INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps

Photographs included in the original manuscript have been reproduced xerographically in this copy Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge Contact UMI directly to order.

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA

UMI®
800-521-0600

PROTECTION DE LA VIE PRIVEE A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES PERSONNELLES

SIBYLLE VAN OUTRYVE D'YDEWALLE

L.L.M Thesis July 1997

Institute of Comparative Law Copy # 1

McGill University, Montreal FINAL

Name of supervisor : PROFESSOR H. PATRICK GLENN

A thesis submitted to the faculty of graduate studies and research in partial fulfillment of the requirements of the degree of Master.

La Commission des Communautés européennes a récemment adopté une directive relative à la protection de la vie privée à l'égard du traitement automatisé des données personnelles. L'auteur examine cette directive et en rappelle les principes fondamentaux ainsi que les autres textes internationaux déjà en vigueur. Cette directive pourrait avoir de sérieuses répercussions sur la circulation internationale des données d'où peuvent être exclus les pays n'incorporant pas dans leur droit national les principes énoncés par la directive. L'auteur étudie par conséquent les législations canadiennes et québécoises en vigueur ainsi que les codes de conduite volontaires afin de déterminer s'ils satisfont aux normes proposées par la directive.

The Commission of European Communities has recently adopted a directive concerning the protection of privacy with regard to automatic processing of personal data. The author examines this directive and highlights its fundamental principles as well as the other international documents already in force. This directive may have serious implications for the international flow of data from which could be excluded countries which do not include in their national law the principles set out in the directive. Consequently the author examines the legislations of Canada and Quebec in force as well as the voluntary codes of conduct in order to determine whether they comply with the standards proposed by the directive.

TABLE DES MATIERES

REMERCIEMENTS

Je tiens à remercier les membres de la DG XIII de la Commission européenne ainsi que de la Commission de la protection de la vie privée pour leurs précieuses suggestions dans l'élaboration de ce travail. La collaboration essentielle de ma secrétaire se doit également d'être soulignée. Je remercie tout particulièrement mon époux et mes parents sans qui rien de tout ceci n'aurait été possible.

INTRODUCTION

Les technologies nouvelles sont une menace certaine pour la vie privée[1]: la somme d'informations qu'à son insu le consommateur livre, par le seul usage de cartes magnétiques, permet de tracer de lui, en connectant les données divulguées, un portrait complet comprenant son emploi du temps, ses préférences, ses opinions, ses pratiques, soit un profil de sa personnalité et, par voie de conséquence, son coefficient de conformité, de marginalité ou de déviance.

A supposer qu'on tienne à la valeur "*vie privée*", il y a une raison décisive de douter non de la légitimité de sa protection mais de sa possibilité. Les nouveaux langages informatiques permettent, par exemple, d'interroger plusieurs bases de données et d'en extraire des renseignements sans laisser aucune trace localisable de l'opération, permettant à l'auteur de se mettre hors d'atteinte de toute répression[2].

Ce qui est ainsi menacé par la connexion des fichiers informatisés est infiniment plus dangereux: c'est l'équilibre même des pouvoirs dans la société[3]. Si l'individu devient transparent aux yeux des pouvoirs publics, de moins en moins maîtres du contrôle des données, et des entreprises privées, réelles détentrices des monopoles de l'information, l'inégalité dans les rapports sociaux s'aggrave. Ce qui doit inquiéter est moins

---

[1] Selon un sondage mené par la Commission européenne, 57 % des citoyens européens estiment que les technologies nouvelles représentent un danger pour la protection de la vie privée (CE, Commission, *DG XV News*, mars 1995, n° 1, p. 19).

[2] Sur la perte de contrôle par l'individu des données en matière de multimédia et services interactifs, voir P. Thomas et M.H. Boulanger, "Y a-t-il un ange gardien dans la salle", C. Doutrelepont, P. Van Binst et L. Wilkin, dir., dans *Libertés, droits et réseaux dans la société de l'information*, Bruxelles, Bruylant, 1996, p. 214 et s.

[3] A. Vitalis, *Information, pouvoirs et libertés*, 2e éd.,Paris, Economica, 1989, p. 160.

l'indiscrétion croissante envers les individus que la concentration du pouvoir[4].

Pour le juriste, la question première n'est pas celle de savoir comment réagir face aux nouvelles technologies mais plutôt celle de savoir si il doit intervenir et par quels moyens. Il convient dès lors de centrer l'analyse de l'intervention juridique sur les attitudes possibles et non sur les solutions existantes, souvent temporelles, fragmentaires ou contradictoires, "*la réponse juridique ne se cantonnant pas dans une seule catégorie formelle du droit*[5]".

Le juriste ferait en effet fausse route s'il croyait pouvoir appliquer ses normes aux mutations technologiques sans n'être au préalable imprégné des forces en présence, des enjeux en cause et des valeurs en péril. Ce conflit entre les technologies nouvelles et le droit à la vie privée est encombré de paradoxes dont il faut prendre la mesure avant de prétendre les conjurer.

C'est pourquoi il semble indiqué d'examiner, dans un premier temps, les sources du droit à la vie privée ainsi que le sens et la portée de ce droit tant en droit privé (en common law et en droit civil), qu'en droit public. Il faudra également analyser ses caractères et leur éventuelle évolution (critique de la qualification dominante des droits de la personnalité: il s'agirait de droits absolus, subjectifs et non patrimoniaux), afin de répondre à l'interrogation: peut-il protéger adéquatement les données personnelles ? A cet effet, qu'en est-il du droit à la vie privée informationnelle ?

---

[4] Jusqu'ici, la diffusion des données personnelles a toujours renforcé les pouvoirs et consolidé les inégalités; F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant, 1990, p. 603, n° 539; F. Rigaux, "La liberté de la vie privée", (1991) 3 R.I.D.C. 539, p. 556.

[5] H.P. Glenn, "Les nouveaux moyens de reproduction audio-visuelle et numérique et les droits de la personnalité: Rapport général", (1986) 46 R. du B. 693, p. 697.

Dans un second temps, nous nous pencherons sur les moyens dont dispose le droit pour assurer la protection transnationale des renseignements personnels. Outre les Lignes directrices *"régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel"*, adoptées par l'O.C.D.E. le 23 septembre 1980, et la Convention du Conseil de l'Europe *"pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel"*, adoptée le 17 septembre 1980, la Directive européenne du 24 octobre 1995 *"relative à la protection des personnes à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données"* offre un cadre législatif intéressant pour appréhender les nouvelles technologies, instaurant des règles de protection communes, parfois qualifiées de *"pratiques équitables en matière d'information"* (*fair information practices*) et qui constituent le faisceau minimal sur base duquel s'effectueront les échanges transfrontières de données personnelles, dans le secteur tant public que privé.

La circulation des données personnelles dépassant les frontières de l'Union européenne, il nous a paru souhaitable d'examiner la Loi fédérale canadienne *"sur la protection des renseignements personnels"*, adoptée en février 1985 et s'appliquant au seul secteur public, ainsi que les Lois québécoises *"sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels"* et *"sur la protection des renseignements personnels dans le secteur privé"*, adoptées respectivement en 1982 et 1994, au regard du principe de *"protection adéquate"* inscrit à l'article 25 de la Directive européenne et selon lequel une restriction à une transmission de données personnelles vers un Etat tiers à l'Union européenne, peut, sous réserve des dispositions nationales, être légitime si ce dernier n'offre pas une protection adéquate au regard de celle qui a cours dans l'Etat exportateur.

Se pose ainsi la question du sens à attribuer à cette expression, à la lumière des instruments nationaux et internationaux. Signifie-t-elle que le pays tiers doit être pourvu

d'une législation en bonne et due forme, dont l'effectivité sera assurée par le respect des principes fondamentaux identifiés dans les instruments internationaux. Dans quelle mesure, l'existence de règles éparses, non assemblées dans un instrument unique et cohérent ou l'auto-réglementation, du type "*code de conduite*" tel celui élaboré par l'Association canadienne de normalisation, satisfait-elle au critère de "*protection adéquate*" ?

La discussion est loin d'être purement académique. De sa réponse dépendra l'exclusion de pays tiers à l'Union européenne, tels les Etats-Unis, le Japon, l'Australie ou le Canada dont il n'est pas certain que le niveau de protection qu'ils sont à même de proposer, puisse être jugé "*adéquat*" au sens proposé par la Directive européenne pour autoriser les transferts de données personnelles à destination de ces pays, leurs institutions publiques et leurs entreprises privées ayant alors à souffrir d'un désavantage commercial qu'elles ne pourraient s'autoriser[4].

---

[4] En 1990, environ 21 % des organisations publiques et des entreprises canadiennes communiquaient des renseignements personnels à l'étranger (R. Laperrière, R. Côté, G.A. Le Bel, P. Roy et K. Benyekhlef, "*Vie privée sans frontières: les flux transfrontières de renseignements personnels en provenance du Canada*", Ottawa, Ministère fédéral de la Justice, 1991).

CHAPITRE 1 - LE DROIT A LA VIE PRIVEE

SECTION 1 - SOURCES DU DROIT A LA VIE PRIVEE

SOUS-SECTION 1 - DROIT PRIVE

Paragraphe 1 - Common law

Si le droit à la vie privée fait l'objet d'une reconnaissance jurisprudentielle aux Etats-Unis - la jurisprudence ayant accueilli très tôt le *"right of privacy"* défini par Warren et Brandeis[7] -, celle-ci ne s'est pas développée de manière cohérente et systématique.

Ce right of privacy *"se limite au droit au secret, à la protection contre toute divulgation portant sur la vie privée du sujet et ayant pour objet ses productions artistiques, intellectuelles ou même des écrits personnels sans valeur littéraire (...). [Ce] principe est tempéré d'une série d'exceptions, notamment la liberté de rendre public ce qui est d'intérêt privé ou général, l'extension de ces exceptions admises en matière de*

---

[7] S.D. Warren et L.D. Brandeis, *"The Right of Privacy"*, (1890) 4. Harv. L.R. 193-220; F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité, supra* note 4, p. 630, n° 566: *" l'un des apports les plus originaux de Warren et Brandeis a consisté à rapprocher l'une de l'autre deux notions dont la première était empruntée au droit constitutionnel, pour les implanter en droit civil. Ces notions sont la privacy, évoquée notamment dans Boyd v. United States, 116 U.S. 616, 630 (1886), et "the right to be let alone", expression introduite par le juge Cooley dans son ouvrage sur les Torts [Cooley on Torts, 2è éd., 1888, p. 29; 3è éd., 1906, p. 33] et que Warren et Brandeis utiliseront pour définir la privacy. (...) ceux-ci ne paraissent pas connaître ou s'abstiennent de citer une décision américaine ayant utilisé la notion de privacy dans une affaire civile" (De May v. Roberts, 46 Mich. 160, 9. N.W. 146 (1881))*, ce qui ne parait pas si curieux dès lors que le fondement de la notion de privacy consacrée par Warren et Brandeis est constitutionnel.

diffamation, le refus de toute action en cas de divulgation orale, le consentement du sujet. En revanche, ni la vérité du fait ni l'absence de dol (malice) ne procurent un moyen de défense à l'auteur d'une atteinte à la privacy", envisagée comme un concept unitaire des différents *"torts"*[8].

Peuvent ainsi être distingués, selon Prosser[9], quatre séries de torts: (i) l'intrusion dans la solitude ou dans les affaires privées du demandeur[10], (ii) la divulgation de faits privés embarrassants[11], (iii) la publicité plaçant le demandeur sous un faux jour devant le public[12] et (iv) l'appropriation au profit du défendeur du nom ou de l'image du demandeur[13].

---

8 Nombre d'auteurs américains ont souligné le caractère *"patricien"* de cette définition qui exprime les valeurs d'une classe sociale restreinte (l'article de 1890 résultant de l'agacement causé à Samuel Warren, avocat réputé de Boston, par un commentaire désobligeant qu'un journal de la ville avait publié sur son épouse et sa fille), qui a contaminé tout le droit de la privacy (voir A.F. Westin, *Privacy and Freedom*, New York, Atheneum, 1967, p. 348; D.R. Pember, *Privacy and the Press, The Mass Media and the First Amendment, 1972, p. 23)*.

9 W.L. Prosser, "Privacy", (1960) 48 *Cal. L.R. 383*, p. 389; Prosser critique l'unité de *"la"* privacy qui serait factice. Il s'agit plutôt d'un conglomérat de *"torts"* qui s'ils auraient en commun le caractère moral ou affectif de l'intérêt protégé, ne peuvent pas être repris sous un concept unitaire, la privacy. Comme l'a observé F. Rigaux, (*La protection de la vie privée et des autres biens de la personnalité supra* note 4, p. 633, n° 567), en réalité, l'article de R. Pound proposait déjà une classification des multiples *"interests of personality"* (R. Pound, "The Right of Privacy" (1932) *Illinois L.R.* 237-260).

10 *Barber v. Lime*, Inc., 348 Mo. 1199, 159 S.W. 2d 291 (1942); *Rhodes v. Graham* 238 Ky. 225, 37 S.W. 46 (1931).

11 *Brents v. Morgan*, 221 ky. 765, 299 S.W. 967 (1927); *Melvin v. Reid*, 112 Cal. App. 285, 297 P. 91 (1931); *Sidis v. F.R. Publishing Corporation*, 113 F. 2nd 806 (2d circ) (1940).

12 *Gill v. Curtis Pub. Co.*, 38 Cal. 2d 273, 239 P. 2d 630 (1952), *Hinish v. Meir and Frank Co.*, 166 Ore. 482, 113 P. 2d 438 (1942).

13 *Fitzsimmons v. Olinger Mortuary Ass'n*, 91 Colo. 544, 17 P. 2d 535(1932).

Cette distinction[14] a été critiquée par certains auteurs[15], actualisée par d'autres[16]. Contrairement à ce que laisse paraître Warren et Brandeis en faisant appel à des sources jurisprudentielles anglaises[17], la common-law anglaise[18] de même que canadienne[19] ou

---

[14] Qui a largement influencé la jurisprudence en Californie, puis dans d'autres Etats et qui a été intégralement reprise dans la section 652 A (2) du Restatement (Second) of Torts.

[15] Voir F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 633, n° 567 et les réf. citées: *"(...) la classification de Prosser n'a pas atteint son principal objectif, conjurer le fantôme de la privacy. De plus, elle n'est pas exhaustive, et la distinction qu'elle établit entre des situations voisines est souvent artificielle. Les cas d'appropriation de l'image ou de la personne d'autrui ont le plus souvent pour effet de présenter cette personne sous un faux jour; certaines hypothèses qui y appartiennent ne se laissent pas clairement distinguer de "torts" traditionnels, distincts de la privacy: tel est le cas pour l'intrusion et le "trespass" ou pour la "false light" et la diffamation. Enfin, elle ne ménage pas une distinction satisfaisante entre une invasion of privacy et l'atteinte à un "proprietary interest" (right of publicity)"*; J.P. Graham, "Privacy, Computers and Commercial Dissemination of Personal Information", (1987) Texas L.R. 1395, p. 1406: *"The classification of Dean Prosser has frozen the development of privacy law despite the creation of new technologies, that detrimentally affect individual privacy"* et pp. 1417-1418: *"Dean Prosser's explication of privacy invasions as falling into four distinct categories has exercised virtual intellectual hegemony over privacy law [...]. The criteria developed to protect the common law notion of privacy, however are no longer appropriate to the task of preventing invasions of privacy made possible through the application of computer technology"*.

