects de la mise en oeuvre du *Federal Privacy Act* sont différents de ceux qu'on trouve dans d'autres pays. Par exemple, d'autres pays ont un Commissaire à la protection de la vie privée et des organismes de surveillance indépendants, mais l'*Office of Management and Budget* [le Bureau de la gestion et du budget] joue un rôle limité lorsqu'il s'agit de décider des politiques des institutions fédérales. En 1999, l'*Office of Management and Budget* s'est doté d'un *Office of the Chief Councelor for Privacy* (ou Bureau du Premier conseiller à la protection de la vie privée) chargé, à titre consultatif, de coordonner les politiques fédérales de protection de la vie privée.

## 2. Les *Federal Privacy of Personal Health Information Rule* de l'an 2000 [Règle fédérale de protection des renseignements personnels sur la santé]

Les *Standards for Privacy of Individually Identifiable Health Information* [les Normes de protection des renseignements sur la santé d'individus identifiables] (ou les *Normes de l'HIPAA*) ont pour objet de protéger le caractère confidentiel des données sur la santé aux É.-U. Elles ont été adoptées par le gouvernement fédéral américain qui, depuis quelques années, s'intéresse de plus en plus à la protection des droits liés à la vie privée et aux opérations à caractère administratif de la santé.

En effet, en 1996, le Congrès américain a adopté une loi fédérale qui avait pour objet, notamment, de permettre aux citoyens américains de conserver leur régime privé d'assurance-maladie et d'assouplir certaines opérations administratives du système de santé. Il s'agit du *Health*

---

76 US Department of Health, Education and Welfare, *Code of Fair Information Practice Principles*, 1973.

Banisar, D., *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*, Electronic Privacy Information Center (EPIC), Washington, 2000, p. 230.

Ministère américain de la Santé et des Services sociaux, *Standards for Privacy of Individually Identifiable Health Information—Final Rule* (ci-après Normes de protection des renseignements personnels sur la santé d'individus identifiables, ou *Normes de l'HIPAA*) *Federal Register*, 28 décembre 2000; 65(250), p. 82462, codifiées au 45 *Code of Federal Register* 160 et 164. Site Web : www.hhs.gov/ocr/hipaa

*Insurance Portability and Accountability Act of 1996* (HIPAA).[77] Les articles 262 et 264 du HIPAA se sont avérés particulièrement importants pour la protection des renseignements personnels au regard de l'efficacité administrative des opérations de santé. Ils sont mentionnés dans une notice explicative sur les normes de protection de la vie privée récemment arrêtées :

Les articles 261 à 264 du HIPAA sont appelés « dispositions de simplification administrative ». On trouve presque toutes ces dispositions de simplification administrative à l'article 262 du HIPAA (…) En adoptant l'article 262, le Congrès a surtout voulu permettre à l'industrie de la santé de réaliser des économies et de réduire ses coûts par un plus grand recours à la technologie électronique. Ainsi, aux termes de l'article 262, le HHS [le Ministère américain de la Santé et des Services sociaux] est tenu de publier des normes visant à faciliter l'échange d'information, par des moyens électroniques, sur les opérations financières et administratives des régimes de soins de santé, des bureau centraux de santé et des intervenants en soins de santé qui transmettent des renseignements sur ce type d'opération par des moyens électroniques. Parallèlement, le Congrès a reconnu que le caractère confidentiel des renseignements sur la santé était menacé par la complexité grandissante de l'industrie de la santé, de même que par les progrès de la technologie et des moyens de communication dont disposent les systèmes d'information sur la santé. Aux termes de l'article 262, le HHS est donc également tenu d'élaborer des normes de protection de la sécurité des renseignements sur la santé, notamment de leur confidentialité et de leur intégrité.[78]

En réponse, le Ministère de la Santé et des Services sociaux (HHS) a proposé des normes de protection des renseignements personnels sur la santé au Congrès américain en 1997. L'article 262 du HIPAA prévoyait également que, si le Congrès n'avait pas adopté une loi parallèle régissant la protection des renseignements personnels sur la santé avant août 1999, le HHS serait obligé de prendre des règlements définitifs avant février 2001. Le Congrès américain n'a pas adopté de loi même si plusieurs projets de loi et rapports connexes[79] ont traité de la question. En décembre 2000, le HHS a arrêté les *Normes de l'HIPAA*.[80]

### a. Champ d'application

Les *Normes de l'HIPAA* s'appliquent aux dossiers médicaux, de même qu'aux autres renseignements sur la santé qui permettent d'identifier la personne concernée et qui sont utilisés ou communiqués par une « entité désignée » par un procédé quelconque, notamment électronique, écrit ou oral. Elles s'appliquent, en général, aux « régimes d'assurance-maladie », aux « bureaux centraux de santé » ainsi qu'aux « intervenants en soins de santé » des secteurs privé ou public qui effectuent des opérations financières et administratives par des moyens électroniques (par exemple, la facturation et les transferts de fonds). Aux États-Unis, de nombreux chercheurs et leurs intérêts seront visés par les *Normes de l'HIPAA* à titre d'intervenants en soins de santé. Les articles 160.201 à 160.205 des *Normes de l'HIPAA* indiquent qu'elles ont pour objet d'établir des normes nationales minimales pour tout le pays.

---

77 *Health Insurance Portability and Accountability Act of 1996* (HIPAA) Public Law 104-191, modifié, 42 United States Code 1320-d.

78 *Normes de l'HIPAA*, précitées, Partie I.

79 Voir, p. ex., le United States General Accounting Office. *Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections is Limited*. Washington, février 1999.

80 *Normes de l'HIPAA*, précitées, *Federal Register* 28 décembre 2000;65(250), p. 82462, qui seront codifiées à 45 *Code of Federal Register* 160 et 164.

Par conséquent, la loi fédérale primera en général les lois des États dont les normes sont moins élevées et complétera celles qui en imposent de plus strictes pour la protection de la vie privée.

Outre son interaction avec les lois des États, le HIPAA est plus large, plus complexe et plus universel à cause de ses recoupements et de son interaction avec d'autres lois fédérales américaines. Par exemple, les *Normes de l'HIPAA* interagissent avec le *Federal Food, Drugs and Cosmetics Act*,[81] avec la politique et les règles fédérales américaines applicables à la recherche sur les être humains,[82] et avec les *Clinical Laboratory Improvements Amendments* de 1988.[83] Quelques-unes de ces lois établissent des normes applicables à la recherche en santé. La présente étude se penche sur certaines des interactions entre les *Normes de l'HIPAA* et ces lois, mais leur examen plus approfondi sortirait du cadre de notre analyse.

### b. Définitions

Il y a des définitions dont celles de quelques termes importants, notamment : « données sur la santé de personnes identifiables », « utilisation », « communication », « intervenant en soins de santé », « données sur la santé dépersonnalisées », « consentement », « agrégation de données » et « recherche ».