[16] Dans la mesure où cette distinction semblait dépassée dans un contexte informatique de gestion et d'échanges de données personnelles, Westin y a ajouté (v) la surveillance psychologique et (vi) la surveillance informationnelle (A.F. Westin, *supra* note 8, pp. 133-168); voir A.R. Miller, *The Assault on Privacy*, Michigan, The University of Michigan Press, 1971, p. 187; M. Rankin, "Privacy & Technology: A Canadian Perspective", (1984) 22 Alberta L.R. 323, p. 325.

[17] Notamment *Prince Albert v. Strange*, (1849) 2 De G. and Sm. 712, 64 ER 304 (Chanc.); *Abernethy v. Hutchinson* (1825) 1 H and Tw. 28, 47 E.R. 1313 (Chanc.); *Gee v. Pritchard* (1818) 2 Swartson 403, 36 E.R. 670 (Chanc.); Sur cet arrêt, voir F. Rigaux, "La liberté de la vie privée", 1991, R.D.I.C., *supra* note 4, p. 542, n° 3-4; F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 630, n° 566: *"(...) alors que la notion n'avait pas et n'a guère acquis depuis une connotation juridique en Angleterre. Telle est une des critiques souvent adressée, même aux Etats-Unis, au concept de privacy ayant sans conteste une signification sociologique, il est privé de portée juridique"*. D'où les critiques qui substituent au concept de privacy un autre concept plus adéquat: *"personality"* (R. Pound, *supra* note 9, p. 988 (Comp.: L. Post, 77 California L.R. 963: l'origine sociale le conduit à parler de *"Social personality"*) ou *"Personhood"* (J.W. Rebone, "Personhood and the Contraceptive Right" (1982) 57 Indiana L.J. 579-604) ou *"autonomy"* ou *"dignity"*; F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, *supra* note 4, p. 3 *"[Ces] modifications terminologiques ne portent pas atteinte à l'idée inspiratrice de Warren et Brandeis: que le sujet est protégé dans ses relations avec autrui (sans que soit spécifiquement abordé le pouvoir de l'administration) par une sphère qui lui appartient en propre (privacy), qui exprime sa*

australienne[20] ne reconnaît pas en tant que tel le droit à la vie privée.

Si la violation de la privacy n'est donc pas un *"tort"* nouveau ainsi qualifié, susceptible de reconnaissance judiciaire[21], certains aspects de ce droit se trouvent protégés par des modes d'actions traditionnels ouverts à la victime par la jurisprudence anglaise[22],

---

personnalité (personality) ou en est une émanation (personhood), qu'il gère de manière autonome (autonomy). Quelle que soit la dénomination utilisée, le concept procure une vision unitaire d'un grand nombre de situations ou de relations hétérogènes". Cette signification unificatrice des divers *"torts"* repris sous un concept unique, la privacy, sera contesté par Prosser (*supra* note 9).

[18] P.H. Winfield, "Privacy", (1931) *The Law Quaterly R.*, 23-42, 39.

[19] P. Burns, "The law and Privacy: the Canadian Experience", (1976) 54 R. du B. can. 1, p. 12: *"At a superficial level the common law of privacy is simple to summarize: there is no protection for personal privacy per se, at least outside the United States"*; D. Johnston, D. Johnston et S. Handa, Getting Canada Online - Understanding the information Highway, Toronto, Stoddart, 1995, p. 196.

[20] S. M. Skala, "Is there a Legal Right to Privacy?", (1977-78) 10 Queensland L.J. 127, p. 133.

[21] Fleming cité par P. Burns, *supra* note 19, p. 12: *"The right of privacy has not so far, at least under that name, received explicit recognition by British Courts. For one thing, the traditional technique in tort law has been to formulate liability in terms of reprehensible conduct rather than of specified interests entitled to protection against harmful invasion. For another, our courts have been content to grope forward, cautiously along the grooves of established legal concepts, nuisance and libel, rather than make a bold commitment to an entirely new head of liability"*.

[22] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 635, n° 569: *"La plupart des auteurs estiment que le droit anglais se passe aisément du concept de privacy et ils ont recueilli auprès d'une fraction de la doctrine américaine l'idée que les "torts" traditionnels suffisent à la tâche. Parmi les plus hostiles au concept [unitaire] de privacy, Raymond Wacks, ayant publié un article dont le seul titre est déjà significatif: "The Proverty of "Privacy"", 96 (1980) The law Quaterly R., 73-89. (...) L'article de Wacks tend à démontrer que toutes les situations visées par la privacy peuvent être réparties entre sept voies d'action effectivement ouvertes à la victime par la jurisprudence anglaise. Ainsi, la condamnation prononcée contre la privacy vise le concept générique couvrant des situations hétérogènes, non sur la nécessité de porter remède aux atteintes improprement dénommées "invasion of privacy". On a en effet rencontré dans la seconde partie de cet ouvrage plusieurs qualifications du droit anglais jugées adéquates en chacune des diverses occurrences: la diffamation (libel) et, plus rarement, l'injure verbale (slander) dont l'efficacité est renforcée par le discours allusif (innuendo), le breach of confidentiality, la protection de "proprietary interests". De manière assez paradoxale d'ailleurs, la victime d'un message diffamatoire est beaucoup plus efficacement protégée par le droit anglais que par le droit américain (...), la preuve de la vérité du fait portant atteinte à l'honneur pouvant (...) être administrés par le défendeur"*; Russel A. Donaldson, "Annotation, False Light Invasion of Privacy - Cognizability and Elements", (1991)

australienne[23] ou canadienne[24].

Face à cette protection indirecte et parcellaire, certaines législations canadiennes ont consacré un *"tort"* sanctionnable sans que le plaignant n'ait à rapporter la preuve d'un dommage au respect de sa vie privée[25]. La notion de vie privée n'est pas pour autant définie. Si ces lois énoncent certains facteurs susceptibles de guider le juge dans la détermination d'une violation de la vie privée[26], les tribunaux, insensibles à ce droit en raison de son inexistence en common law, ont refusé d'en étendre la portée en l'absence d'une volonté claire du législateur.

---

57 A.L.R. 4 22.

[23] G. Dworkin, "The Common Law Protection of Privacy", (1967) Univ. of Tasmania L. R., p. 422, pp. 432-433; *Victoria Park Racing and Recreation Co. Ltd v. Taylor*, (1937) 58 C.L.R. 479, 496.

[24] Raport du Groupe d'étude, *L'ordinateur et la vie privée*, Ottawa, Ministères des Communications et de la Justice, Ottawa, 1972, pp. 132-138: *"la common law pourrait bien, avec le temps, créer le concept général de délit en matière de vie privée. Pour le moment, toutefois, c'est sous les rubriques de diffamation et de violation de foi qu'elle offre la protection la plus immédiate, en ce qui concerne l'information"*; C. Dockrill, "Computer Data Banks and Personal Information: Protection Against Negligent Disclosure", (1988) 11 Dalhousie L.J. 546; D. Johnston, D. Johnston et S. Handa, *supra* note 19, pp. 203-204.

[25] Par exemple, Privacy Act, R.S.B.C., 1979, c. 336 (Colombie Britannique) en vertu duquel la violation délibérée de la vie d'autrui sans apparence de droit ou l'utilisation du nom ou de l'image d'autrui à des fins commerciales sans consentement constituent des *"torts"*; Privacy Act, S.M. 1970, c. 74 (Manitoba); Privacy Act, R.S.S., 1979, c. P-24, (Saskatchewan); An Act Respecting the Protection of Personal Privacy, S.N., 1981, c. 6 (Terre-Neuve); P.H. Osborne, "The Privacy Acts of British Columbia, Manitoba and Saskatchewan" dans D. Gibson, *Aspects of Privacy Law*, Toronto, Butterworths, 1980, p. 75; P. Burns, *supra* note ..., p. 32; d'autres dispositions législatives éparses protègent, parfois indirectement, le droit à la vie privée, telle que la partie VI du Code criminel (articles 183 et s.).

[26] Pour déterminer si l'acte ou la conduite d'un tiers constitue une violation de la vie privée, il faut tenir compte de la nature et des conséquences de l'acte ou de la conduite et de la nature des relations, familiales ou autres, entre les parties. Certaines activités n'attentent pas à la vie privée: lorsqu'il y a consentement du demandeur ou si l'acte ou la conduite a eu pour fondement la légitime défense, etc.; P. Burns, *supra* note ..., p. 32; Rapport du Groupe d'étude, *L'ordinateur et la vie privée*, *supra* note 24, pp. 141-143.

Paragraphe 2 - Droit civil

Les controverses doctrinales du XIXe siècle, tant celles des pandectistes que celles des germanistes (privatistes et publicistes)[27] se sont terminées à la fin du siècle, notamment sous l'influence des spécialistes des droits intellectuels, par la reconnaissance du droit de la personnalité dans les relations de droit privé. La jurisprudence allemande postérieure à la seconde guerre mondiale a également déduit du droit constitutionnel à l'épanouissement de la personnalité[28] un *"droit général de la personnalité"*, existant à côté des droits de la personnalité particuliers[29] et protégeant tout sujet de droit contre les atteintes émanant d'autres agents juridiques privés[30]. Ce droit général de la personnalité est considéré comme un droit absolu et subjectif[31].

De même, la doctrine française, à la suite de la reconnaissance par la jurisprudence du

---

[27] Voir F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 611, n° 546 et s.

[28] Article 2, alinéa I de la Loi fondamentale de 1949; *supra, Sous-section 2. Droit public.*

[29] Tels le droit au nom, le droit moral de l'auteur, le droit à la propre image, etc., sanctionnés par quelques lois spéciales.

[30] Sont ainsi protégés: la sphère privée, le droit au secret et la sphère d'intimité, l'honneur, le droit de maîtriser la manière dont une personne se présente en public, le droit à la propre image et à la maîtrise de l'expression orale ou écrite ainsi qu'en certaines circonstances, le droit d'être protégé contre l'imputation de propos que le sujet n'a pas tenus. (BVerfG, 3 juin 1980, *Heimrich Böll*, BVerfGE 54, 148, 154); la doctrine entérinant la jurisprudence civile a tenté de regrouper les différents droits de la personnalité autour d'une division bipartite: sphère individuelle et sphère de secret (H. Hubmann, Das Persönlichtkeitsrecht, 2te veränd. und erweiterte Auflage, Böhan Verlag, Köln, Graz, 1967, p. 269; Palandt BGB, Beck'sche Kurz Kommentar, Bd 7, 44 neubearbeite Aufl., C.H. Beck'sche Verlagsbuckhandi., München, 1915, § 823 Anm. 15).

[31] H. Hubmann, *supra* note 30, pp. 83, 120, 130 et 140 précisant de façon ambiguë que le droit général de la personnalité doit être le modèle originel d'un droit subjectif. Sur la critique de cette qualification dominante dans la doctrine du continent européen, *infra*, Section 2 - Critique de la qualification dominante des droits de la personnalité: il s'agirait de droits absolus, subjectifs et non patrimoniaux.

"droit au respect de la vie privée"[32], a classé les droits de la personnalité parmi les droits subjectifs privés[33], de nature extrapatrimoniale [34].

Après quelques hésitations, la doctrine italienne s'est ralliée à l'enseignement de la Cour de Cassation en ce qui concerne l'existence du *"diritto alla rizervatezza"*[35], tout en affirmant le caractère indisponible et intransmissible des droits de la personnalité[36].

Cette conception contestée et revue[37] des droits de la personnalité n'a été que

---

[32] F. Rigaux, "La liberté de la vie privée", *supra* note 4, p. 546, n° 8 *"En France, les termes très larges de l'article 1382 du Code civil ont permis aux cours et tribunaux de tenir pour fautives les atteintes les plus graves aux biens de la personnalité. le "droit au respect de la vie privée" a été introduit sous un nouvel article 9 du Code civil par la loi n° 70-643 du 17 juillet 1970".*

[33] Qui semblent comprendre quatre subdivisions: les droits réels, les droits de créance, les droits intellectuels et les droits de la personnalité dont le droit à l'image paraît le mieux satisfaire à la définition du droit subjectif avec la maîtrise apparemment inconditionnelle reconnue au sujet sur son image; F. Rigaux, "La liberté de la vie privée", *supra* note 4, p. 558, n° 27 et s.

[34] R. Nerson, *Les droits extrapatrimoniaux*, Lyon, Bosc Frère M. et L. Riou, 1939; P. Roubier, *Droits subjectifs et situations juridiques*, Paris, Dalloz, 1963, pp. 340-353. D'aucuns ont jeté le doute sur la distinction pourtant nette entre droits patrimoniaux et droits extrapatrimoniaux (J. Ghestin et G. Goubeaux, Traité de droit civil, Introduction générale, I, 2e éd. L.G.D.J., 1983, n° 204-208, n° 286). D'autres auteurs ont reconnu aux droits de la personnalité une nature mixte (P. Kayser, *La protection de la vie privée. Protection du secret de la vie privée*, 1ère éd., Paris, Economica, Presses Universitaires d'Aix-en-Provence, 1984, p. 114; D. Acquarone, "L'ambiguïté du droit à l'image", D., 1985, Chr., 129-136, cité par F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 625, n° 561).

[35] Ou droit de se soustraire à toute intrusion de tiers, ce qui inclut le caractère illicite de la divulgation de faits privés embarrassants, l'appropriation du nom ou de l'image, les atteintes à l'honneur ou à la considération. (Cass. Scz. I civ., 27 mai 1975, n. 2629, Principessa Soraya Esfarandi, Giust. Civile, 1975, I, 1686, 1696).

[36] A. De Cupis, I diritti della personnalità, 1a ed., t. I, 1959, Milano, Giùffre, dans Trattato di diritto civile e commerciale diritto dei prof A. Cicu et F. Messineo, vol IV, 2a ed. riv. e aggiornata, 1982, p. 85, n° 29, p. 89, n° 30; Comp.: A. De Vita, Persone fisische. Commentario del codice civile, Scialoja - Branca, Libro primo, Persone e familia, art. 1-10, Zanchelli éd. Bologna, Il foro italiano, Roma, 1988, pp. 552-570.

[37] *Infra*, Section 2 - critique de la qualification dominante des droits de la personnalité: il s'agirait de droits absolus, subjectifs et non patrimoniaux.

partiellement reçue en droit québécois[38]. La jurisprudence québécoise a usé des principes du droit de la responsabilité civile[39] afin de protéger le droit à la vie privée[40].

L'effectivité de cette protection était toutefois tributaire des caractéristiques de ce mode de sanction[41] *"en sorte que seuls les cas les plus graves de violation non-intentionnelle de la vie privée [étaient] sanctionnés"*[42]. La consécration du droit au respect de la vie privée à l'article 5 de la Charte des droits et libertés de la personne[43] et l'insertion d'un

---

[38] P.A. Molinari, "Les nouveaux moyens de reproduction et les droits de la personnalité", (1986) 46 *R. de B.* 717, p. 719: *"On serait tenté d'affirmer qu'il n'existe pas, au Québec, de théorie des droits de la personnalité mais qu'il existe plutôt une variété de normes juridiques qui, si elles étaient inscrites dans une trame unique, constitueraient néanmoins un réseau de protection des attributs de la personnalité tout à fait comparable à celui qu'on peut identifier dans les états où l'importance du contentieux et le volume de la doctrine sont les indices d'une forte préoccupation pour l'exercice de ces droits"*.

[39] K. Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'informations*, Thémis, Université de Montréal, 1992, p. 19: *"Le Code civil" (...) fonde la protection du droit à la vie privée, en grande partie, sur l'action en responsabilité délictuelle (article 1053). L'injonction peut aussi constituer un moyen de prévenir ou de mettre fin à une atteinte au droit à la vie privée* [voir H.P. Glenn, "Le droit au respect de la vie privée", (1979) 39 *R. du B.* 879, p. 881] (...) Malgré tout *l'action en responsabilité nous apparaît une source déficiente du droit à la vie privée. (...) Ainsi le caractère a postériori de cette protection constitue une sérieuse lacune. De plus, il convient de se demander si cette approche peut répondre adéquatement au progrès technologique* [voir P.A. Molinari, *supra* note 38, pp. 732-733]".