Par exemple, aux termes des *Normes de l'HIPAA*, les données de personnes identifiables forment un sous-ensemble des données générales sur la santé. Ainsi, l'article 164.501 définit en termes larges l'expression « données sur la santé de personnes identifiables » « comme étant des données sur la santé mentale ou physique ou une affection, passées, présentes ou futures, d'une personne », qui, soit l'identifient, soit portent raisonnablement à croire qu'elles peuvent servir à l'identifier ». Les données sur la santé de personnes identifiables qui ont été dépersonnalisées échappent aux *Normes de l'HIPAA* si certaines conditions sont remplies (voir plus loin, à la section e.).

Les *Normes de l'HIPAA* n'emploient pas l'expression « traitement de données ». Elles définissent en termes larges les mots « utilisation » et « communication ». Ainsi tout renseignement sur la santé d'une personne identifiable échangé, examiné, analysé ou employé au sein d'une entité est « utilisé », alors que tout renseignement échangé ou transféré hors de l'entité est « communiqué ». On trouvera une analyse plus détaillée des définitions d'autres termes importants plus loin.

### c. Protections spéciales : données sensibles

Aux termes des *Normes de l'HIPAA* : « De toutes les données personnelles, les données sur la santé comptent parmi les plus sensibles ». Les *Normes de l'HIPAA* sont donc en accord sur cette approche avec plusieurs autres pays et avec les normes de la communauté internationale.

Selon les *Normes de l'HIPAA*, les renseignements sur la santé sont sensibles, mais les *Normes* sont encore plus strictes à l'égard de la protection des notes psychothérapeutiques. Aux termes de l'article 164.501, les notes psychothérapeutiques sont les notes consignées (par un moyen quelconque) par un intervenant en soins de santé spécialisé en santé mentale qui documentent

---

81 21 *United States Code Annotated* 301 et suite, mis en œuvre en partie à 21 *Code of Federal Register* 310 et suite.

82 Voir, p. ex., Ministère américain de la Santé et des Services sociaux. (*Basic DHHS Policy for Protection of Human Research Subjects*) *Regulations on Protection of Human Subjects*. *Federal Register* 18 juin1991; 56:28003, codifié à 45 *Code of Federal Register* 46. Site Web : http://ohsr.od.nih.gov/mpa/45cfr46.php3

83 42 *United States Code* 263a, mis en oeuvre en partie à 42 *Code of Federal Register* 493.3(a)(2).

ou analysent le contenu d'une conversation qui a eu lieu pendant une séance de counselling privée, de groupe ou familiale et qui ne sont pas conservées dans le même dossier médical de la personne concernée.

La définition exclut les ordonnances médicales et le contrôle des médicaments, l'heure du début et de la fin des séances, les modalités et la fréquence du traitement offert, les résultats des essais cliniques, ainsi que les résumés portant sur le diagnostic, l'état fonctionnel, le programme de traitement, les symptômes, le pronostic et les progrès réalisés. Aux termes de l'alinéa 168.508(a)(2), la communication ou l'utilisation de ces notes ne peut être faite sans autorisation valable, sauf dans quelques rares cas, notamment dans celui du traitement par la personne qui a rédigé les notes, dans celui de certaines poursuites judiciaires ou de programmes de formation en établissement. Aux termes de l'article 164.524, les personnes concernées n'ont pas un droit d'accès général aux notes psychothérapeutiques.

### d. Consentement : collecte, utilisation et communication des données

Dans les *Normes de l'HIPAA* sont décrites les normes générales applicables au traitement des données sur la santé; elles sont semblables à celles des *Lignes directrices de l'OCDE* et de la *Directive de l'UE relative aux données à caractère personnel*. Voici une description de trois de ces normes.

Tout d'abord et parallèlement à la *Directive de l'UE relative aux données à caractère personnel*, les *Normes de l'HIPAA* imposent une interdiction générale d'« utilisation » et de « communication » des « renseignements sur la santé de personnes identifiables », sauf avec l'autorisation ou le consentement de la personne concernée. Aux termes des *Normes de l'HIPAA*, les mots « consentement » et « autorisation » ne sont pas synonymes. En règle générale, il faut le consentement écrit de la personne concernée pour l'utilisation et la communication de données personnelles à des fins de « traitements » (thérapeutiques), de « paiement » et de « soins de santé ». Les *Normes de l'HIPAA* définissent ces termes. Pour d'autres fins, une autorisation écrite est requise, notamment et normalement pour la recherche. Les *Normes de l'HIPAA* précisent également quels sont les divers éléments qui doivent normalement figurer dans une autorisation valable. Les alinéas 164.508(b) et (c) prévoient notamment qu'une autorisation valable doit être rédigée en termes simples et indiquer quels renseignements seront utilisés ou communiqués, qui sera autorisé à demander les renseignements, quels en seront les destinataires, quel sera le moyen de transmission et quelle sera la date de réception. Devrait de même être inclus un avis du droit de révoquer l'autorisation. En règle générale, les autorisations peuvent être révoquées par écrit à tout moment, sauf si l'entité « a pris des mesures sur la foi de » l'autorisation. D'autres exigences s'appliquent selon que l'autorisation d'utilisation ou de communication est demandée pour l'entité ou à des fins de communications par des tiers. Lorsqu'il s'agit d'une recherche qui comprend un traitement thérapeutique, comme par exemple dans certains essais cliniques de médicaments, il est précisé dans les *Normes de l'HIPAA* qu'en règle générale il faut, entre autres, une autorisation particulière adaptée au contexte de la recherche. Aux termes de l'alinéa 164.508(f), il faut notamment une description de la manière dont l'utilisation ou la communication des renseignements serviront les fins du traitement. L'alinéa exige également qu'il y ait respect des *Normes de l'HIPAA* régissant le consentement, sous réserve des exceptions applicables.

Ensuite, les *Normes de l'HIPAA* imposent une obligation générale de limiter le plus possible l'ampleur des atteintes à la vie privée jugées nécessaires. Tel que susmentionné dans la Troisième

partie, tant les *Lignes directrices de l'OCDE* que la *Directive de l'UE relative aux données à caractère personnel* requièrent de façon générale que la portée de toute atteinte à la vie privée considérée comme nécessaire soit limitée. Les *Normes de l'HIPAA* s'assurent de cette limitation par une norme générale. En conformité avec l'article 164.502, l'entité doit « s'efforcer de limiter au minimum nécessaire l'utilisation des renseignements personnels sur la santé compte tenu de la finalité de l'utilisation, de la communication ou de la demande ». Aux termes de l'alinéa 164.514(d), la mise en application de la norme du « minimum nécessaire » exige des mesures précises d'ordre organisationnel et administratif. Par exemple, les entités qui communiquent des renseignements confidentiels sur la santé de façon systématique et répétitive doivent mettre en place des politiques et des protocoles de communication limitant les renseignements communiqués aux seuls raisonnablement nécessaires, qui permettent d'atteindre les buts visés par la communication. Les établissements doivent également déterminer qui, parmi leurs employés, auront accès aux renseignements confidentiels sur la santé, et prendre des mesures raisonnables pour limiter le plus possible le nombre de ces personnes.