[40] Entendu du droit à la solitude et à la quiétude (P.A. Molinari, *supra* note 38, p. 732), qu'il faut se garder de confondre avec le droit à l'honneur et à la réputation (H.P. Glenn, "Le droit au respect de la vie privée", *supra* note 39, p. 892.

[41] C'est-à-dire la preuve de la faute, du dommage et du lien de causalité (K. Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'informations*, *supra* note 39, p. 22).

[42] H.P. Glenn, "Le droit au respect de la vie privée", *supra* note 39, p. 894: *"Ce processus d'évaluation [du degré de violation de la vie privée] est essentiellement le même que celui de la détermination de la faute quasi-délictuelle dans d'autres cas. La nouveauté se trouve dans son application à l'égard d'un dommage plus éphémère. Etant donné le caractère purement moral du dommage; il est probable que seuls les cas les plus graves de violation non intentionnelle de la vie privée seront sanctionnés"*; Comp.: P.A. Molinari, *supra* note 38, p. 731 cité par K. Benyekhlef, La protection de la vie privée dans les échanges internationaux d'informations, *supra* note 39, p. 23.

[43] L.R.Q., c. C-12. A diverses reprises, la Cour suprême du Canada a rappelé le caractère

recours à l'article 49 indépendant de la preuve d'un dommage subi[44], paraît davantage rencontrer la spécificité de la protection de ce droit fondamental[45].

SOUS-SECTION 2 - DROIT PUBLIC.

D'abord apparue dans la doctrine des pandectistes, des germanistes et des juristes de common law[46], la protection des biens de la personnalité s'est acclimatée plus tardivement en droit constitutionnel. Elle y a joué un rôle complexe, différent selon les jurisprudences.

De l'application combinée de l'article 2, alinéa 1er (droit à l'épanouissement de la personnalité) et de l'article 1er, alinéa 1er (intangibilité de la dignité humaine) de la Loi fondamentale de 1949, la jurisprudence constitutionnelle allemande a déduit l'existence

---

fondamental de la Charte québécoise *(Commission ontarienne des droits de la personne c. Simpson - Sears Inc.*, [1985] 2 R.C.S. 536, pp. 546-547; *Winnipeg School Division n° 1 c. Craton*, [1985] 2 R.C.S. 150, p. 156; *Insurance Corporation of British columbia C. Heerspink*, [1982] 2 R.C.S. 145, p. 158; *Action travail des femmes c. Compagnie du Chemin de fer nationaux du Canada*, [1987] 1 R.C.S. 1114, pp. 1134-1137. Voir A. Ouimet, "Vers un régime universel de protection des renseignements personnels dans le secteur privé" dans *Developpements récents en droit de l'accès à l'information (1991)*, Coswanville, éd. Yvon Blais, 1991, p. 190.

[44] K. Benyekhlef, La protection de la vie privée dans les échanges internationaux d'informations, *supra* note 39, p. 24: *"le recours confère à la victime de toute atteinte illicite à un droit ou à une liberté reconnu par la charte, le droit d'obtenir la cessation de cette atteinte et la réparation du préjudice moral ou matériel qui en résulte. Dans le cadre de ce recours, le débat s'articule alors exclusivement autour de la définition et de la portée du droit à la vie privée et non plus autour de la question d'un dommage causé, par exemple"*; *Adde:* P.A. Molinari et P. Trudel, "le droit au respect de l'honneur, de la réputation et de la vie privée: Aspects fédéraux et applications" dans *Application des Chartes des droits et libertés en matière civile* (Formation permanente du Barreau), Coswanville, éd. Yvon Blais, 1988, p. 218.

[45] P.A. Molinari, *supra* note 38, p. 721: *"Les droits de la personnalité, longtemps articulés sur une problématique de droit privé (...) sont de plus en plus conçus comme appartenant au vaste champ des droits fondamentaux de la personne"*.

[46] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 611 et s., n° 546-549, n° 555-556.

d'un droit de la personnalité *(das Persönlichkeitsrecht)*[47].

A ce droit fondamental a été réservée une fonction subsidiaire: il n'est mis en oeuvre que pour protéger une liberté individuelle qui n'est pas expressément garantie par une autre disposition de la Loi fondamentale[48]. Ainsi, dans le domaine du droit public, les dispositions constitutionnelles ont protégé le citoyen contre les lois ou les mesures administratives dont l'inconstitutionnalité n'aurait pu être conservée en vertu d'une autre disposition de la Loi fondamentale[49].

Après quelques hésitations, la Cour constitutionnelle italienne a fondé sur les articles 2 et 3, alinéa 2 de la constitution républicaine l'illégitimité des lois ou mesures administratives portant atteinte à un droit fondamental dans la mesure où elles ne coïncidaient pas avec une liberté spécifique. Elle a aussi admis que la liberté d'expression était contrebalancée par le droit à l'honneur ou par le respect du à la vie privée *(riservatezza)* garantis par le même article 2[50].

---

[47] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 641, n° 574; F. Rigaux, "La liberté de la vie privée", *supra* note ..., p. 546.

[48] BverfG; 24 février 1971, *Mephisto*, BterfGE 3O, 173, 192; BverfG, 16 juin 1959, BverfGE 9, 338, 343; BverfG, 22 juin 1960, BverfGE 11, 234, 238.

[49] Par exemple, les dispositions du BGB dans les matières de droit familial ont été déclarées inconstitutionnelles, notamment parce qu'elles étaient incompatibles avec l'égalité des sexes garantie par l'article 3, alinéa 2 de la Loi fondamentale (BverfG, 18 décembre 1953, BverfGE 3, 225, 241-242; BverfG, 29 juillet 1959, BverfGE 10, 59, 67-69). De même, la disposition législative (§ 687 ZPO) ordonnant la publication officielle des décisions judiciaires d'interdiction prononcée du chef de prodigalité ou d'alcoolisme ont été jugées incompatibles avec les articles 2, alinéa 1er, et 1er, alinéa 1er de la Loi fondamentale. (BverfG, 9 mars 1988, BverfGE 78, 77) Cette décision s'appuyait sur un arrêt affirmant le droit à la libre détermination des données personnelles (BverfG, 15 décembre 1983, BverGE 65, 1, 41). Comme la protection à ce droit n'est pas illimitée, le tribunal constitutionnel a appliqué la méthode de pondération des intérêts (F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, *supra* note 4, pp. 642-644, n° 575).

[50] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 651, n° 581: *"dans son arrêt du 12 avril 1973, la cour constitutionnelle a été saisie d'un conflit entre l'exercice de la liberté d'expression (art. 21) et l'application des lois civiles protégeant*

Se prononçant sur la question de savoir si la liberté d'expression permettait une atteinte à la vie privée[51] ou sur des ingérences étatiques dans la vie privée[52], la Cour européenne des droits de l'homme a consacré le droit au respect de la vie privée protégé par l'article 8 de la Convention européenne: il implique le droit de développer des rapports sociaux, d'avoir des relations affectives et intimes avec autrui, il impose la protection de l'honneur et de la réputation et ne permet les mesures d'investigation, de contrôle et de surveillance que si elles poursuivent l'un des objectifs inscrits au deuxième alinéa de l'article 8 et à condition qu'elles ne soient pas disproportionnées par rapport à ceux-ci[53].

Aux Etats-Unis, les premières applications[54] notables d'un droit constitutionnel[55] à la

---

l'honneur, la réputation et la vie privée. Elle a décidé, en mettant en oeuvre "les droits inviolables de l'homme", auxquels appartiennent "le droit à la considération (decoro), à l'honneur, à la respectabilité, à la vie privée (riservatezza), à l'intimité et à la réputation", ces lois civiles protègent des intérêts auxquels les articles 2, 3, alinéas 2 et 13, alinéa 1er de la Constitution confèrent une valeur équivalente à celle que la liberté d'expression a reçue de l'article 21" (C. cost., 12 avril 1973, n. 38, Giurispr. cost., 1973, I, 354, 362).

51 Affaire *Lingens* (1986), Cour Eur. D.H., 8 juillet 1986, , Sér. A, No. 103, p. 11; Affaire *Barford* (1989), Cour Eur.D.H., Sér. A, No 149, p. 12; pour plus de développements, voir F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 259, n° 190 et p. 269, n° 197.

52 Affaire *Klass et autres* (1978), Cour Eur.D.H., Sér. A, No 28, p. 17; Affaire *Malone* (1984), Cour Eur.D.H., Sér. A, No 82, p. 6; Affaire *Kruslin et Huvig* (1990), Cour Eur. D.H.,Sér. A., No 1; pour plus de développements, voir F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 196 et s., n° 132-138.

53 P. Martens, "La vie privée est-elle soluble dans l'éther?" dans C. Doutrelepont, P. Van Binst et L. Wilkin, dir., *Libertés, droits et réseaux dans la société de l'information*, Bruxelles, Bruylant, 1996, p. 183; J. Velu et R. Ergec, "Convention européenne des droits de l'homme, R.P.D.B., compl. t. VII, n° 656.

54 L'un des plus anciens arrêts de la Cour suprême ayant évoqué la notion de privacy est relatif à l'application du IVe amendement de la Constitution américaine par lequel la Cour déclare inconstitutionnelle la loi imposant à un commerçant la production de ses livres comptables *(Boyd. v. United States*, 116 U.S. 616 (1986)). La Cour suprême a maintenu une interprétation exégétique du IVe amendement jusqu'en 1967, date à laquelle elle a reconnu une protection constitutionnelle au secret des communications téléphoniques *(Berger v. New York*, 338 U.S. 41 (1967); *Katz v. United States*, 389 U.S. 347 (1967)). Les applications les plus spectaculaires de

privacy ont pour objet l'ingérence étatique dans des sphères d'intimité qui sont d'une part la liberté de faire des choix existentiels dans les domaines qui relèvent de la privacy et, d'autre part, le droit au secret, auxquels la Cour suprême a reconnu une protection constitutionnelle[56].

De même, la Cour suprême du Canada a reconnu une protection constitutionnelle[57] à

---

la notion de privacy restent celles de la constitutionnalité d'une loi d'Etat réprimant la distribution de produits contraceptifs (*Griswold v. Connecticut*, 381 U.S. 484 (1965); *Eisenstadt v. Baird*, 405 U.S. 438 (1972)) ou réprimant pénalement l'avortement (*Roe v. Wade*, 410 U.S. 113 (1973)); pour plus de développements, voir F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 191 et s., n° 129 et s., p. 167 et s., n° 113 et s., p. 644 et s., n° 576 et s.; K. Benyekhlef, La protection de la vie privée dans les échanges internationaux d'informations, *supra* note 39, p. 31 et s.; Laurence H. Tribe, *American Constitutional Law*, 2e éd., Mineola, New York, Foundation Press, 1988, pp. 1302-1435.

[55] Le Bill of Rights américain ne contient pas de mention expresse d'un droit au respect de la vie privée. Toutefois, dans une série de décisions, la Cour suprême a reconnu qu'un droit au respect de la vie privée ou la garantie de certaines zones d'intimité existent en vertu de la Constitution; voir F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 169, n° 114.

[56] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 648, n° 579: *"la Cour suprême n'a guère eu de peine à qualifier le privacy de droit fondamental, émanation des pénombres (...) ou, si l'on préfère, de l'esprit de la Constitution"*. Ce droit fondamental se dégage de l'ensemble constitutionnel du Bill of Rights dont il serait erroné de prétendre qu'il ne protège que les droits qui y sont spécifiquement énoncés (Juge Goldberg, *Griswold v. Connecticut*, 381 U.S. 484 (1965)).

[57] Contrairement à l'article 5 de la Charte québécoise des droits et libertés de la personne, la Charte canadienne des droits et libertés (L.R.Q., 1977, c. C-12) ne contient aucun énoncé explicite sur le droit au respect de la vie privée. Toutefois, la Cour suprême a posé le principe de l'interprétation des dispositions de la Charte, notamment de l'article 8, en fonction des objectifs plus larges de ce document constitutionnel (Juge Dickson, *Hunter c. Southam*, [1982] 2 R.C.S. 145, pp. 159-160: *"A l'instar de la Cour suprême des Etats-Unis, j'hésiterais à exclure la possibilité que le droit à la protection contre les fouilles, les perquisitions et les saisies abusives protège d'autres droits que le droit à la vie privée (...). Cette limitation du droit garanti par l'article 8, qu'elle soit exprimée sous la forme négative, c'est à dire comme une protection contre les fouilles, les perquisitions et les saisies "abusives", ou sous la forme positive comme le droit de s'attendre "raisonnablement" à la protection de la vie privée, indique qu'il faut apprécier si, dans une situation donnée, le droit du public de ne pas être importuné par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins, et notamment, d'assurer l'application de la loi"*; Juge La Forest, *La Reine c. Dyment*, [1988] 2 R.C.S. 417, p. 426: *"Le point de vue qui précède est tout à fait approprié dans le cas d'un document constitutionnel enchassé à une époque où (...) la société a fini par se*

l'immixtion de l'Etat[58] dans des zones d'intimité ainsi qu'un droit à la vie privée informationnelle[59]. En outre, certaines dispositions législatives protègent, de façon

---

rendre compte que la notion de vie privée est au coeur de celle de la liberté dans un Etat moderne.(...). Fondée sur l'autonomie morale et physique de la personne, la notion de vie privée est essentielle à son bien-être. Ne serait-ce que pour cette raison, elle mériterait une protection constitutionnelle mais elle revêt aussi une importance capitale sur le plan de l'ordre public. L'interdiction qui est faite au gouvernement de s'intéresser de trop près à la vie des citoyens touche à l'essence même de l'Etat démocratique"; D. Johnston, D. Johnston et S. Handa, *supra* note 19, p. 196: *"section 8 is frequently used to ensure that law enforcement officers take the proper steps prior to searching a person and his belongings. Without the requisite authority, such as during an arrest or with a search warrant, the police must respect an individual's right to privacy"*; voir D.H. Flaherty, *Protecting Privacy in Two-way Electronic Services*, White Plains New York, Knowledge Industry Publications, 1984.

[58] K. Benyekhlef, La protection de la vie privée dans les échanges internationaux d'informations, *supra* note 39, pp. 29 et 30: *"En dehors du cas patent de la non application de [l']article [8] aux relations purement privées, nous croyons que la phraséologie, utilisée par le constituant restreint le champ de l'article 8, malgré l'amplitude conférée par une interprétation téléologique, à des cas où il y a intrusion effective de la puissance publique. Ainsi, (...) nous voyons mal comment cet article pourrait établir, de manière effective, des règles en ce qui concerne la cueillette, le traitement et la gestion des données personnelles dans le cadre d'un programme gouvernemental quelconque, par exemple. Et ce, bien que la Cour suprême ait reconnu clairement que le droit à la vie privée, énoncé à l'article 8, comportait une facette informationnelle (...). Nous croyons, à cet égard, que seule la loi peut aménager un droit réel et effectif à la vie privée informationnelle. (...) La protection effective du droit à la vie privée informationnelle ne saurait se satisfaire d'un énoncé général de la nature de l'article 8. La complexité du traitement informatisé de l'information nécessite l'élaboration de règles spécifiques, claires et sûres à laquelle ne saurait aspirer une disposition de nature constitutionnelle, particulièrement au regard de l'évolution technologique qui caractérise ce domaine. Les délais qui accompagnent le développement jurisprudentiel d'une règle de droit, de même que les incertitudes qui entourent celles-ci, ne peuvent que nous convaincre des insuffisances d'une solution exclusivement constitutionnelle"*.

[59] Juge La Forest, *La Reine c. Dyment*, [1988] 2 R.C.S., 417, pp. 429-430: *"Enfin il y a le droit à la vie privée en matière d'information. Cet aspect aussi est fondé sur la notion de dignité et d'intégrité de la personne. Comme l'affirme le groupe d'étude (...): "Cette conception de la vie privée découle du postulat selon lequel l'information de caractère personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il l'entend". Dans la société contemporaine tout spécialement, la conservation de renseignements à notre sujet revêt une importance accrue. Il peut arriver, pour une raison ou pour une autre, que nous voulions divulguer ces renseignements ou que nous soyons forcés de le faire, mais les cas abondent où on se doit de protéger les attentes raisonnables de l'individu que ces renseignements seront gardés confidentiellement par ceux à qui ils sont divulgués, et qu'ils ne seront utilisés que pour les fins pour lesquelles ils ont été divulgués. Tous les paliers du gouvernement ont, ces dernières années, reconnu cela et ont reconnu des règles et des règlements en vue de restreindre l'utilisation des données qu'ils recueillent à celle pour laquelle ils le font (...)"*. K. Benyekhlef, La protection de la vie privée dans les échanges internationaux d'informations, *supra* note 39, p. 30: *"[Ces] énoncés de la Cour suprême peuvent [également] servir à l'interprète dans l'appréhension du droit à la vie privée informationnelle dans le contexte de la Charte québécoise"*.

parcellaire, les atteintes étatiques à la vie privée[60] ou *"l'utilisation d'informations obtenues d'une personne à l'occasion de l'exercice d'un pouvoir de la puissance publique"*[61].

Au regard du droit constitutionnel qui régit les relations entre les citoyens et l'administration, le droit de la personnalité ou droit à l'autodétermination et le right of privacy sont des libertés dont la violation par l'administration ouvre au sujet un droit d'action devant les tribunaux constitutionnels[62].

SECTION 2 - CRITIQUE DE LA QUALIFICATION DOMINANTE[63] DES DROITS DE LA PERSONNALITE: IL S'AGIRAIT DE DROITS ABSOLUS, SUBJECTIFS ET NON PATRIMONIAUX

SOUS-SECTION 1 - LE CARACTERE ABSOLU DES DROITS DE LA PERSONNALITE.

---

[60] Ainsi, les articles 175, 177, 181 et 184 (1) du Code criminel ou l'article 6 de la Loi sur le télégraphe ou 17 de la Loi sur les compagnies de télégraphe et de téléphone; sur la jurisprudence (*R.c. Kirby*, [1970] 1 C.C.C. (2e) 286 (C.A. Qué.); *R.c. Zundel*, [1987] 31 C.C.C. (3e) 97 (C.A. Ont.)), voir K. Benyeklehef, *La protection de la vie privée dans les échanges internationaux*, *supra* note 39, p. 25.

[61] P.A. Molinari, *supra* note 38 p. 736.

[62] Ainsi, au Canada, le Juge Wilson indiquait *"je conclus donc que le droit à la liberté énoncé à l'article 7 [de la Charte canadienne] garantit à chaque individu une marge d'autonomie personnelle sur ses décisions importantes touchant intimement à sa vie privée"* (*Morgentaler c. La Reine*, [1988] 1 R.C.S. 30, p. 171); F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 641, n° 574: *"C'est de manière beaucoup plus discrète que le Bundesverfassungsgericht a parfois déduit du droit à l'épanouissement de la personnalité un devoir positif mis à charge de l'Etat"*; celui de *"respecter la dignité humaine et contribuer à l'épanouissement de chaque personnalité individuelle ou, à tout le moins, ne pas s'y immiscer de façon illicite ou excessive"*; *ibid*, p. 650, n° 580: *"La conception selon laquelle la privacy est une liberté à diverses conséquences que la Cour suprême [des Etats-Unis] n'a pas toujours aperçues. La motivation de Bowers v. Hardwik, 478 U.S. 186 (1980), fait clairement apparaître que (...) la Cour s'est laissée déviée du concept de liberté vers celui de droit subjectif"*.

[63] Dans les doctrines du continent européen.

Les théoriciens des droits de la personnalité enseignent généralement que ces droits sont absolus, c'est-à-dire, à l'instar des droits réels, opposables à tous[64].

L'analogie ainsi établie entre les droits de la personnalité et les droits réels est peu appropriée en raison de leur objet distinct. Si les droits réels ont pour objet un bien du monde physique sur lequel le sujet exerce son droit de propriété dont l'assiette est ainsi déterminée à l'égard des tiers, les droits de la personnalité ont pour objet le corps du sujet ainsi que ainsi que les éléments non corporels tels ses affections, ses pensées, son patrimoine, etc.[65] qui présentent un caractère diffus ne permettant pas aux tiers de savoir précisément ce qu'ils doivent respecter, ce qui sera déterminé dans les cas limites par les tribunaux[66].

La protection relative et circonstancielle des droits de la personnalité est donc très éloignée de la protection rigide qui s'attache à la maîtrise des droits réels restrictivement énumérés par la loi, ou des droits de créance[67] qui ont un objet

---

[64] A la différence des droits de créance qui ont pour seul destinataire le débiteur; J. Carbonnier, Droit civil, I. Introduction. Les personnes, 16e éd., P.U.F., Coll. Thémis, 1987, p. 363, n° 70; A. Bucher, Personnes physiques et protection de la personnalité, éd. Helbing et Lichtenhahm, Bâle et Frankfurt a/M, 1985, p. 131; J.M. Grossen, "La protection de la personnalité en droit privé (quelques problèmes actuels)", (1960) 79 Revue de droit suisse, 2 p. 9a; P. Tercier, *Le nouveau droit de la personnalité*, Schlulthess, Zurich, 1984, p. 131; A. De Cupis, *supra* note 36, n° 20; *Contra*: C. Neuner, *Wesen und Arten der Privatrechsverhältnisse*, Kiel, Schwers'sche Buchhandlung, 1866, p. 14.

[65] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 730, n° 656: *"La maîtrise exercée par le sujet sur son corps et sur ses activités créatrices ou intellectuelles n'est pas un droit mais une liberté. Il n'entre dans l'espace des rapports juridiques que par l'effet d'une agression ultérieure"*.

[66] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 731, n° 656: *"La notion de droit absolu paraît ici singulièrement impropre. Pareille objection est d'autant plus décisive que la doctrine contemporaine réduit la multiplicité des droits de la personnalité à un droit subjectif unique, totalement indéterminé, tels le droit général de la personnalité ou le droit au respect de la vie privée"*; *Adde:* W. Rotelmann, "Persönlichkeirechte, inbesondere der widerruf ehrenrühriger Behauptungen", (1971) N.J.W. 1637.

[67] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p.

immatériel, une obligation de faire, de ne pas faire ou de donner, dont le contenu est lui aussi rigoureusement délimité[68] ou des droits intellectuels confiant eux aussi à leurs titulaires des prérogatives limitativement énoncées par la norme qui les institue[69].

SOUS-SECTION 2 - LE CARACTERE NON PATRIMONIAL DES DROITS DE LA PERSONNALITE.

Selon la doctrine civiliste, les droits de la personnalité seraient, à la différence des droits réels et des droits de créance, de nature extrapatrimoniale, c'est-à-dire inaliénables et intransmissibles.

Cette conception, née de la confusion entre le droit général de la personnalité que constitue la maîtrise préjuridique du sujet sur son corps et sur ses activités créatrices, intellectuelles ou patrimoniales, et son insertion dans un rapport juridique à l'occasion d'une relation particulière que noue le sujet avec un autre sujet de droit, est aujourd'hui dépassée.

Si cette maîtrise préjuridique est hors commerce, indisponible[70], rien n'empêche à un sujet, sauf l'ordonnancement normatif, l'ordre public et les bonnes moeurs, de disposer d'un attribut de la personnalité et de l'insérer dans un rapport juridiquement protégé, tel

---

731, n° 656: *"la méthode de pondération des intérêts est aussi éloignée que possible du schéma apparemment rigoureux auquel la notion de droit absolu donne une illusoire solidité"*.

[68] Seul *"(un) objet certain"* peut former *"la matière de l'engagement"* (article 1108 du Code civil).

[69] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 742, n° 668.

[70] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 732, n° 657: *"ni plus ni moins que les autres libertés publiques ni même que "le" patrimoine au sens qu'Aubry et Rau avaient donné à cette notion [le patrimoine, élément de la personnalité du sujet est inaliénable, les actes de disposition ne frappant jamais que des biens et non le sujet toujours patrimonial]"*.

le droit des contrats[71]. L'on rejoint ici la distinction opérée par la doctrine et la jurisprudence américaine[72] entre *"le right of privacy"*, de nature extrapatrimoniale, et le *"right of publicity"*, objet d'une exploitation économique non réductible au droit d'auteur[73].

La commercialisation des droits de la personnalité par les tiers à laquelle s'expose le sujet pose également de délicates questions quant aux atteintes à un intérêt protégé par le droit positif[74].

---

[71] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 733, n° 658: *"ainsi, l'objet du contrat n'est pas, directement, un attribut du droit de la personnalité, conçu comme une parcelle de la maitrise exercée par le sujet lui-même, mais un élément rendu négociable par la spécification qu'il reçoit de la relation particulière dans laquelle il se trouve inséré (...). En outre, un droit de repentir ou de retrait, analogue à celui que connaît le droit d'auteur et exercé de manière discrétionnaire sous réserve de la réparation des dommages contractuels, suffit à permettre la réintégration dans la sphère privée (exclusive de tout rapport intersubjectif) des attributs personnels ayant fait l'objet du contrat"*.

[72] F. Rigaux, "La liberté de la vie privée", *supra* note 4, p. 547, n° 8; sur les autres principales causes de l'accession des biens de la personnalité à la qualité de biens juridiques, voir F. Rigaux "La liberté de la vie privée", *ibid.*

[73] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 734, n° 658: *"si la création non volontairement divulguée est aujourd'hui intégrée au droit d'auteur, n'est-ce pas parce qu'elle est perçue comme droit patrimonial en attente?"*. En ce sens, les droits intellectuels, qui sont des droits exclusifs d'exploitation économique dont le droit moral de l'auteur intervient ultérieurement, s'opposent aux droits de la personnalité, de caractère expatrimoniaux, qui peuvent cependant faire ultérieurement l'objet d'une exploitation patrimoniale.

[74] Voir à ce sujet, Rapport du Groupe de travail sur la commercialisation des banques de données des organismes publics, Ministère des Communication du Québec, Québec, 1991; Y. Poullet et Ph. Gérard, "Pour un cadre juridique de la diffusion des produits informationnels juridiques", (1994) D.A.O.R., pp. 39-52; Y. Poullet, "La commercialisation des données par le secteur public et vie privée", (1994) Droit de la Consommation, p. 68 et s.; C. de Terwangne et Th. De La Croix-Davio, "L'accès à l'information administrative et la commercialisation des données publiques", C.R.I.D., Namur, 1994, pp. 105-118.

SOUS-SECTION 3 - LE CARACTERE SUBJECTIF DES DROITS DE LA PERSONNALITE

Comme on l'a observé[75], contrairement à une opinion qui a longtemps fait autorité aux Etats-Unis, le right to privacy n'est pas le *droit* d'être laissé seul (the right to be let alone), il s'agit plus exactement de la *liberté* de conduire ses relations avec autrui sans être exposé à une immixtion illicite de l'Etat dans cette relation et sans qu'un autre agent privé s'approprie la sphère privée des personnes qui y participent[76]. Le Tribunal constitutionnel fédéral allemand a tenu le droit de la personnalité, qui inclut notamment les attributs de la vie privée, pour un droit à l'autodétermination[77], c'est-à-dire pour une liberté, encore indéterminée.

De la même manière que la liberté de l'individu ne pénètre dans le champ du droit que si elle est atteinte par un organe de l'Etat[78] ou par un autre agent juridique privé, les biens de la personnalité *"ne se transforment en biens juridiques que par l'établissement d'une relation intersubjective apte à être qualifiée de rapport juridique"*[79]. La liberté ne

---

[75] F. Rigaux, "la protection de la vie privée à l'égard des données à caractère personnel", Ann. dr. Louvain, 1993, p. 53, n° 6.

[76] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 735, n° 660: *"A cet égard, l'hésitation terminologique de la Cour suprême des Etats-Unis est très significative: ce sont des libertés qui protègent le citoyen contre l'administration et la substitution récente de la notion de privacy à celle de liberty a eu pour principal effet d'oblitérer la différence entre un concept de droit constitutionnel et une notion de droit civil"*.

[77] Bverf, 15 décembre 1983, Volkszählengsgesetz, BverfGE, 65, 1, 41; F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 736, n° 662: *"A la vérité, le mot "droit" ne désigne pas ici un droit subjectif mais une liberté: l'originalité de celle-ci est de trouver en elle-même l'objet de sa propre spécification. Rien d'extérieur à elle ne la détermine, l'ordre juridique objectif se bornant à lui imposer des limites sans la prédéterminer"*; Comp.: P. Kayser, *supra* note 34, 2e éd, 1990, n° 1: *"Il n'est pas moins important de protéger les personnes contre les atteintes à la liberté de leur vie privée"*.

[78] Protégés par les libertés constitutionnelles.

[79] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p.

donne ainsi naissance à un droit subjectif[80] que par la médiation d'une norme objective *"qui ne saurait saisir le sujet que sorti de sa solitude"*[81].

Si les attributs de la personnalité ne sont pas comme tels l'objet d'un rapport juridique ni d'un droit subjectif, en revanche l'insertion des biens de la personnalité dans une relation à autrui est de nature à conférer au sujet une certaine protection juridique. Cependant, tant que ces attributs ne constituent que des *"intérêts légitimes protégés par une action en justice"*[82], il n'existe pas de protection prenant la forme d'un droit subjectif de cet intérêt lésé, encore indéterminé[83]. Comme on l'a souligné[84], pas plus que *"le"* droit réel, *"le"* droit de créance ou *"le"* droit intellectuel, *"le"* droit de la

---

739, n° 663 et 664.

[80] Ou un *"interest"* au sens de la common law; le droit subjectif est une prérogative, concédée à une personne par le droit objectif et garantie par des voies de droit, de disposer en maitre d'un bien qui est reconnu lui appartenir, soit comme le sien, soit comme dû (J. Dabin, Le droit subjectif, Paris, Dalloz, 1952, p. 103); F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 740, n° 665: *"la qualification du right to privacy ne saurait susciter des difficultés semblables pour les juristes de Common law. En effet, cette expression ne donne pas à la privacy la protection magique d'un droit subjectif. Dans la matière de la privacy, les tribunaux américains parlent plus volontiers de "privacy interest" ou de "liberty interest" que de "privacy right";*. Voir notamment Geoffrey Samuel "Le droit subjectif" and English Law", (1987) 46 *Cambridge L.J.*, 264-286.

[81] F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, *supra* note ...., *ibid.*

[82] P. Roubier, *supra* note 34, *ibid.*

[83] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 742, n° 668: *"Les biens de la personnalité ne présentent pas la précision requise pour qu'en émane l'objet d'un droit subjectif. A tout prendre, seul le droit à l'intégrité corporelle pourrait satisfaire à cette condition, la relation qui s'établit entre le corps du sujet et ceux qui seraient en mesure d'y porter atteinte imposant un devoir d'abstention impérieux. Ce ne sont toutefois pas les atteintes à l'élément physique qui ont donné naissance à la transformation des droits de la personnalité en droit subjectifs: la protection traditionnelle assurée à l'intégrité physique par le droit pénal et par le droit à la responsabilité civile rendait superflue une telle ingénuosité";* sur le caractère inadéquat de la doctrine des droits subjectifs à l'exercice d'un droit de la personnalité particulier, tel le droit à l'image ou le secret des lettres missives, voir *ibid.* n° 699-670.