Enfin, les *Normes de l'HIPAA* prévoient, pour la personne concernée, un droit d'information général et particulier sur les données recueillies. L'article 164.524 par exemple, lui reconnaît un droit général de consultation des informations sur la santé qui la concernent, hors le cas des notes psychothérapeutiques, et celui d'en obtenir copie. Et l'alinéa 164.522(a) lui reconnaît le droit d'exiger des limitations d'utilisation et de communication. Enfin, aux termes de l'article 164.528, il est permis de demander un compte-rendu de toutes les communications effectuées au cours des six années précédentes.

### e. Exceptions et recherche

Les *Normes de l'HIPAA* prévoient plusieurs exceptions à l'obligation générale d'obtention d'un consentement ou d'une autorisation, ainsi que d'autres dispositions et exceptions qui s'avèrent particulièrement pertinentes en ce qui a trait à la recherche. Comme dans d'autres pays, les exceptions recherchent un juste équilibre entre la protection de la vie privée et d'autres valeurs et besoins sociétaux qui se font de plus en plus sentir.

En ce qui concerne les exceptions générales, l'article 164.512 autorise l'utilisation ou la communication non consenties de renseignements sur la santé aux fins, notamment : a) des mesures de contrôle sanitaire, par exemple les vérifications, les investigations administratives, les inspections, les mesures des autorités dispensant des autorisations et les inflictions de sanctions disciplinaires; b) de questions de santé publique, par exemple aux fins de recueillir ou d'obtenir des renseignements sur la santé, conformément à une autorisation légale, à des fins épidémiologiques, de statistiques d'état civil ou d'application des lois nationales sur les drogues et les moyens thérapeutiques; c) lorsque nécessaire, afin de prévenir un danger grave et imminent pour la santé ou la sécurité publiques. Ces dispositions sont semblables aux exceptions prévues par la *Directive de l'UE relative aux données à caractère personnel*, susmentionnées, dans la Troisième partie, en C, point 3.

Les *Normes de l'HIPAA* contiennent également des dispositions et des exceptions particulières qui s'appliquent aux activités de recherche. Au sens de l'article 164.501, la « recherche » s'entend « d'une étude systématique, notamment par les recherches en développement, des essais et des évaluations, qui a pour objet de perfectionner ou d'augmenter les connaissances généralisables ». Les *Normes de l'HIPAA* excluent expressément la recherche de la définition d'autres termes importants. Ainsi, la définition large des « activités de soins de santé » exclut expressément la recherche. On trouve dans les *Normes de l'HIPAA* des normes applicables aux

essais cliniques, une forme de recherche. Par exemple, le sous-alinéa 64.524(a)(2)(iii) prévoit que l'accès aux renseignements personnels peut être limité lorsque les malades qui participent à la recherche sont en traitement. L'accès peut être suspendu pendant la recherche si la suspension était prévue aux termes du consentement que le malade a donné en faveur de la recherche et si l'intervenant en soins de santé l'a informé qu'il pourra avoir accès à l'information une fois la recherche terminée. En outre, l'on trouve dans les *Normes de l'HIPPA* des normes pour la recherche effectuée sans consentement dans certains cas. Les normes qui s'appliquent à l'utilisation des données dépersonnalisées et à la recherche qui peut être effectuée sur la foi d'une renonciation à l'obligation d'autorisation ou d'obtention du consentement de la personne concernée en sont deux exemples importants. Il en sera maintenant traité.

Les données dépersonnalisées et les données codées : L'alinéa 164.502(d)(2) des *Normes de l'HIPAA* prévoit que les renseignements sur la santé qui remplissent les conditions autorisant leur dépersonnalisation ne sont pas assujettis à ses normes générales d'utilisation et de communication. Aux termes de la disposition, les données dépersonnalisées sont des données qui « n'identifient pas la personne concernée et dont il ne serait pas raisonnable de croire qu'elles pourraient être utilisées pour l'identifier ». Cet alinéa vient compléter l'alinéa 164.514(a) qui indique comment, en pratique, les normes applicables à la dépersonnalisation peuvent être mises en oeuvre. En vertu de ce dernier alinéa, les établissements sont autorisés à dépersonnaliser les renseignements sur la santé de deux façons.

Une première consiste à ce qu'un spécialiste juge que le risque d'identification, par le destinataire prévu, par utilisation de l'information ou par rapprochement de l'information à d'autres renseignements probablement disponibles, est « infime ». Seule « une personne qui possède les connaissances et l'expérience nécessaires des principes et des méthodes statistiques et scientifiques généralement reconnus de dépersonnnaliser les renseignements » peut porter ce jugement. Le spécialiste doit appliquer les principes et les méthodes susmentionnés et évaluer le risque. Il doit documenter les méthodes utilisées et les résultats de son analyse.

L'autre façon est celle-ci : l'entité peut éliminer les identificateurs : les noms, adresses, codes postaux, images photographiques, empreintes vocales, numéros de téléphone, numéros de télécopieur, dossiers médicaux, permis, comptes ou plaques d'immatriculation, ou « tout autre numéro, caractéristique ou code permettant d'identifier une personne ». Cette dépersonnalisation doit être effectuée sans qu'il ait été établi que le renseignement identifie la personne concernée ou permettrait, avec d'autres données, de l'identifier. Soulignons qu'aux termes de l'alinéa 164.514(c) les codes qui permettent une réidentification après dépersonnalisation sont autorisés sous réserve de l'observation de certaines mesures de sécurité, et à condition que ces codes ne soient pas dérivés de renseignements donnés au sujet de la personne concernée, ou pouvant leur être rattachés, et qu'il ne soit pas possible de les décoder et d'identifier cette personne.

Les dispenses : Outre les exceptions générales et les protocoles de dépersonnalisation, la recherche effectuée avec des renseignements personnels de santé est permise lorsqu'une dispense d'autorisation est approuvée par une instance indépendante de protection de la vie privée ou par un comité d'éthique de recherche. Le sous-alinéa 164.512(i) prévoit de façon générale que trois conditions doivent être réunies pour que la dispense soit valable.

Première condition : l'entité qui demande la dispense doit obtenir du chercheur des assurances précises ou la promesse que le Comité sera saisi de la demande de recherche. Parmi les déclarations qu'il fait au sujet de la confidentialité et de ses exigences, le chercheur doit faire valoir que les renseignements demandés sont « nécessaires à la recherche ».

Seconde condition : la dispense doit être approuvée par un comité d'éthique de la recherche constitué en bonne et due forme ou par une Commission de protection de la vie privée. La Commission ne doit pas être en conflit d'intérêts et elle doit être composée de personnes provenant de milieux différents possédant « les compétences appropriées ». Pour que le comité d'éthique de la recherche puisse approuver la dispense, il doit satisfaire aux normes de composition et d'indépendance exigées par le droit fédéral américain applicable en matière de recherche.[84] Le contrôle éthique doit également être effectué en conformité avec la procédure normale prévue par le droit fédéral applicable en matière d'éthique et de recherche.

Troisième condition : outre les exigences d'ordre procédural, la Commission de protection de la vie privée ou le comité d'éthique de recherche de l'établissement doivent habituellement fonder l'approbation de la dispense sur la constatation que la recherche ne comporte qu'une atteinte minimale à la vie privée, justifiée compte tenu de son importance, et qu'il est peu réaliste d'espérer l'effectuer autrement. Le comité doit donc tout particulièrement s'assurer que : a) le risque que fait courir l'utilisation de renseignements personnels sur la santé est minimal; b) la dispense ne portera atteinte ni aux droits ni au bien-être des personnes concernées; c) la recherche ne pourrait pas raisonnablement être entreprise sans la dispense et sans les renseignements (l'expression « raisonnablement » n'est pas définie); d) le rapport entre les risques d'atteinte à la vie privée et l'importance des connaissances qu'on peut raisonnablement s'attendre à obtenir est raisonnable; e) des mesures de protection de la sécurité des données particulières ont été prises pour empêcher leur utilisation ou communication irrégulières; f) enfin, des mesures adéquates de conservation des données sont prévues par le protocole de recherche. Ces plans doivent prévoir la destruction des identificateurs « dès que la possibilité s'en présente » compte tenu du déroulement de la recherche, sauf si leur conservation à plus long terme est autorisée par la loi ou qu'elle devient légitime pour des raisons de santé ou parce qu'elle est justifiée aux fins de la recherche.

### f. Conservation et sécurité des données

En règle générale, les *Normes de l'HIPAA* ayant trait à la sécurité sont semblables à celles prévues par les *Lignes directrices de l'OCDE* initiales. En conformité avec l'exigence administrative de l'article 164.530, les établissements « doivent avoir mis en place les sauvegardes administratives, techniques et physiques appropriées de protection de la confidentialité des renseignements personnels sur la santé. Il y a également obligation de « prendre des mesures raisonnables pour assurer la sauvegarde » de ces renseignements. D'autres *Normes de l'HIPAA* viennent compléter et développer ces normes générales. Par exemple, les mesures de sécurité administratives qui doivent être associées aux normes d'accès aux renseignements codés et à l'enlèvement des codes ont été décrites à la section e. qui précède. En outre, le critère du « minimum nécessaire » susmentionné implique la prise de mesures de protection organisationnelles et administratives de limitation de l'accès aux renseignements sur la santé. De surcroît, aux termes de l'article 164.530, le personnel doit recevoir la formation nécessaire afin que l'on puisse avoir l'assurance qu'il est en mesure de se conformer aux politiques et aux protocoles de protection des renseignements personnels de l'établissement.

En ce qui a trait à la durée de conservation des données, les *Normes de l'HIPAA* ne semblent prévoir aucun critère distinct, explicite et détaillé. Il semble plutôt que l'on s'attaque au problème indirectement par le truchement d'autres normes. Par exemple, l'on mentionne la conservation de données dans les normes sur lesquelles doivent se fonder les comités d'éthique de la recherche

[84] Voir, p. ex., 45 *Code of Federal Register* 46.107 (DHHS); 21 *Code of Federal Register* 56.107 (US Food and Drug Administration).

pour décider s'il y a lieu d'accorder une dispense de l'autorisation de la personne concernée normalement requise en matière de recherche sur la santé. Tel que susmentionné, dans les protocoles de recherche, la destruction des identificateurs devrait être prévue, « dès que la possibilité s'en présente » et que le permet le déroulement de la recherche, sauf si leur conservation à long terme est autorisée par la loi ou devient légitime pour des questions de santé ou parce que justifiée aux fins de la recherche. Les termes précis utilisés et l'importance accordée à la recherche diffèrent, mais la finalité semble identique à celle des normes de conservation raisonnable énoncées dans les *Lignes directrices de l'OCDE*.

### g. Autres dispositions intéressantes

Plusieurs dispositions des *Normes de l'HIPAA* ont pour objet de favoriser leur mise en oeuvre tant à l'échelon national qu'à celui de l'établissement. Certaines dispositions sont calquées sur des dispositions analogues de mise en œuvre des lois nouvelles de protection des données personnelles et du droit à la vie privée d'autres pays mentionnés dans le présent rapport; d'autres s'en écartent. Par exemple, la surveillance et l'application des *Normes de l'HIPAA* ont été confiées à l'Office for Civil Rights (OCR) [le Bureau des droits civils] du HHS. L'OCR aide les intervenants de la santé, les régimes d'assurance-maladie et les bureaux centraux de santé à se conformer aux *Normes de l'HIPAA*. L'OCR est également chargé de connaître des plaintes d'atteinte au droit à la vie privée et d'ouvrir les enquêtes pertinentes. Dans d'autres pays, contrôle et mise en œuvre sont habituellement confiés à une instance gouvernementale autonome, comme une commission de protection des données personnelles ou du droit à la vie privée.

Les *Normes de l'HIPAA* traitent de leur mise en œuvre à l'échelon de l'établissement. Par exemple, en conformité avec les normes administratives de l'article 164.530, les entités visées doivent adopter des protocoles écrits d'accès, d'utilisation et de communication des renseignements confidentiels. Elles doivent également former leurs employés et nommer un agent de protection de la vie privée chargé de veiller au respect de ces protocoles.

L'article 164.520 impose également aux entités visées l'obligation générale d'informer les personnes concernées, en termes clairs et par écrit, de leurs pratiques de protection des renseignements confidentiels sur la santé. L'avis doit notamment donner des informations au sujet des utilisations et des communications, des droits des personnes concernées, des obligations de l'établissement en matière de protection de la vie privée et des personnes ressources à joindre. L'avis doit être donné en temps opportun, être précis et être révisé à intervalles réguliers. Les intervenants en soins de santé doivent se conformer à des normes particulières d'information lorsqu'ils traitent directement la personne concernée.

Enfin, contrairement aux *Lignes directrices de l'OCDE* et à la *Directive de l'UE relative aux données à caractère personnel*, les *Normes de l'HIPAA* ne contiennent aucune disposition expresse sur l'échange de données sur la santé avec d'autres États. Ces dispositions sont prévues dans une mesure distincte à portée plus large.

## 3. Les *Safe Harbor Privacy Principles** de 2000 *[*les *Principes d'exonération]*

À l'instar de plusieurs pays, les É.-U. viennent d'adopter des mesures qui ont pour objet d'harmoniser leurs normes nationales de protection de la vie privée avec les dispositions de la *Directive de l'UE relative aux données à caractère personnel*. Tel que susmentionné dans la

* N.d.T. : Littéralement : Principes pour « un havre sûre » pour la vie privée.