[84] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 746, n° 672.

personnalité ne saurait être tenu pour un droit subjectif unique. La même critique doit être adressée à la prétendue reconnaissance par la jurisprudence française *"d'un droit subjectif, de portée générale, au respect de la vie privée"*[85].

SECTION 3 - DEFINITION DE LA VIE PRIVEE

Comme on l'a souligné[86], face à l'incapacité de définir les notions fondamentales (personnalité, vie privée), deux voies ont été suivies. La première a consisté à distinguer dans ces concepts des sous-catégories. Telle a été pour l'essentiel la voie suivie par la doctrine et la jurisprudence américaine à la suite de Prosser[87]. La reconnaissance d'un droit général de la personnalité par la jurisprudence européenne est également suivie par la doctrine d'une énumération des droits de la personnalité particuliers, mettant ainsi en oeuvre la même méthode.

Une autre voie a consisté à rechercher le *"noyau dur"* de la personnalité à partir de la méthode de pondération des intérêts utilisée par la jurisprudence allemande[88] et française, ce qui s'est révélé largement insatisfaisant. Tandis que la doctrine allemande regroupait les différents droits de la personnalité[89] autour d'une division bipartite: sphère individuelle (*Individualsphäre)* et sphère de secret *(Geheimsphäre)*[90], la doctrine

---

[85] Pierre Kayser, *supra* note 34, p. 69.

[86] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 725, n° 649 et s.

[87] *Supra*, Section 1. source du droit à la vie privée.

[88] *Supra*, Section 1. source du droit à la vie privée. (La doctrine allemande postérieure à la seconde guerre mondiale).

[89] Limités aux éléments *"spirituels"*, affectifs, créateurs ou moraux de la personnalité; pour plus de développements, voir F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, *supra* note 4, pp. 726-729, n° 650-654; pp. 719-721, n° 643-645.

[90] H. Hubmann, *supra* note 30, p. 269; Palandt BGB, Beck'sche Kurz Kommentar, Bd 7, 44

française considérait que l'intimité de la vie privée[91] constituait le *"noyau dur"* de la vie privée, ayant notamment pour objet la vie affective et sexuelle, la santé, les opinions religieuses et politiques.

De ces éléments qui semblent correspondre aux *"données sensibles"* dans les législations de protection du traitement des données à caractère personnel, on peut distinguer deux catégories, l'une portant sur le corps du sujet (santé, relations familiales, affectives) et qui pourrait être rattachée au droit d'être laissé seul, l'autre en relation avec les libertés constitutionnelles (protection du sujet contre le risque de discrimination en raison de ses opinions) et qui pourrait être rattachée à la distinction vie privée et vie publique[92]. Qu'on définisse la vie privée par opposition à la vie publique[93] ou qu'elle désigne ce qui est protégé par le secret[94] conduit à une impasse[95].

---

neubearbeitite Aufl., C.H. Beck'sche Verlagsbuchhande., München, 1985, § 823, Anm. 15.

[91] En droit positif français, le concept de vie privée couvre trois catégories de situation: l'atteinte à la vie privée (article 9, alinéa 1er du Code Civil), l'atteinte à l'intimité de la vie privée (article 9, alinéa 2 du Code civil) et l'atteinte qui fait l'objet d'une incrimination pénale (article 368 et 369 du Code Pénal); pour plus de développements, voir F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 718 et s., n° 740 et s.

[92] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 719, n° 642.

[93] A. Roux, *La protection de la vie privée dans les rapports entre l'Etat et les particuliers*, Paris, Economica, 1983, p. 8: *"(...) la vie privée est cette partie de la vie qui n'est pas consacrée à une activité publique et où les tiers n'ont en principe pas accès, afin d'assurer à la personne le secret et la tranquillité auxquels elle a droit"*.

[94] J. Ravanas, *La protection des personnes contre la réalisation et la publication de leur image*, Paris, L.G.D.J., 1978, p. 135: *"la vie privée est pour l'individu une sphère secrète de la vie où il a le pouvoir d'écarter les tiers"*; R.B. Parker, "A Definition of Privacy", (1973-74) 27 Rutgers L.R. 275, p. 281; T. Gerety, "Redefining Privacy", (1977) 12 Harvard Civil Rights-Civil Liberties L.R. 233, p. 267; A.F. Westin, "Science, Privacy and Freedom: Issues and Proposals for the 1970's", (1996) 66 Col. L.R. 1003, pp. 1020-1021 qui identifie quatre composantes à la vie privée: la solitude permettant à l'homme de réfléchir; l'intimité pour le développement de relations familiales et affectives; l'anonymat permettant à l'homme d'exister en dehors de toute identification, et la réserve permettant la retenue d'informations le concernant; H.P. Glenn, "Le droit au respect de la vie privée", *supra* note 39, pp. 884 et 881: *"Le droit au respect de la vie privée est protecteur d'un intérêt distinct de celui de la jouissance des choses matérielles. Il s'agit d'un intérêt qui ne peut être défini qu'en fonction de la solitude*

La limite de cette conceptualisation de la vie privée ainsi que la multiplicité des approches définitionnelles[96] démontre qu'il est impossible - et, au surplus, inutile - de définir la vie privée, notion essentiellement protéiforme[97], dont il appartiendra ultimement aux tribunaux d'en circonscrire l'étendue[98].

---

de l'individu, et cette notion de solitude doit signifier une sorte d'intégrité mentale ou spirituelle, une condition dans laquelle l'individu est libre de toute entrave injustifiable à son état d'esprit. Bien que ce droit de solitude coexiste souvent avec un droit à l'isolement physique (...) le droit existe aussi dans l'absence de tout droit à l'isolement physique"; ce droit constitutif de la vie privée, la solitude, ainsi que l'anonymat ont été reconnus par les tribunaux qui ont condamné deux comportements y portant atteinte: *"Le [premier] c'est l'intrusion injustifiable qui a comme effet de porter un renseignement personnel à la connaissance de l'intrus ou tout simplement de gêner la victime. C'est la solitude de l'individu qui semble atteinte par cette intrusion, une condition de séparation des autres membres de la société, ou de la plupart des autres membres de la société. En deuxième lieu, et encore en l'absence de faits justificatifs, il y a atteinte à la vie privée qui provient de la diffusion de renseignements ou d'images. En ce cas, la prohibition de l'acte de diffusion protège l'anonymat de la personne, une situation qui est celle de ne pas être identifiable"*. Comp.: F. Rigaux, "La liberté de la vie privée", *supra* note 4, pp. 548-556, n° 10-19. Voir également la définition de H. Gross, "Privacy and Autonomy", dans *Nomos XIII, Privacy*, éd. J. Chapman et J. R. Pennock, New York: Lieber-Atherton, 1971, pp. 169-182, cité par D. Johnston, D. Johnston et S. Handa, *supra* note 19, p. 191.

[95] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 724, n° 647: *"L'intimité du sujet n'intéresse les tiers qu'en raison de ses activités extérieures (professionnelles, politiques) et, presque toujours, dans la mesure où elle est en relation avec pareilles activités. Quant au secret, il protège nombre de biens autres que ceux d'une prétendue vie privée, le droit au secret ayant une portée beaucoup plus étendue que la protection des biens qu'il serait possible d'enfermer à l'intérieur du "mur de la vie privée""*.

[96] Pour plus de développements, voir K. Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'informations*, *supra* note 39., pp. 38-49. P. Mackay, P. Péladeau et R. Laperrière, *Droit, informatique et vie privée: bibliographie sélective, canadienne et internationale*, Montréal, SOQUIJ, 1986; A. Vitalis, *Informatique, pouvoirs et libertés*, Paris, Economica, 1988; H. Maisl et A. Vitalis, *Les libertés, enjeu d'une société informatisée* (Etudes, avril 1985), 472; H.D. Flaherty, *Protecting Privacy in Two-way Electronic Service*, *supra* note 57, *ibid.*

[97] F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, *supra* note 4, p. 725, n° 648.

[98] Qui variera selon l'intérêt public ou privé avec lequel il entre en conflit.

SECTION 4 - LE DROIT A LA VIE PRIVEE INFORMATIONNELLE

L'aspect informationnel que représentent la collecte, le traitement et la communication des données personnelles par les institutions publiques, les organismes ou groupements privés à des fins multiples, constitue la pierre angulaire du droit de la vie privée[99]. Selon d'aucuns[100], l'information constitue un bien (*"commodity"*) susceptible d'appropriation. Le sujet des données (*"data subject"*) peut donc exercer un droit de propriété sur l'information qui le concerne[101].

---

[99] Qui s'entend ici de la maîtrise par l'individu de l'information qui circule à son propos, de la maîtrise de son *"image informationnelle"*; A.F. Westin, *Privacy and Freedom*, *supra* note 8, p. 7: *"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others"*; A. Miller, *supra* note 16, p. 25. Le Comité consultatif sur l'autoroute de l'information a défini la privacy de deux manières: "the right to be left alone, free from intrusion or interruption, and the right to exercise control over one's personal information (Information Highway Advisory Council, *Privacy and the Canadian Information Highway*, Ottawa: Industry Canada, 1994, p. 5, cité par D. Johnston, D. Johnston et S. Handa, *supra* note 19, p. 192).

[100] M. Rankin, *supra* note 16, p. 326: *"The claim of informational privacy assumes that all information about an individual is fundamentally the property of that individual: for him to communicate or withhold as he determines"*; A.F. Westin, *Privacy and Freedom*, *supra* note 8, pp. 324-325: *"First personal information, thought of as the right of decision over one's private personality, should be defined as a property right, with all the restraints on interference by public or private authorities on due-process garantees that our law of property has been so skillful in devising"*; R.A. Reiter, "The Legal Protection of Personal Information in the Context of Videotext: A Preliminary Inquiry", (1986) 2 Intel. Prop. J. 273, p. 291: *"If personal information could be defined as property, the owner (usually the subject of the information) could control the use of such knowledge"*; C. Reich, "The New Property", (1964) 73 Yale L.J. 733; P. Leclercq, "Essai sur le statut juridique des informations" dans A. Madec, *Les flux transfontières de données: vers une économie internationale de l'information?*, Paris, La Documentation française, 1982, p. 124: *"Est un bien toute valeur bénéficiant de l'opposabilité absolue"*. Or, on ne peut refuser de reconnaître *"l'existence de principe de la valeur de l'information"*.

[101] A. Miller, *Privacy and Freedom*, supra note 16, pp. 211-212; A.S. Weinrib, "Information and Property", (1988) 38 U.T.L.J. 117; Comp. Juge Lamer *Stewart c. La Reine*, [1988] 1 R.C.S. 963: *"Quant à moi, je crois qu'étant donné les progrès technologiques récents, les renseignements confidentiels, et en fait toute information ayant une valeur commerciale, ont besoin d'une certaine protection en vertu de notre droit criminel"*.

Nombre d'auteurs ont rejeté ou nuancé cette conception propriétaire (ou théorie des biens informationnels) en ce qu'elle ne constitue pas un mode approprié de protection de la vie privée[102], ou la base sur laquelle la personne revendique la maîtrise des informations la concernant[103] (droit d'*habeas data* ou *habea scriptum)*[104], en ce qu'elle

---

[102] A. Miller, *Privacy and Freedom*, supra note 16, p. 212: *"The objective of protecting individual privacy is to safeguard emotional and psychological tranquility by remedying an injurious dissemination of personal information; it never was intended to serve as a vehicle for defiming. The legal title to information or as a method for determining who has the right to control its commercial exploitation - typical functions of the law of property"*; Warren et Brandeis ont également réfuté cette théorie qui présente une idée, un sentiment, une réflexion ou une qualification comme un bien patrimonial susceptible d'être approprié (K. Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'informations*, *supra* note 39, p. 52); H.P. Glenn, "Le droit au respect de la vie privée", *supra* note 39, pp. 888-889 qui estime que la reconnaissance des notions de solitude et d'anonymat en tant qu'intérêts protégés par le droit à la vie privée *"(...) permet le rejet de l'affirmation fréquente que le droit [à la vie privée] n'est rien d'autre qu'un droit de propriété"* qui se caractérise par la valeur patrimoniale qui y est attachée. Or, la solitude ou l'anonymat n'ont souvent aucune valeur patrimoniale, ce qui a pour conséquence de les exclure du champ propriétaire. *"Ainsi, le droit au respect de la vie privée ne peut pas être un simple droit de propriété, bien que les droit de propriété puissent fournir une protection subsidiaire de la vie privée, dans la mesure qu'ils permettent la jouissance exclusive d'une chose corporelle ou incorporelle"*.

[103] A. Lucas, *Le droit de l'informatique*, Paris, P.U.F, 1987, p. 353: *"Celle-ci est fondée sur le postulat de la valeur patrimoniale de l'information. Or, si la personne concernée revendique une certaine maîtrise sur des informations la concernant, ce n'est pas en invoquant leur valeur patrimoniale mais en faisant valoir un droit de la personnalité"*; K. Benyekhlef, La protection de la vie privée dans les échanges internationaux d'informations, *supra* note 39, p. 52: *Lucas croit d'ailleurs que la polémique (...) est compliquée par l'utilisation du mot "information" pour désigner des réalités très différentes. Ainsi, en ce qui touche les informations non nominatives, l'auteur remarque que le terme "information", dans le cadre de cette théorie, recouvre des réalités trop diverses et est, par conséquent, trop large. Il faut donc éviter d'attribuer un droit privatif à l'information (...). Il serait plus logique et plus conforme aux traditions juridiques et au bon sens de protéger non pas l'information (...) mais l'exercice ou l'effort menant à une création informationnelle"*.

[104] Il s'agit de *"l'exercice pour le particulier de son nouveau droit positif de la personnalité (...) de vérifier le contenu des informations tenues par le système à son égard et d'exiger la rectification de son dossier. Le droit d'habeas data réintroduit dans les systèmes de communication la notion du consentement individuel comme justification pour le contrôle et la circulation de données personnelles. Si le droit est exercé, le consentement est explicite; si le droit n'est pas exercé, ce qui est généralement le cas, le consentement est implicite"*. (H.P. Glenn, "Les nouveaux moyens de reproduction audio-visuelle et numérique et les droits de la personnalité: Rapport général", *supra* note 5, p. 708, 710 et 711); H.P. Glenn, "Le droit en l'an 2000: L'envahissement des contrôles gouvernementaux et des technologies nouvelles dans la vie privée des citoyens, (1987) R.G.D. 705, p. 711: *"Dans la mesure où ces pratiques de circulation de données restent*

affecte la libre circulation de l'information[105] et impose du titulaire de l'information d'assurer seul le respect de son droit[106]. Plutôt que sous l'angle propriétaire, insatisfaisant[107], le droit à la vie privée informationnelle doit s'envisager comme une

---

occultes, il y a bien sûr lieu de les rendre plus transparentes par le moyen de l'habeas data, et ce moyen peut-être même renforcé. (...) L'habeas data nous permet de savoir si les décisions sont prises à notre égard sur la base de données erronées et d'agir en justice en connaissance de cause".