Troisième partie, en C, point 3, l'article 25 de la *Directive de l'UE relative aux données à caractère personnel* interdit en général le transfert de données personnelles des pays membres de l'UE à d'autres pays n'assurant pas « un niveau de protection adéquat ». En raison de l'absence de loi fédérale uniforme ou centralisée de protection des données aux É.-U., le Ministère américain du Commerce a voulu adopter des normes qui permettraient aux compagnies américaines de ne pas être exclues du transfert de données personnelles en provenance d'Europe. Après deux années de pourparlers, de négociations et de révisions d'une première proposition américaine déposée en 1999, la version définitive du Cadre de référence d'exonération, l'*US Safe Harbor Privacy Framework*[85] a été approuvée et par les É.-U. et par l'UE, en juillet 2000. Le Cadre regroupe plusieurs documents provenant des É.-U. et de l'UE, dont les principaux sont *Safe Harbor Privacy Principles* (les « *Principes d'exonération* ») du Ministère américain du Commerce et les *Frequently Asked Questions (la Foire aux questions, ou* FAQ)).

### a. Champ d'application

Les *Principes d'exonération* ne peuvent être invoqués que par les organisations américaines qui reçoivent des données personnelles en provenance de l'Union européenne « à des fins d'exonération et de présomption de "conformité" ». Les Principes s'appliquent au traitement manuel ou électronique des données par les compagnies américaines qui décident volontairement de s'y conformer de manière à pouvoir obtenir et conserver les avantages qu'entraîne leur participation. Ils s'appliquent tant et aussi longtemps que l'organisation conserve les données personnelles pertinentes, même si elle a mis fin à sa participation au programme d'exonération.

### b. Définitions

Les *Principes d'exonération* définissent en termes larges l'expression « renseignements personnels » et « données personnelles », qui s'entendent de données sur une personne qui l'identifient ou la rendent identifiable, visées par la *Directive de l'UE relative aux données à caractère personnel*, reçues par une organisation américaine en provenance de l'Union européenne et enregistrées sous une forme quelconque. Les Principes reprennent donc la norme applicable aux données à caractère personnel de la *Directive de l'UE relative aux données à caractère personnel.*

### c. Protections spéciales : données sensibles

Les *Principes d'exonération* offrent une protection accrue aux données sensibles, notamment aux renseignements personnels qui révèlent l'origine raciale ou ethnique, les préférences sexuelles ou l'état de santé. Le principe du choix interdit de façon générale l'utilisation des renseignements sensibles sauf si la personne concernée a expressément consenti à leur utilisation. Cette approche est conforme à la plupart des normes internationales contemporaines.

### d. Consentement : collecte, utilisation et communication des données

Le *Safe Harbor Framework* (le Cadre de référence d'exonération) pose sept principes de protection des renseignements personnels semblables aux principes décrits dans les *Lignes directrices de l'OCDE* modifiées par la *Directive de l'UE relative aux données à caractère personnel*. Ces principes sont :

- La notification;
- Le choix;

[85] Ministère américain du Commerce. *Safe Harbor Framework*. Washington, juillet 2000. Site Web : www.export.gov/safeharbor/sh_documents.html

- La retransmission (par exemple, utilisation par un tiers);
- La sécurité;
- L'intégrité des données;
- L'accès;
- Le contrôle.

Les normes générales de traitement des données personnelles du Cadre de référence d'exonération sont énoncées dans les principes. Une liste complémentaire de la FAQ, portant sur quinze questions problèmes, donne des explications sur les principes, des précisions, leur contexte et fait état de quelques exceptions.

Ainsi, par exemple, les principes de notification et de choix fixent de façon générale les normes applicables à la collecte et à l'utilisation des données lorsqu'il y a eu consentement éclairé.

Aux termes du principe de notification, l'établissement est tenu d'informer la personne concernée « de la finalité de la collecte et de l'utilisation qui sera faite de l'information qui la concerne, des moyens d'entrer en contact avec l'organisation pour s'informer ou porter plainte, des tiers auxquels il communiquera l'information et des possibilités et des moyens qu'il lui offre de limiter cette utilisation et cette communication ».

Cette information vient compléter les normes sur le consentement du principe de choix. Selon la FAQ sur le choix, le but du principe de choix, c'est d'assurer que les renseignements personnels sont utilisés et communiqués conformément aux attentes et aux choix de la personne concernée. Ainsi ces personnes peuvent choisir de consentir ou non à la communication des renseignements personnels qui les concernent à un tiers ou à une utilisation « à une fin incompatible avec l'objet pour lequel ils ont été recueillis au départ ou qui avait subséquemment été autorisée par la personne concernée ». Pour faire ces choix, la personne concernée doit être informée au moment où l'on s'adresse à elle pour la première fois au sujet de l'utilisation des renseignements personnels ou dès que « cela peut se faire » par la suite. Le principe de retransmission prévoit de façon générale que les normes de notification et celles relatives au choix s'appliquent à la retransmission des renseignements à un tiers. La norme du principe d'intégrité des données est applicable aux utilisations secondaires et fondée sur la notion de « finalité incompatible ». Selon ce principe, l'organisation « ne peut traiter des renseignements personnels d'une manière qui est incompatible avec l'objet pour lequel ils ont été recueillis ou ultérieurement autorisé par la personne concernée ».

### e. Exceptions et recherche

Le *Safe Harbour Framework* prévoit des exceptions générales et, à la fois, comporte des dispositions et des exceptions ayant directement trait à la recherche. Le Cadre de référence d'exonération indique de façon générale que le respect des principes peut être limité : « a) dans la mesure où la sécurité nationale, l'intérêt public ou la répression des infractions à la loi l'exigent; b) par une loi, un règlement gouvernemental ou le droit jurisprudentiel lorsqu'ils créent des obligations contraires ou accordent expressément des autorisations, pourvu que dans l'exercice de l'autorisation, l'organisation puisse démontrer qu'elle ne s'écarte des principes que dans la mesure nécessaire, exigée par les intérêts légitimes supérieurs justifiant l'autorisation; c) si l'effet de la *Directive de l'UE relative aux données à caractère personnel* ou du droit interne de l'État membre est de permettre des exceptions ou des dérogations, pourvu que de telles exceptions ou dérogations soient reconnues dans des situations comparables ». L'expression « intérêt public » n'est pas définie et diffère quelque peu de l'expression « intérêt économique ou financier important » utilisée dans la *Directive de l'UE relative aux données à caractère*

*personnel*. Quoi qu'il en soit, comme la *Directive de l'UE relative aux données à caractère personnel*, les *Normes de l'HIPAA* et les *Lignes directrices de l'OCDE*, le Cadre de référence d'exonération adopte une norme fondée sur la nécessité pour justifier les atteintes au droit à la vie privée. Selon cette norme, les atteintes nécessaires à la vie privée doivent en général être limitées au strict nécessaire permettant d'atteindre les fins recherchées.

Le Cadre de référence d'exonération comporte également des dispositions et des exceptions applicables à la recherche. À la question nº 1 de la FAQ, on prévoit des exceptions à l'interdiction générale d'utiliser les renseignements sensibles, dont les renseignements personnels sur la santé. Le traitement des renseignements sera permis, notamment, pour la sauvegarde des intérêts primordiaux de la personne concernée, lorsqu'il sera nécessaire à des fins médicales ou de diagnostic, ou aux fins d'une poursuite judiciaire. Ces exceptions sont calquées sur les exceptions de la *Directive de l'UE relative aux données à caractère personnel*.

La question nº 14 de la FAQ vise directement les problèmes d'utilisation des renseignements personnels sur la santé concernant une personne identifiable dans la recherche pharmaceutique et dans celle sur les produits médicaux. La FAQ interprète ou clarifie certains points tels l'anonymat, le codage, l'utilisation secondaire et l'application des normes de l'UE plutôt que celle des normes américaines lorsque l'information reçue aux États-Unis provient d'Europe. Il indique que des données codées d'une manière particulière reçues d'un pays de l'UE pourront échapper à l'emprise des principes dans certaines circonstances. La FAQ prévoit qu'il en sera ainsi lorsque, par exemple, un chercheur européen lié par les principes aura codé les données d'une manière particulière, de manière à ce que la compagnie pharmaceutique commanditaire et les chercheurs américains ne puissent les identifier. À la question nº 14 de la FAQ, on prévoit également une règle générale connexe : les données utilisées à des fins de recherche pharmaceutique et à certaines autres fins doivent être rendues anonymes lorsque cela s'impose. La FAQ prévoit aussi que l'utilisation secondaire des données transférées d'Europe est autorisée lorsqu'elle est conforme aux fins générales de la recherche pour laquelle elles ont été recueillies ou lorsqu'un nouveau consentement a été obtenu. Pour éviter toute ambiguïté au sujet des fins compatibles ou incompatibles, on propose à la question nº 14 de la FAQ d'inclure dans la notion de consentement éclairé à une recherche l'explication qu'une recherche future qui à ce moment ne peut être précisée ni être prévue pourrait exiger l'utilisation des données personnelles de la personne concernée compte tenu de la nature de la recherche.

### f. Conservation et sécurité des données

Le principe de sécurité oblige les organismes qui ont adhéré aux normes d'exonération *Safe Harbor* à prendre des « précautions raisonnables » pour protéger les données personnelles contre les accès non autorisés, l'utilisation abusive, la destruction, l'altération ou la perte. Le Cadre de référence d'exonération ne semble pas comporter de norme explicite sur la durée de conservation des données.

### g. Autres dispositions intéressantes

Le contrôle général d'application du Cadre de référence d'exonération et celui de son observation ont été confiés à la *Federal Trade Commission* (FTC), un organisme de réglementation indépendant associé au Ministère américain du Commerce. Ce contrôle comprend l'étude des plaintes portées en matière de protection à la vie privée et la réponse à ces plaintes. Les entités qui engagent la procédure écrite d'autocertification au Ministère du Commerce de leur adhésion aux principes doivent reconnaître l'autorité répressive de la FTC. Les pouvoirs limités de la FTC préoccupent les analystes de l'UE.

# Bibliographie

**Cette bibliographie comporte trois parties :**
- **Ouvrages généraux**
- **Organisations internationales**
- **Pays**

## Ouvrages généraux

Annas G.J. et Grodin M.A., *The Nazi Doctors and the Nuremberg Code : Human Rights in Human Experimentation.* Oxford University Press, New York, 1992.

Banisar D, *Privacy and Human Rights : An International Survey of Privacy Laws and Developments*, Electronic Privacy Information Center (EPIC), Washington, 2000.

Callens S., The Privacy Directive and the Use of Medical Data for Research Purposes, *European J. Health L.*, nº 2, 1995, p. 309-340.

Mason J.K, McCall Smith R.A. *Law and Medical Ethics.* 4th ed. Butterworth's: London, 1994.

Michael J., *Privacy and Human Rights,* UNESCO et Dartmouth Publishing, Paris, 1994.

Treseder P., Williams P., The Common Principles of Health Informatics Standardisation that Require Exchange of Information Between the Standardisation Bodies of Different Countries, *Int. J. Med. Inf.* nº 48, 1998, p. 39-42.

*Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No. 10.*, volume 2. Washington, DC: U.S. Government Printing Office, 1949.

## Organisations internationales

### *Association médicale mondiale*

*Déclaration de Genève : Serment de Genève : Le serment medical*, modifié, Genève, 1948.

*Déclaration d'Helsinki : Recommandations à l'adresse des médecins dans le domaine de la recherche biomédicale portant sur des sujets humains,* Helsinki, 1964.

*Déclaration d'Helsinki* : *Principes éthiques applicables aux recherches médicales sur des sujets humains,* Édimbourg, 2000. Site Web : http://www.wma.net/f/policy/17-c_f.html

*Déclaration sur l'utilisation des ordinateurs en médecine*, fondée sur la résolution adoptée par la 27e assemblée médicale mondiale, Munich, octobre 1973, amendée par la 35e assemblée médicale mondiale, Venise (Italie), octobre 1983.

The 27th World Medical Assembly: Munich, October 14–20, 1973, 2 *World Med. J.*, 1974, pp.4-10.

## *Conseil de l'Europe*

*Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, Rome, 4 novembre 1950, R.T.E. nº 5, 213 R.T.N.U. 222. Site Web : http://conventions.coe.int/Treaty/fr/cadreprincipal.htm

*Convention 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*, Oviedo, 1997, R.T.E. nº 164. Site Web : http://conventions.coe.int/Treaty/FR/CadreListeTraites.htm

*Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28 janvier 1981, R.T.E. nº 108. Site Web : http://conventions.coe.int/Treaty/FR/Treaties/Html/108.htm

*Projet de protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (RTE* nº *108) concernant les autorités de contrôle et les flux transfrontaliers de données et Rapport explicatif*, Strasbourg, 2000. Site Web : http://stars.coe.fr/ta/TA00/fopi217.htm

Cour européenne des droits de l'homme, Recueil des arrêts, *M.S. c. Suède*, 27 août 1997; *Z. v. Finland*, 25 février 1997, 45 B.M.L.R.107.

### Recommandations du Conseil de l'Europe

*Recommandation* nº *R(83)10 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques*, Strasbourg, 1983.

*Recommandation* nº *R(91)10 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics*, Strasbourg, 1991.

*Recommandation nº R(97) 18 concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques*, Strasbourg, 1997.