105 R.A. Reiter, *supra* note 100, p. 291; E. Mackay, "Les biens informationnels ou le droit de suite dans les idées", dans *L'appropriation des informations*, Paris, Litec, 1985; (1986) 3 Informatica e diritto 45, pp. 49, 64 et 65: *"Contrairement aux biens ordinaires, l'information , lorsqu'elle est appelée à circuler, devrait être non appropriable, sauf dans la mesure nécessaire pour assurer sa création"*. Définissant les biens informationnels comme *"(...) des structures d'information dont la création a exigé un investissement non nul et dont on espère tirer des revenus commerciaux par la suite"*, l'auteur observe que les droits sur l'information constituant *"(...) des exceptions au principe général de la libre circulation des idées, doivent, pour cette raison, être formulés restrictivement. (...) On observe, en dernier lieu, que le droit se perd à défaut d'exploitation. La règle contraire, en mettant l'accent sur la valeur d'assurance des droits exclusifs, retiendrait inutilement la circulation de l'information et, partant, la concurrence et l'innovation. Les droits sur l'information servent à encourager la création de l'information. Cet énoncé cache un paradoxe: en encourageant les uns, au moyen de droits exclusifs, à créer de l'information, on décourage les autres, au moins dans l'immédiat. Il se pose alors un problème de choix entre groupe de créateurs potentiels"*; K. Benyekhlef, La protection de la vie privée dans les échanges internationaux d'informations, *supra* note 39, p. 54.

106 *"Evitant ainsi d'imposer aux détenteurs et aux distributeurs d'informations de strictes obligations relatives à la collecte et à la dissémination de ces informations (...). L'inadaptation de la théorie des biens informationnels dans le monde technologique actuel et dès lors frappante"*, (K. Benyekhlef, La protection de la vie privée dans les échanges internationaux d'informations, *supra* note 39, p. 53); F.W. Hondius, "Data Law in Europe", (1980) 16 Stanford J. of Int'l. L. 87, pp. 96-97: *"any attempt to regulate control over information by a concept of ownership faces certain failure. One cannot recover information disclosed wrongfully. A court of law cannot order the recipient of such information to forget it. The correct approach to the problem of control over information must involve definition of the rights and obligations of the various parties with regard to the information"*.

107 Y. Poullet, "Le fondement du droit à la protection des données nominatives: Propriété ou Libertés" dans *Nouvelles technologies et propriété*, Montréal, Les Editions Thémis et Litec, 1991, pp. 184-185: *"Au vu des considérations qui précèdent, la thèse du droit de propriété ou des droits réels comme fondement justificatif des législations sur la protection des données nous apparaît à la fois erronée, dangereuse et incapable d'expliquer l'évolution du débat de la protection des données (...) La thèse est fausse dans la mesure où elle prétend isoler la donnée de son contexte pour la définir comme objet d'un droit réel. Or même pour les données sensibles, les législations de protection des données ne reconnaissent pas une valeur aux données en soi mais les envisagent dans leur contexte fonctionnel, c'est-à-dire en considération des finalités de leur enregistrement ou de leur traitement. A cet égard, les législations de protection de données entendent d'abord et avant tout contrôler la nature et le droit à l'information des ficheurs plutôt*

liberté dont le conflit avec d'autres libertés (la liberté d'expression, de communication et le droit à l'information[108] se résoudra par la méthode de pondération des intérêts en présence[109].

Certains auteurs ont à cet égard souligné l'incapacité du droit, et notamment de la Common law[110] de saisir dans leur globalité - en l'absence d'une définition unitaire du

---

que de connaître a priori un lien direct entre la personne et la donnée la concernant. La thèse est dangereuse, situant le droit à la protection sur le terrain des droits réels elle induit l'idée d'une commercialisation possible de ce droit (...). En d'autres termes, selon Possner, la "privacy" pourrait comme tout autre bien marchandable s'acheter ou du moins se négocier (...). La thèse, enfin, est incapable de rendre compte des évolutions réglementaires. Ainsi, le droit au consentement libre et éclairé préconisé par des réglementations nouvelles suscitées par des nouveautés technologiques comme le R.N.I.S. ou les cartes à mémoire ne se justifie pas par l'existence de nouvelles données mais bien dans la mesure où l'évolution du fait technologique crée de nouvelles formes de circulation de l'information appelant des garanties supplémentaires pour les libertés des citoyens".

[108] Voir K. Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'informations d'information*", *supra* note 39, p. 283 et s.; P. Trudel, "Réflexion pour une approche critique de la notion de droit à l'information en droit international", (1982) 23 Les Cahiers de Droit, pp. 847-871; P. Péladeau, "Esquisse d'une théorie juridique des procès d'information relatifs aux personnes" (1989) 34 Revue de droit de Mc Gill, pp. 953-982.

[109] Y. Poullet, *supra* note 107, p. 60. *"puisque l'individu n'est pas propriétaire des données le concernant, ni même titulaire sur elles d'un droit proche d'un droit réel, puisque c'est de façon spontanée que l'individu projette dans la société une certaine image de lui, cette image précisément peut-être captée par autrui, rapprochée d'autres informations et prendre ainsi un sens aux yeux de celui qui la traite. Il ne peut être question a priori de nier à autrui, le droit d'utiliser l'image que je donne de moi-même. A ma liberté, qu'il s'agisse de la liberté d'association dans le cadre de traitements opérés par un syndicat, de la liberté religieuse dans le cadre de traitements gérés par l'autorité religieuse ou plus fréquemment de la liberté d'entreprendre des le cas de fichiers d'entreprises. Le conflit de libertés doit se résoudre par la méthode de pondération des intérêts par laquelle l'autorité chargée de trancher le conflit appréciera les intérêts légitimes respectifs propres à chaque partie exprimant sa liberté".*

[110] A. Miller, *Privacy and Freedom*, *supra* note 16, p. 205 et 206: *"Although many aspects of individual privacy are recognized by the law and are protectible either on a constitutional basis or by means of a private common-law action, the available protection is not adequate to meet the threat to informational privacy that already exists and is certain to become more accute in the future. (...) Unless marked and rapid changes in judicial attitude take place, it is unrealistic to expect the common-law privacy action to reverse this shift in the balance. The crippling limitations on the individual's ability to maintain a successful suit for injuries resulting from a loss of personal privacy make it an inadequate source of protection. And even the constitutional recognition given privacy has been relatively narrow, has developed episodically, and has served*

droit à la vie privée[111] - les questions relatives au stockage des données personnelles dont la menace potentielle à la vie privée, bien que reconnue par la Cour suprême[112], n'a pas été l'objet de considérations permettant de dégager des paramètres de conduite qui s'imposeraient sinon aux entreprises privées, à tout le moins aux institutions publiques. Les remèdes traditionnels du droit civil sont en effet insuffisants pour protéger le citoyen contre l'usage abusif des données personnelles dans le secteur public[113].

---

principally as a partial retaining wall against the tide of governmental invasions. The private sector remains unaffected by the existing constitutional restraints"; K. Gormley, One Hundred Years of Privacy (1992) Wis. L. R. 1335; R.A. Sterling, "Privacy, Computerized Information Systems, and the Common Law-A Comparative Study in The Private Sector", (1983) 18 Gonzaga L.R. 567; T. Gerety, supra note 94, p. 286; K. Benyekhlef, La protection de la vie privée dans les échanges internationaux d'informations, *supra* note 39, p. 60: *"La situation ne peut être que plus incertaine au Canada où le common law ne reconnaît pas le droit à la vie privée. Au Québec, la vie privée bénéficie d'un meilleur sort, mais il est loin d'être évident que l'état actuel du droit nous permette de solutionner avec efficacité les multiples problèmes soulevés par l'informatisation"*; Rapport du Groupe d'étude, *L'ordinateur et la vie privée*, *supra* note 24, p. 144.

111 Cette inefficacité à saisir les violations potentielles à la vie privée créées par l'informatisation des secteurs publics et privés résulte du fait que la common law ne protège que certains aspects du droit à la vie privée. Cette vision catégorielle du droit à la vie privée stérilise toute innovation; J. P. Graham, *supra* note 15, p. 1411; *Comp.* en ce qui concerne l'autoroute de l'information, D. Johnston, D. Johnston et S. Handa, *supra* note 19, pp. 200-204.

112 Whalen v. Roe, 429 U.S. 589 (1977). L'analyse de la Cour suprême américaine ne porte que sur la constitutionnalité d'une loi d'Etat et sur les moyens énoncés par celle-ci pour assurer la sécurité et la confidentialité des données personnelles. Si l'énoncé du juge Brennan est porteur de développements, il ne suffit pas à appréhender toutes les questions (collecte et utilisation des données, modifications des finalités pour lesquelles elles ont été recueillies, couplage des données, qualité des données, etc.) relatives au traitement automatique des données personnelles; voir R.E. Peck, "Extending the Constitutional Right to Privacy in the New Technological Age", (1984) 12 Hofstra L.R. 893, p. 911.

113 H.P. Glenn, "Le droit au respect de la vie privée", *supra* note 39, p. 903: *"Tout d'abord, les frais et les délais entraînés par des poursuites judiciaires ont été jugés excessifs par rapport aux intérêts en cause. Deuxièmement, la complexité des systèmes contemporains de renseignements entraîne la création de systèmes complexes de contrôle, et les remèdes du droit civil ne comprennent pas la programmation et l'installation de telles mesures préventives. Finalement, l'action civile nécessite un demandeur averti et un défendeur identifiable, tandis qu'une bonne partie de la diffusion contemporaine de données est effectuée à l'insu des intéressés, et par des inconnus"*.

Ceci explique la tentation législative à protéger la vie privée des citoyens en adoptant des instruments législatifs propres à combler les lacunes du droit existant en matière de droit à la vie privée informationnelle[114], l'auto-réglementation enrichissant le réseau de protection dont pourrait bénéficier le citoyen et la jurisprudence constituant une assurance contre les risques d'obsolescence des lois de protection du traitement automatisé des données personnelles.

---

114 K. Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'informations*, *supra* note 39, p. 60 et réf. citées.

CHAPITRE 2 - LA VOIE LEGISLATIVE

SECTION 1 - LES LIGNES DIRECTRICES DE L'O.C.D.E. ET LA CONVENTION DU CONSEIL DE L'EUROPE

SOUS-SECTION 1 - CADRE GENERAL

Dans le milieu des années 70, de nombreux Etats européens se sont dotés de lois spécifiques de protection des données personnelies. Ces lois nationales[115] furent sans aucun doute induites par le travail de deux organisations internationales, le Conseil de l'Europe[116] et l'organisation de Coopération et de Développement Economique[117] qui, initiant une réflexion à ce sujet dès le début des années 70[118], adoptèrent deux

---

115 Ainsi la France en 1978, la République fédérale d'Allemagne en 1977, l'Angleterre en 1984, la Suède en 1973, la Finlande en 1987, les Pays-Bas en 1988, le Luxembourg en 1979, la Belgique et l'Espagne en 1992, etc.

116 M.P. Roch, "Filling the void of Data Protection in the United States: Following the European Example" (1996) 12 Santa Clara Computer and High Technology L. J. 71, p. 73: "*The council of Europe was founded in 1948 by several European nations in order to further unities among its members and to promote civil liberties*". H.E. Pearson, Data Protection in Europe, (1991) 8 Computer L. 24, 24 fn. 1.

117 M.P. Roch, *supra* note 116, p. 73: "*The Organization for Economic Development, founded in 1960 by 20 nations including the United Sates, aims "to promote economic and social welfare throughout the OECD area by assisting member governments in the formulation and coordination of policies; to stimulate and harmonize members'aid efforts in favor of developing nations; and to contribute to the expansion of world trade*"; R.C. Boehmer et T.S. Palmer, "The 1992 EC Data Protection Proposal: An Examination of its Implications for V.S. Business and U.S. Privacy Law" (1993) 31 Am. Bus. L.J. 265, 271, n. 33.

118 L'O.C.D.E. a commencé à s'intéresser à la protection des données à caractère personnel et à la question des flux transfrontières dès 1971 (OECD, *Policy Issues in Data Protection and Privacy*, dans 10 OECD Informatics Studies (1974)). Suite à la conférence de Vienne de 1977, un groupe d'experts a été chargé d'étudier la problématique. (Voir H.P. Gasmann, "The Activities of the OECD in the Field of Transnational Data Regulation in Online, Data Regulation and Third

conventions une dizaine d'années plus tard: *les Lignes directrices de l'O.C.D.E. régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel* du 23 septembre 1980[119] et *la Convention du Conseil de l'Europe pour la*

World Realities", (1978) Int'l L.R. 177, p. 182; A.H. Robertson, European Institution Co-operation, Integration, Unification, 3e éd., London, Stevens/Matthew/Bender, 1973, p. 83). Le mandat du groupe de travail consiste à: "*develop guidelines on basic rules governing transborder flow and the protection of personal data and privacy in order to facilitate a harmonization of national legislation, without precluding the establishment of an International Convention at a later date; and (2) investigate the legal and economic problems relating to the transborder flow of non personal data in order to provide a basis for the development of guidelines in this area to take into account the principle of free flow of information*" (M.D. Kirby, "Transborder Data Flows and the "Basic Rules" of Data Privacy" (1980) 16 Stanford J. Int'L L. 27, p. 43. Leur travail aboutira le 21 novembre 1979 à un projet de Lignes directrices qui ne seront adoptées que le 23 septembre 1980 par Recommandation du Conseil: "*le Conseil recommande: (1) Que les pays Membres tiennent compte, dans leur législation interne, des principes concernant la protection de la vie privée et des libertés individuelles exposées dans les lignes directrices figurant en Annexe à la présente Recommandation dont elle fait partie intégrante; (2) Que les pays Membres s'efforcent de supprimer ou d'éviter de créer, au nom de la protection de la vie privée, des obstacles injustifiés aux flux transfrontières de données de caractère personnel; (3) Que les pays Membres coopèrent pour mettre en oeuvre les lignes directrices énoncées en Annexe; (4) Que les pays Membres conviennent dès que possible de procédures spécifiques de consultation et de coopération en vue de l'application des présentes lignes directrices*".

Quant au Conseil de l'Europe, ses réflexions en la matière datent de la Conférence de Téhéran de 1968 (Council of Europe, Parliamentary Assembly Recommandation 509 (1968)). En 1970, un rapport relatif à la protection de la vie privée des individus au regard de l'informatique rédigé par un comité d'experts sur les droits de la personne est soumis au Comité des ministres du Conseil de l'Europe (A.C. Evans, "European Data Protection Law" (1981) 29 Am. J. Comp. L. 571, p. 573; F.W. Hondius, *supra* note 106, p. 91. A la suite de ce rapport, un nouveau comité d'experts sur la protection de la vie privée a développé des propositions relatives à la protection des données à caractère personnel. A la suite de ces propositions, deux résolutions relatives à la protection des renseignements nominatifs sont adoptées par le Comité des ministres en 1973 en ce qui concerne le secteur privé et en 1974 en ce qui concerne le secteur public (Recommandations (73) 22 et (74) 29); P.E. Cole "New Challenges to the U.S. Multinational Corporation in the European Economic Community: Data Protection Laws", (1985) 17 N.Y.V.J. Int'l L. & Pol. 893, 898 n. 30. Ces résolutions poseront les principes fondamentaux de la Convention de 1981, ainsi d'ailleurs que ceux des Lignes directrices de l'O.C.D.E. La Convention ouverte à la signature des Etats membres le 21 janvier 1981, est entrée en vigueur le 1er octobre 1985, suite à sa ratification par cinq Etats membres (la République fédérale allemande, l'Espagne, la France, la Norvège et la Suède), conformément à l'article 22 (2) de la Convention (R.J. Schweizer, "La Convention du Conseil de l'Europe sur la protection des données personnelles et la réglementation des flux transfrontières de données" (1986) 4 Droit de l'informatique 191, p. 191).