*Recommandation nº R(97)5 du Comité des ministres aux États membres relative à la protection des données médicales*. Strasbourg, 1997. Site Web : http://cm.coe.int/ta/rec/1997/f97r5.html

*Exposé des motifs, Recommandation R97(5) relative à la protection des données médicales, par. 41, 43 et 44.* Site Web : http://cm.coe.int/stat/F/Public/1997/fExpRec(97)5.htm

## *Nations Unies*

*Charte des Nations Unies, Préambule,* San Francisco, Nations Unies, juin 1945.

*Déclaration universelle des droits de l'homme,* New York, United Nations, adoptée par résolution de l'Assemblée générale nº 3/217A du 10 décembre 1948. Site Web : http://www.unhchr.ch/udhr/lang/frn.htm

Organisation mondiale de la santé, *Déclaration sur la promotion des droits des patients en Europe,* Consultation européenne sur les droits des patients, Amsterdam 1994, Réimpression (en anglais) dans *European J. Health L.*, nº 1, 1994, pp. 279-291 Site Web : http://www.who.int/library/reference/information/declarations/index.fr.shtml

*Pacte international relatif aux droits civils et politiques,* adopté et ouvert à la signature, à la ratification et à l'adhésion par résolution de l'Assemblée générale nº 2200A (XXI) du 16 décembre 1966, R.T.C. 1976, nº 47, RTNU, vol. 999, nº 171. Site Web : http://www.unhchr.ch/french/html/menu3/b/a_ccpr_fr.htm

*Pacte international relatif aux droits économiques, sociaux et culturels,* adopté et ouvert à la signature, à la ratification et à l'adhésion par résolution de l'Assemblée générale nº 2200A (XXI) du 16 décembre 1966.

*Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel,* adoptés par l'Assemblée générale le 14 décembre 1990, résolution 45/95, New York, 1990. Site Web : http://www.unhchr.ch/french/html/menu3/b/71_fr.htm

Unesco, *Déclaration universelle sur le génome humain et les droits de l'homme,* Paris, 1997. Site Web : http://www.unesco.org/ibc/fr/genome/projet/

Unesco, *Groupe de travail du Comité international de bioéthique sur la confidentialité et les données génétiques, Rapport sur la confidentialité et les données génétiques,* Paris, juin 2000.

## *Organisation de coopération et de développement économiques (OCDE)*

Conférence ministérielle, *Un monde sans frontières : Concrétiser le potentiel du commerce électronique mondial.* Voir la Déclaration ministérielle sur la protection de la vie privée sur les réseaux mondiaux. Site Web : http://www.oecd.org/dsti/sti/it

*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel,*OCDE, Paris, 1981. Site Web : http://www1.oecd.org/dsti/sti/it/secur/prod/priv-fr.html

Exposé des motifs : Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, OCDE, Paris, 1981. Site Web : http://www1.oecd.org/dsti/sti/it/secur/prod/priv-fr.html

### *Union européenne*

Groupe européen d'éthique des sciences et des nouvelles technologies auprès de la Commission européenne, *Aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information*, Avis nº 13, Bruxelles, 30 juillet 1999. Site Web : http://europa.eu.int/comm/european_group_ethics/docs/avis13_fr.pdf

Parlement européen et Conseil de l'Europe, *Charte des droits fondamentaux de l'Union européenne*, Nice, 2000. Site Web : http://www.europarl.eu.int/charter/default_fr.htm

Parlement européen et Conseil de l'Europe, *Directive 95/46/EC 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*, Journal officiel L 281, 23/11/1995 p. 0031-0050 Site Web : http://europa.eu.int/eur-lex/fr/lif/dat/1995/fr_395L0046.html

## Pays

### *Australie*

**National Health and Medical Research Council.**

*Guidelines Under Section 95 of the Privacy Act 1988*, Canberra, 2000. Site Web : http://www.health.gov.au/nhmrc/issues/researchethics.htm

*National Statement on Ethical Conduct in Research Involving Humans*, Canberra, 1999.

*Joint National Health and Medical Research Council/Australian Vice-Chancellors'Committee Statement and Guidelines on Research Practice (1997).*

**Bureau du Commissaire à la Protection de la vie privée**

*Draft Health Privacy Guidelines*, Canberra, 14 mai 2001. Site Web : http://www.privacy.gov.au

*National Principles for Fair Handling of Personal Information, Australia*, Canberra, 1999. Site Web : http://www.privacy.gov.au/news/health.html

Parliament of the Commonwealth of Australia, House of Representative Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000*. Site Web : http://www.aph.gov.au/house/committee/laca/privacybill/contents.htm

*Privacy Act 1988*, Act No. 119 of 1988, modifié. Site Web : http://www.austlii.edu.au

*Privacy Amendment (Private Sector) Act 2000*, Act nº 155 of 2000, modifiant le *Privacy Act 1988* Site Web : http://www.privacy.gov.au

*The Private Sector : National Privacy Principles* Voir *Privacy Amendment (Private Sector) Act 2000*.

*The Public Sector Standards : Information Privacy Principles*, Voir *Privacy Amendment (Private Sector) Act 2000*, Senate Debate on Privacy Amendment (Private Sector) Bill. Site Web : http://www.law.gov.au/privacy/senatedebate.htm

*The Commonwealth of Australia Constitution Act.* Site Web : http://www.republic.org.au/const/cconst.html

## *Canada*

*Instituts de recherche en santé du Canada, Recueil des dispositions législatives canadiennes sur la protection des renseignements personnels dans le contexte de la recherche en santé*, Travaux publics et Services gouvernementaux du Canada, Ottawa, 2000. Site Web : http://www.cihr.ca.

*Loi sur la protection des renseignements personnels et les documents électroniques, L.C. (2000), ch. 5.* Site Web : http://www.privcom.gc.ca

## *États-Unis*

*Clinical Laboratory Improvements Amendments*,1998. United States Code, vol. 42, alinéa 263a, mise en œuvre en partie en vertu du *Code of Federal Register*, vol. 42, alinéa 493.3(a)(2).

*Federal Food, Drugs and Cosmetics Act*, United States Code, vol. 21, alinéa 263a, mise en œuvre en partie en vertu du *Code of Federal Register*, vol. 42, alinéa 493.3(a)(2).

*Federal Privacy Act*, 1974. PL 93-579, 5 USC 552a, modifié, Site Web : http://www.epic.org/privacy/laws/privacy_act.html

Freeman P. et Robbins, A., US Health Data Privacy Debate : Will There be Comprehension Before Closure?, *Int. J. Technol. Assess. Health Care*, vol. 15, nº 2, 1999, p. 316-331.

General Accounting Office, *Medical Records Privacy : Access Needed for Health Research, but Oversight of Privacy Protections is Limited*, Washington, February 1999.