[119] OECD, *Guidelines Governing the Protection of Privacy and Transborder Data Flow of Personal Data*, dans 80 OECD Document C58 final (1980) [ci-après les *Lignes directrices*]; sur la résolution de 1989 des Nations-Unies "*for the regulation of computerized personal data files*",

protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981[120]. Ces deux textes sont toujours d'application, nonobstant l'adoption de la Directive européenne.

Soulignons que si la Convention est juridiquement contraignante pour les Etats signataires[121], il n'en va pas de même pour les Lignes directrices qui se présentent sous la forme d'une annexe à une Recommandation du Conseil[122]. L'intérêt de la Convention est donc de s'imposer à un certain nombre de pays, alors que celui des Lignes directrices réside plutôt dans le nombre plus étendu d'Etats auxquels elles s'adressent. L'O.C.D.E. comprend en effet des Etats ne faisant pas partie du Conseil de l'Europe: le Canada, les Etats-Unis, l'Australie, le Japon, la Nouvelle-Zélande, la Suisse et la Turquie[123].

---

voir U.U. Wuermeling, "Harmonisation of European Union Privacy Law", (1996) 14 the John Marshall J. of Computer & Information L., p. 418: *"the principles of the UN Resolution are very similar to those of the COE Convention, but have no direct legal effect on the Member states"*.

120 Ou *"Convention 108"*; Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, (Jan. 2, 1981); Eur. Treaty Series No.108 [ci-après, la *Convention du Conseil*]; Pour une analyse détaillée de la Convention; voir G.W. Coombe et S.L. Kirk, "Privacy, Data Protection and Transborder Data Flow: A Corporate Response to International Expectations", (1983-84) 39 Business Lawyer 33.

121 A distinguer de l'effet direct des traités; voir U.U. Wuermeling, *supra* note 119, p. 418: *"while the COE Convention came into force on october 1, 1985, it has no legal direct effect on the law or juridiction of the member states, because it is a ""non self-executing" treaty"* et note 22: *"Non-self executing" means that each Members states must enact enabling legislation for the COE Convention to become effective"*; Th. Zerdick, "European Aspects of Data Protection: what rights for the citizen?" (1995) 2 Legal Issues of European Integration 59, pp. 60 et 63.

122 *"Pour commencer, les lignes directrices de l'O.C.D.E. n'ont pas de caractère obligatoire du point de vue juridique, alors le Conseil de l'Europe a établi une Convention qui liera juridiquement les pays qui l'auront ratifiée"*, (Exposé des motifs, p. 24); Council of Europe, Convention for the Protectio of Individuals with Regard to Automatic Processing of Personal Data, *supra* note 120, *ibid.*

123 Le Canada, l'Australie, l'Irlande, le Royaume-Uni et la Turquie n'ont pas souscrit à la recommandation du Conseil du 23 septembre 1980. Le Canada a officiellement adhéré aux lignes directrices le 29 juin 1984; voir Ministère de la Justice, *Les lignes directrices régissant la protection de la vie privée et les flux transfrontières de caractère personnel de l'O.C.D.E.:*

Cette différence de statut juridique explique les divergences dans la rédaction des articles concernant la mise en oeuvre de ces conventions. La Convention adopte un ton plus directif que les Lignes directrices, en imposant à chaque Etat de prendre dans son droit interne les mesures nécessaires pour donner effet aux principes fondamentaux de protection des données personnelles[124]. Selon le rapport explicatif de la Convention[125], les *mesures nécessaires dans son droit interne peuvent revêtir, outre la loi, différentes formes telles que règlements, directives administratives, etc... [Ces] mesures (...) peuvent être complétées par des mesures de réglementation volontaire (...), telles que codes de (...) conduite (...)"*. La Convention ajoute en outre un délai contraignant pour la mise en oeuvre de ces mesures[126]. En revanche, les Lignes directrices adoptent un ton permissif qui convient à une recommandation non contraignante[127]. L'article 19 des Lignes directrices prévoit en effet que les Etats membres devraient établir des procédures juridiques, administratives et autres, ou des institutions pour protéger la vie privée par rapport aux données à caractère personnel. Les pays membres sont invités à adopter une législation nationale appropriée (article 19 a)) ou à favoriser et soutenir des systèmes d'auto-réglementation tels que des codes de conduite (article 19 b)[128].

---

incidences pour le Canada, Ottawa, Ministère des Approvisionnements et Services, 1985, p. 1.

[124] Article 4 de la Convention.

[125] Conseil de l'Europe, *Rapport explicatif concernant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (Strasbourg, 1981), p. 16.

[126] Au plus tard au moment de l'entrée en vigueur de la Convention à son égard (article 4.2 de la Convention).

[127] L'exposé des motifs nous en rappelle l'esprit, *"Les modalités (de mise en oeuvre) vont nécessairement varier selon les différents régimes et traditions juridiques et la paragraphe 19 s'efforce donc simplement d'établir un cadre général exposant dans ses grandes lignes le type de mécanisme national qui est envisagé pour mettre les lignes directrices en application"* (Exposé des motifs, p.39).

[128] Ce second moyen de mise en oeuvre est le résultat des pressions américaines dont le législateur n'intervient que de manière sectorielle dans certains secteurs qui, à ses yeux, ne peuvent être

SOUS-SECTION 2 - CHAMP D'APPLICATION

Ces deux conventions s'appliquent tant au secteur public qu'au secteur privé[129]. Elles ne couvrent cependant pas les mêmes fichiers: les Lignes directrices s'appliquent indistinctement aux fichiers manuels et automatisés[130] tandis que la Convention ne vise que les fichiers automatisés[131]. La possibilité est néanmoins laissée aux Etats de préciser lors du dépôt de leur instrument de ratification qu'ils appliqueront également la Convention aux fichiers manuels[132]. A l'inverse, les Etats membres de l'O.C.D.E. peuvent prévoir de ne pas appliquer les lignes directrices aux fichiers manuels[133].

SOUS-SECTION 3 - PRINCIPES FONDAMENTAUX

Les Lignes directrices ainsi que la Convention consacrent la notion de «*noyau dur*» qui, à des degrés divers, s'est peu a peu imposée dans les différents Etats membres. Comme on l'a observé[134], *"plus que d'amener les Etats à prendre conscience d'un problème qui en Europe n'est plus guère ignoré, il s'agit d'amener ces Etats à se persuader du caractère opportun d'une harmonisation des législations nationales, fût-ce de façon minimale autour d'un "noyau dur" qui devrait être commun".*

---

protégés autrement que par la voie législative; A.P. Miller, "Teleinfomatics, Transborder Data Flaws and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age", (1986) 20 Colum. J.L. & Social Prob. 89, pp. 115-116.

129 Article 2 des Lignes directrices et 3 (1) de la Convention.

130 Article 2 des Lignes directrices.

131 Article 3.1 de la Convention.

132 Th. Zerdick, *supra* note 121, p. 61; U.U. Wuermeling, *supra* note 119, p. 432: *"The English Data Protection Act (...) applies only to automatically stored data and The German Bundesdatenschutzgesetz applies only in some circonstances to manuel data"*.

133 Article 3.c. des Lignes directrices.

134 Lamy, note 145, p. 1345 n° 2074, cité par K. Benyekhlef, *La protection des la vie privée dans les échanges internationaux d'informations*, *supra* note 39, p. 45.

L'article 6 des Lignes directrices dispose à cet égard que *"les présentes lignes directrices devraient être considérées comme des normes minimales susceptibles d'être complétées par d'autres mesures visant à protéger la vie privée et les libertés individuelles"*.

Plutôt que l'expression *«normes minimales»*, la Convention fait explicitement référence au vocable *«noyau dur»*: *"les principes du noyau dur reconnaissent aux personnes concernées dans tous les Etats où la Convention s'applique, un certain minimum de protection au regard du traitement automatisé de données à caractère personnel. (...) En outre, le noyau dur aboutira à une harmonisation entre les Parties et, par conséquent, comportera une diminution des possibilités de conflits de lois ou de juridictions"*[135].

La notion de "*noyau dur*" permet donc une harmonie législative minimale autour d'un plus petit commun dénominateur[136]. L'objectif en est de faciliter la libre circulation de l'information dans la mesure à grâce à ce corpus de règles communes, *"un Etat n'aurait*

---

[135] Conseil de l'Europe, *Rapport explicatif concernant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, *supra* note 125, p.12

[136] Plutôt que de chercher à harmoniser les législations elles-mêmes, ce qui apparaît difficile, voire impossible, eu égard à la diversité juridique existante dans les Etats membres de l'O.C.D.E. ou du Conseil de l'Europe, il s'agit d'harmoniser les principes de base (noyau dur); K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 39, pp. 162 et 89; H.P. Gasmann, "Vers un cadre juridique international pour l'informatique et autres nouvelles techniques de l'information" (1985) Annuaire français de droit international 747, p. 755: *"Il ne sera probablement jamais possible d'harmoniser les législations elles-mêmes, du fait des diversités de tradition, d'approche et même de philosophie entre pays; mais une harmonisation des principes de base et des concepts sur lesquels les législations nationales reposent, serait déjà un bon résultat. L'avantage d'une telle démarche est que par un effet d'osmose internationale, un consensus proposé par une organisation internationale fait disparaître les effets de domination de tel ou tel pays pionnier et accélère la diffusion de ces conditions-cadre au plan international"*.

plus à se soucier du sort des données personnelles concernant ses nationaux qui sont exportées vers un Etat ayant souscrit aux Lignes directrices ou à la Convention du Conseil de l'Europe, puisque ces données bénéficient d'une protection équivalente à celle dont elles jouissent sur le territoire national"[137]. Cette technique souple permet également aux Etats membres de prévoir dans leur législation interne une protection de certaines données plus étendue que celle minimale du *"noyau dur"*, telles les données *"sensibles"*, c'est-à-dire les données à caractère personnel qui révèlent l'origine raciale ou ethniques , les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que les données relatives à la santé et à la vie sexuelle, etc. auxquelles les Etats sont tenus d'octroyer une protection renforcée, conformément aux articles 3.a des Lignes directrices et 11 de la Convention[138].

Constituent le *"noyau dur"* les neufs principes de base suivants[139]: la limitation en matière de contenu ou le principe de collecte loyale et licite,[140] la qualité et la proportionnalité des données,[141] la spécification des finalités,[142] la limitation de l'utilisation,[143] les garanties de sécurité,[144] la transparence,[145] la participation

---

137 R. Lapière, R. Coté, G.A. Le Bel, P. Roy, et K. Benyekhlef, *Vie privée sans frontières: les flux transfrontières de renseignements personnels en provenance du Canada, supra note 6*, p. 247.

138 T. Zerdick, *supra* note 127, p. 62: *"Article 11 follows a party to include in its domestic law other categories of sensitive data, the processing of which is prevented or restricted"*; Voir U.U. Wuermeling, *supra* note 119, p. 442.

139 Ces principes fondamentaux, outre le principe de justification sociale, ont été dégagés par le Juge Kirby (M.D. Kirby, supra note 118, p 42).

140 Articles 7 des Lignes directrices et 5.a. de la Convention.

141 Articles 8 des Lignes directrices et 5.c - 5.d. de la Convention.

142 Articles 9 des Lignes directrices et 5.b. de la Convention.

143 Articles 10 des Lignes directrices et 5.b. de la Convention.

144 Articles 11 des Lignes directrices et 7 de la Convention.

individuelle,[146] la responsabilité[147] et la détention limitée.[148] Ces principes sont explicitement consacrés par les deux textes, hormis les principes de détention limitée pour la Convention et de responsabilité pour les Lignes directives. Une lecture conjuguée d'autres principes permet toutefois d'en retrouver implicitement la trace.

SOUS-SECTION 4 - FLUX TRANSFRONTIERES DE DONNEES A CARACTERE PERSONNEL

Tant les Lignes directrices que la Convention examinent la question des flux transfrontières de données personnelles[149], sous le seul angle cependant des flux internes aux Etats membres. Elles n'envisagent pas les flux transfrontières vers les Etats tiers non signataires. L'Etat exportateur peut donc tout aussi bien interdire ou restreindre les flux de données personnelles vers ces Etats que les autoriser purement et simplement.

Les articles 17 des Lignes directrices[150] et 12 de la Convention[151] disposent qu'il ne peut

---

145 Articles 12 des Lignes directrices et 8a. de la Convention.

146 Articles 13 des Lignes directrices et 8, de la Convention.

147 Articles 13 des Lignes directrices et 8.d. - 10 de la Convention.

148 Articles 8 des Lignes directrices et 5.e. de la Convention.

149 U.U. Wuermeling, *supra* note 119, p. 416: *"the OECD Guidelines seem to be free data flow regiration rather than a data protection regulation"*; *Adde*: A.C.M. Nutger, *Transborder Flow of Personal Data Within the E.C.*, Kluwer, Computer Law Series, p. 308.

150 *"Un pays Membre devrait s'abstenir de limiter les flux transfrontières de données de caractère personnel entre son territoire et celui d'un autre pays Membre, **sauf lorsque ce dernier ne se conforme pas encore pour l'essentiel aux présentes Lignes directrices** ou lorsque la réexportation desdites données permettrait de contourner sa législation interne sur la protection de la vie privée et des libertés individuelles. Un pays Membre peut également imposer des restrictions à l'égard de certaines catégories de données de caractère personnel pour lesquelles sa législation interne sur la protection de la vie privée et des libertés individuelles prévoit des réglementations spécifiques en raison de la nature de ces données et pour lesquelles l'autre pays Membre ne prévoit pas de **protection équivalente**."*

151 *"Une partie ne peut pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel à destination*

y avoir restriction légitime à une transmission de données personnelles vers l'Etat importateur si celui-ci offre une "*protection équivalente*" à celle qui existe dans l'Etat exportateur, ce qui fait l'objet d'une présomption.

Le principe est donc la liberté des flux transfrontières entre Etats parties aux Lignes directrices ou à la Convention et la faculté d'y opposer des restrictions dans le cas de flux vers les Etats non signataires ou s'il n'existe pas de protection équivalente dans l'Etat destinataire[152].

Cette voie suppose donc une étude approfondie du système juridique du pays récepteur par l'agence de protection des données du pays exportateur chargée de contrôler le trafic international de données personnelles[153]. Le contrôle des flux transfrontières de données personnelles s'estompe dès que l'Etat importateur respecte l'essence des normes législatives nationales de l'Etat exportateur[154].

---

du territoire d'une autre Partie. 3 - Toutefois, toute Partie a la faculté de déroger aux dispositions du paragraphe 2: a) dans la mesure où sa législation prévoit une règlementation spécifique pour certaines catégories de données à caractère personnel ou des fichiers automatisés de données à caractère personnel, en raison de la nature de ces données ou de ces fichiers, sauf si la réglementation de l'autre Partie apporte une ***protection equivalente****: b) lorsque le transfert est effectué à partir de son territoire vers le territoire d'un Etat non contractant par l'intermédiaire du territoire d'une autre Partie, afin d'éviter que de tels transferts n'aboutissent à contourner la législation de la Partie visée au début du présent paragraphe.*

[152] Parce qu'un Etat membre a prévu une réglementation plus exigeante pour une catégorie particulière de données qu'elle juge plus sensible.

[153] J. de Houwer, *Privacy and Transborder Data Flows (A comparative study of International and National Regulations)*, Document inédit, Vrije Universiteit Brussel, octobre 1989, p. 43: "*This requirement to examine the legal system of the recipient country does however put an enormous burden on the data protection authorities as they would have to assess the legal order of a foreign country*".

[154] K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", (1991-1992) 2 Média and Communications L.R. 157, pp. 177 - 178.