*Health Insurance Portability and Accountability Act of 1996*, PL 104-91, 42 USC 1320-d, modifé. Washington, September 1997. Site Web : http://aspe.hhs.gov/admnsimp/pvcrec0.htm

*Heroic Assemblage of Information About State Laws by Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, Shows Complexity, The State of Health Privacy : An Uneven Terrain (1999).* Site Web : http://www.healthprivacy.org/info-url_nocat.htm

Hodge J.G., Gostin L.O. et Jacobson, P.D., Legal Issues Concerning Electronic Health Information : Privacy, Quality and Liability, *J. Amer. Med. Assoc.*, nº 282, 1999, p. 1466-1471.

*Public Health Service Act*, modifié, 42 USC 241(d) et 299dd-2, Regulations, CFR, vol. 42, Partie 2.

*United States Privacy Protection Study Commission, Personal Privacy in an Information Society : Report of the Privacy Protection Study Commission*, Washington, 1977.

US Department of Commerce, *Safe Harbor Framework*, Washington, juillet 2000. Site Web : http://www.export.gov/safeharbour/sh_documents.html

**US Department of Health and Human Services (DHHS) [Ministère de la Santé et des Services sociaux]**

*(Basic DHHS Policy for Protection of Human Research Subjects)*, Regulations on Protection of Human Subjects, Federal Register 18 juin 1991; 56 p. 28003, Code of Federal Register, vol. 45, nº 46. Site Web : http://ohsr.od.nih.gov/mpa/45cfr46.php3

*Recommendations of the Secretary of Health and Human Services, Pursuant to Section 264 of the Health Insurance Portability and Accountability Act of 1996*, Washington, septembre 1997. Site Web : http://aspe.hhs.gov/admnsimp/pvcrec0.htm

*Standards for Privacy of Individually Identifiable Health Information—Final Rule*, Fed. Reg. 28, décembre 2000, vol. 65, nº 250, p. 82467. Site Web : http://www.hhs.gov/ocr/hipaa

US Department of Health and Human Services (DHHS) *Code of Fair Information Practice Principles*, 1973 [Code des principes de pratiques d'information loyale].

## *France*

Braibant G., *Données personnelles et société de l'information*, Rapport au Premier Ministre sur la transposition en droit français de la directive nº 95/46, Paris, 3 mars 1998. Site Web : http://www.cnil.fr/textes/indextranspo.htm

*Code civil*. Site Web: http://www.legifrance.gouv.fr/citoyen/new_code.ow

*Code de déontologie médicale.* Site Web : http//www.legifrance.gouv.fr/citoyen/new_code.ow

*Code Pénal.* Site Web : http://www.legifrance.gouv.fr/citoyen/new_code.ow

Commission nationale de l'informatique et des libertés [CNIL], Traitements des données de santé à caractère personnel, délibération nº 97-008 du 4 février 1997, *Journal Officiel* du 12 avril 1997. Site Web : http://www.cnil.fr

Conseil Constitutionnel, *Décision 94-352* du 18 janvier *1995*.

*Décret nº 78-774* du 17 juillet 1977. *Journal officiel* du 23 juillet *1997.*

*Décret nº 95-682* du 9 mai 1995*. Journal Officiel* du 11 mai 1995.

*Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Journal Officiel du 7 janvier 1978*. Site Web : http://www.legifrance.gouv.fr

*Loi nº 79-18 de 3 janvier 1979 sur les archives, Journal Officiel* du 5 janvier 1979, nº 49, corrigé dans le *Journal Officiel* du 6 janvier 1979, nº 55. Site Web : http://www.cnil.fr/textes/text052.htm

*Loi nº 94-548 du 1er juillet relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé* et modifiant *la Loi nº 78-17 du 6 janvier relative à l'informatique, aux fichiers et aux libertés. Journal officiel* du 2 juillet 1994.

## *Nouvelle-Zélande*

*Application by L*. (1997), 3 HNRX 716 (Tribunal d'examen des plaintes).

*Health Act 1956, modifié. Lois réimprimées de la Nouvelle-Zélande, 1993 ; 31(1), pp. 467-563.*

*Health (Retention of Health Information) Regulations* 1996, pris en vertu de l'art. 121 du *Health Act 1956 modifié.*

*Privacy Act 1993*. Site Web : http://www.privacy.org.nz/recept/rectop.html

**Commissaire à la protection de la vie privée de la Nouvelle-Zélande.**

*Discussion Paper No 12: New Privacy Protections*, Auckland, 1998. Site Web : http://www.privacy.org.nz/slegisf.html

*Health Information Privacy Code 1994*, Auckland, 1994, Modifié, Édition révisée, 2000. Site Web : http://www.privacy.org/nz/recept/rectop.html

Von Tigerstrom B., The Hidden Story of Bill C-54 : The Personal Information Protection and Electronic Documents Act and Health Information, *Health Law Rev.* vol. 8, nº 2, 1999, p. 12.

## *Pays-Bas*

*Constitution du royaume des Pays-Bas, 1989,* art.10.

Ploem M.C., Medical Research and Informational Privacy, 17 *Medicine and Law,* 1998, pp. 287-297.

*Wet persoonsregistraties ( Loi sur l'enregistrement des données personnelles*), 28 décembre 1988. Site Web : http://home.planet.nl/~privacy1

*Wet bescherming persoonsgegevens ( Loi sur la protection des données personnelles*), 6 juillet 2000, Staatsblad 2000 302 (traduction non-official). Sites Web : http://www.registratiekamer.nl/; http://home.planet.nl/~privacy1

*Wet geneeskundige behandelingsovereenkomst (Loi sur le contrat de traitement médical, Loi du 17 novembre 1994, modifiant le Code civil et d'autres lois relativement à l'incorporation de dispositions concernant le contrat de traitement médical).* Stb 1994, p. 837.

### *Royaume-Uni*

British Medical Association, *Confidentiality and Disclosure of Health Information*, London, 1999. Site Web : http://www.bma.org.uk (ethics/guidelines)

*Data Protection Act 1998*, ch. 29, remplaçant le *Data Protection Act* de 1984. Site Web : http://www.data protection.gov.uk

*Human Rights Act 1998*, c. 42.

Medical Research Council (Grande-Bretagne), *Personal Information in Medical Research, (Ethics Series)*, Londres, 2000. Site Web : http://www.mrc.ac.uk/ PDFs/PIMR.pdf

Strobl J., Cave E. et Walley T., Data Protection Legislation : Interpretation and Barriers to Research, *BMJ*, 2000, nº 321, pp. 890-892.

Royaume-Uni, Secrétariat d'État, *The Data Protection (Processing of Sensitive Personal Data) Order 2000 : Statutory Instrument 2000 nº 417*. Londres, février 2000, para. 9.

Royaume-Uni, Secrétariat d'État, *The Data Protection (Subject Access Modification) (Health) Order 2000 : Statutory Instrument 2000* No *413*, Londres, février 2000.

Warlow C., Using Patient-Identifiable Data for Observational Research and Audit, *BMJ*, 2000, nº 321, pp.1031-1032.