Ce principe d'équivalence[155] soulève de sérieuses difficultés d'interprétation[156]: signifie-t-il que l'Etat importateur doit être pourvu d'un législation en la matière ? La voie contractuelle ou l'auto-réglementation constitue-t-elle un substitut adéquat à l'absence d'un texte législatif ?[157]

Si l'article 4 de la Convention[158] paraît consacrer l'auto-réglementation comme un mode de régulation complémentaire à une approche législative, l'article 19 des Lignes directrices[159] semble autoriser les Etats à recourir exclusivement à l'auto-réglementation. Un rapport récent de l'O.C.D.E. semble toutefois indiquer que l'autoréglementation ne peut exclusivement régir la protection des données dans le secteur tant public que privé dans la mesure où il n'assurerait pas à la personne concernée la sanction effective de ses

---

155 Que n'exige pas la Directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel; *infra*, Section 2 - la directive européenne, *Sous-section 3 - Flux transfrontières de données personnelles, paragraphe 2 - notion de "protection adéquate"*.

156 M.P. Roch, *supra* note 116, p. 85: "(...) "h*owever, the exact standard of equivalency was never determined*".

157 K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, pp. 182-186 citant M. Briat, "Personal Data and the Free Flow of Information", dans G.P.V. Vanderberghe éd., *Freedom of Data Flows and EEC Law*, (Proceeding of 2nd CELIM Conference), Deventer, Kluwer Law & Taxation Publishers, 1988, p. 47.

158 L'article 4 de la Convention prévoit que chaque Etat Membre prend, dans son *"droit interne"*, les mesures nécessaires pour donner effet aux principes de base de protection des données énoncées au Chapitre II. Le rapport explicatif de la Convention, ajoute que *"de telles mesures contraignantes [telles la loi, les règlements, les directives administratives, etc.] peuvent utilement être complétées par des mesures de réglementation volontaire dans le domaine de l'informatique, telles que codes de bonne pratique ou des règles de conduite professionnelle. Toutefois ces mesures volontaires ne suffisent pas par elles-mêmes pour donner suite à la Convention"* (Conseil de l'Europe, *Rapport explicatif concernant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg; 1981, p. 16).

159 *Supra* Sous - Section 1 - Cadre général; l'article 19 précise que les Etats Membres, dans le cadre de la mise en oeuvre des principes fondamentaux, devraient notamment s'efforcer d'adopter une législation nationale appropriée (art. 19a) ou de favoriser ou de soutenir des systèmes d'autorégulation (codes de conduite ou autres formes) (art. 19b).

droits par un tiers habilité quant à ce[160].

Comme on l'a observé[161], "*il est sans doute imprudent de prétendre que la voie de l'autoréglementation ne représente plus un mode licite de mise en oeuvre des principes fondamentaux dans le cadre des Lignes directrices de l'OCDE*".

Comme nous le verrons, ces questions d'interprétation seront également soulevées dans le cadre de la Directive européenne.

Envisageant la question des flux transfrontières sous l'angle des données provenant d'un Etat membre à destination d'un Etat tiers à l'Union européenne, la problématique sera radicalement différente. Les réponses le seront également.

---

[160] OECD, *Present Situation and Trends in Privacy Protection in the Area*, DSTI/ICCP/88.5 (1er juin 1988), p. 19 ("Rapport de l'OCDE de 1988"): *These recommendations (codes de conduite) will, in these circumstances, make a positive contribution. Indeed, the development of voluntary codes is a recognition that data privacy laws are an essential concomitant of automated processing of personal data. Such codes may also have the effect of promoting, customer confidence in the services offered so that there may be favourable trade implications [...]. In countries where there is existing data protection legislation, the existence of voluntary codes of practice is seen as a fine-tuning mechanism which translates the general terms of the legislation into practical terms to be adopted by the particular sector or organisation. Doubtless these organisations must comply with the provisions of the legislation, however it is not always easy to determine the precise application of general legislation to specific circumstances in an organisation or sector. From the foregoing, it can be seen that there is voluntary convergence in personal data regulation towards the principles outlined in the OECD Guidelines. It must be added however that voluntary adherence to a code of conduct unsupported by legislation does not provide data subjects with inviolable rights against data users or collectors so that this must always be a reservation where the voluntary regulatory approach is used*".

[161] K. Benyekhlef, "*Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes*", *supra* note 154, p. 186.

SOUS-SECTION 5 - MISE EN OEUVRE

La mise en oeuvre des Lignes directrices, instrument juridique non contraignant[162], diffère considérablement entre Etats signataires[163]. Comme indiqué[164], les Lignes directrices laissent le choix - même, semble-t-il exclusif - entre deux mises en oeuvre dont l'approche législative a été adoptée par la plupart des pays européens dans le secteur tant public que privé et par les pays de common law, en particulier les Etats-Unis, l'Australie et le Japon dans le secteur public, ces législations[165] laissant au secteur privé le soin d'élaborer des codes de conduite[166]. Les Etats-Unis ont choisi une formule souple d'auto-réglementation qui, en pratique, s'éloigne radicalement du respect des principes de base des Lignes directrices. Le Canada, à l'exclusion du Québec, qui a récemment adopté une législation couvrant le secteur privé, s'oriente au contraire vers une formule plus rigoureuse d'auto-réglementation, sous la forme du *"CSA Model*

---

162 U.U. Wuermeling, *supra* note 119, p. 416: *"The legal effect of the OECD Guidelines was limited because of three additional reasons: first, the OECD members (24 nations) do not have a legal duty to implement the OECD regulations. Second, the exent of wide exemptions in the OECD Guidelines limits its effect. Third, the council of Europe took action in the field of data protection regulation by passing the council of Europe convention on data Protection"*; Adde: R. Elger, *Dater export* dans Drissraten, 1 CR 2 (1993); P. Lume, "An EEC Policy for Data Protection", (1992) 11 Computer L.J. 399, 405; en ce qui concerne le bilan de la Convention du Conseil, voir Th. Zerdick, *supra* note 121, pp. 63-64.

163 M.P. Roch, *supra* note 116.., p. 76: *"This deficiency and the inherent differences betwee, each country's implementing legislation have contributed to a lack of harmony between the European nations laws"*.

164 *Supra Sous - Section 1, Cadre général.*

165 Sur les législations spécifiques adoptées aux Etats-Unis, essentiellement le *"Privacy Act*, 54 U.S.C. 522 a (1974)", voir R. Bigelow, *Privacy*, (1993) 2 Comp. Law Ser. Rep 50; R.J. Krotoszinsky, Autonomy, Community, and Traditions of Liberty: The Contrast of British and American Privacy Law", (1990) Duke L.J. 1398, 1434; J.R. Reidenberg, "The Privacy Obstacle Course Hurdling Barriers to Transnational Financial Services", (1992) 60 Fordham L.R. S137; W. Freedman, *The right of Privacy in the Computer Age*, New York, Quorum Books, 1977.

166 K. Benyekhlef *"Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes"*, *supra* note ..., p. 151.

Code"[167].

Suite de l'adoption de la Convention, le Conseil de l'Europe a adapté à des secteurs particuliers les principes de base qu'il avait établi. Il a ainsi émis des recommandations en matière d'échange internationaux d'informations de police, particulièrement sensible depuis l'adoption de l'Accord de Schengen et la Convention de Dublin, de technologie et de données médicales[168]. Le Conseil de l'Europe élabore actuellement des projets de recommandations concernant les données personnelles collectées et traitées à des fins statistiques et concernant les compagnies d'assurances (le problème des listes noires est dans ce domaine particulièrement sensible).

Les Communautés européennes n'ont à ce jour pas adhéré à la Convention. Suite à la recommandation de la Commission européenne lors de l'adoption de la Directive européenne, des négociations ont été engagées en ce sens. Vu la différence de vocation entre ces deux institutions, l'adhésion prévue pour la fin 1997 améliorerait la protection des données à caractère personnel.

SECTION 2 - LA DIRECTIVE EUROPEENNE

SOUS-SECTION 1 - CADRE GENERAL

La Directive européenne 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

---

[167] Voir *infra* Chapitre 3 - les codes de conduites, Section 2 - CSA Model.

[168] Voir Recommandation n° R (97) 5 relative à la protection des données médicales, adoptée par le Comité des ministres le 13 février 1997.

circulation de ces données[169], est l'aboutissement d'une évolution continue dans les institutions et pays européens; elle n'est ni le premier ni le seul texte consacré à cette matière.

Bien avant l'adoption de la Directive, en 1973, la Commission européenne, pressentant que *"l'établissement de banque de données, aux ramifications internationales"* obligerait la Communauté à *"instaurer des mesures communes de protection des particuliers"*, avait établi un rapport précisant qu'*"il serait préférable que la Communauté recherche un consensus politique véritable en vue d'instaurer des règles de base communes, plutôt que d'être tenue d'harmoniser ultérieurement des législations nationales contradictoires"*[170]. Le Parlement européen, quant à lui, avait adopté une série de résolutions en 1974,[171] en 1975,[172] 1976[173] et 1979[174] par lesquelles il invitait la Commission européenne à édicter une directive instaurant un équilibre entre la protection de la vie privée et la libre circulation de l'information à l'intérieur de la

---

169 CE, *Directive (CEE) No 95/46 du Parlement européen et du Conseil du 24 octobre 1995*, J.O. Législation (1995) n° L281, p. 31, [ci-après la *Directive européenne*].

170 L. Focsaneanu, "La protection des données à caractère personnel contre l'utilisation abusive de l'informatique", (1982) 109 J. Droit Int'l 55, p. 62; R.C. Mathews, "Protection of Rights on Individuals in the EEC in Relation to Automatic Processing of Personal Data" (1987) Int'l Bus. L. 410, p. 410.

171 A.C.M. Nutger, *supra* note 149, p.29.

172 CE, *Resolution (EEC) of the European Parliament on the Protection of the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing*, J.O. Communications (1975) n°C60, p. 48.

173 CE, *Resolution (EEC) of te European Parliament on the Protection of the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing*, J.O. Communications (1976) n°C100, p. 27.

174 CE, *Resolution of the European Parliament on the Protection of the Rights of the Individual in Connection in the Face of Technical Developments in Data Processing*, J.O. Communications (1979) n° C140, p. 34; voir K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, p 157; U.U. Wuermeling, supra note 119, p. 419.

Communauté[175]. Aucune de ces résolutions[176] n'a abouti à l'élaboration d'une directive, la Commission considérant que les Etats membres et la Communauté européenne ratifieraient la Convention du Conseil de l'Europe.

En dépit de leur adhésion, conformément aux recommandations de la Commission et du Parlement,[177] certains Etats membres, n'ont pas élaboré de législations nationales spécifiques[178] ou ont adopté des législations dont ce niveau de protection n'est pas équivalent[179], créant ainsi des obstacles à la circulation transnationale des données

---

175 J. de Houwer, *supra* note 153, pp. 38-39: *"This resolution is an attempt to balance the principles of competition and circulation of goods and services and the importance of personal data protection, and it recommends that the Membre States coordinate their efforts is all international forums where there questions are discussed, and that they work for the accession to the Council of Europe Convention by as many states as possible"*.

176 U.U. Wuermeling, supra note 119, p. 419: *"a resolution itself has no direct binding force"*.

177 La Commission, par recommandation du 29 juillet 1984 (CE, *Recommendation (EEC) No 81/679 of the Commission Relating to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, J.O. Législation (1981) n° L246, p. 31) et le Parlement, par résolution du 9 mars 1982 (CE, *Resolution (EEC) of the European Parliament on the Protection of the Rights of the Individual on the Face of Technical Developments in Data Processing*, J.O. Communications (1982) n° C87, p. 39), ont recommandé aux Etats membres de ratifier la Convention avant la fin 1982. La résolution du 9 mars 1982, s'écartant d'un rapport précédent qui concluait à la nécessité d'une action régulatrice de la Commission, en dépit de l'existence de la convention, précisait que *"s'il appert que le dispositif de la Convention (...) est incapable d'appréhender et de traiter les problèmes liés à la protection de la vie privée et au principe de la libre circulation de l'information, il y aura lieu d'élaborer une directive communautaire en la matière"*; R.C. Matthews, *supra* note 170, p. 413; J de Houwer, *supra* note 153, pp. 38-39; U.U. Wuermeling, *supra* note 119, p. 419.

178 L'Espagne, le Portugal et la Belgique n'ont adopté de législation qu'au cours des années 90. A ce jour, seules la Grèce et l'Italie n'ont pas adopté de législation en matière de protection de la vie privée à l'égard du traitement de données à caractère personnel.

179 *"Si l'objectif de ces législations nationales est le même, assurer la protection de la personne concernée, elles adoptent, toutefois, des solutions différentes en raison de la multiplicité des options possibles pour garantir une telle protection. Ainsi, par exemple, la couverture des fichiers manuels, la protection des personnes morales [prévue par les lois danoise, norvégienne, autrichienne, luxembourgeoise et irlandaise], les procédures préalables à la création de fichiers, l'étendue de l'obligation de notification [à une autorité administrative prévue par les lois françaises ou britanniques], l'information lors de la collecte des données, le traitement des données sensibles, le transfert vers d'autres pays [soumis par la loi britannique à des contrôles*

personnelles et faussant le jeu de la concurrence *"entre les opérateurs privés selon le degré de contraintes auxquelles ils sont soumis dans leur pays"*[180].

Afin d'assurer une certaine uniformité normative[181], la Commission, sur la base de l'article 100 A du traité CEE, s'est résolue à énoncer, en septembre 1990, une série de propositions[182] qui ont abouti à l'élaboration de la Directive du 24 octobre 1995 qui, à

---

ou autorisations préalables], sont autant de questions qui peuvent faire l'objet d'une approche différente. En outre, les développements de la technologie peuvent conduire les Etats à réagir différemment et à accentuer ainsi cette disparité" (CE, *Proposition (CEE)de Directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Exposé des motifs)*, COM (90) 314 final - SYN 287 (Bruxelles, septembre 1990), p. 15 ("Exposé des motifs"); pour plus de développements, voir K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, p. 174: *"De plus, certaines législations laissent au secteur privé [banques, assurances, marketing direct] le soin d'élaborer des codes de conduite tout en encadrant strictement cet exercice [par exemple, la loi néerlandaise les astreint à une série de principes minimaux et les laisse libres de développer des règles précises adaptées à la spécificité de leurs activités. Les codes de conduite doivent néanmoins être approuvés par une agence de protection des données personnelles. A défaut pour le secteur privé d'élaborer des codes de conduite ou à défaut d'approbation par l'agence, le gouvernement impose alors des règles de gestion de l'information personnelle]"*.

[180] La Commission justifie également une intervention communautaire par *"la coopération et la collaboration entre les administrations nationales, [lesquelles] sont amenées à s'intensifier. Les administrations nationales sont appelées ainsi à remplir des tâches qui relèvent d'une administration d'un autre Etat membre. Dans ce contexte, la circulation des données devient une condition indispensable du processus de coopération. Ainsi, les devoirs de collaboration ou d'information qui seront imposés aux administrations par le droit communautaire nécessitent que, parallèlement, la protection des personnes à l'égard des personnes concernées soit pleinement assurée"* (*Ibid*, p. 15-17).

[181] *"La Convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel n'a pas permis de limiter cette disparité dans la mesure où, d'une part, elle laisse ouvert un grand nombre d'options pour la mise en oeuvre des principes de base qu'elle définit et, d'autre part, elle n'a été ratifiée que par sept Etats membres (Allemagne, Danemark, Espagne, France, Irlande, Luxembourg, Royaume-Uni) dont un (Espagne) qui n'a toujours pas de législation interne. La recommandation de la Commission du 29 juillet 1981 invitant les Etats membres de la Communauté à ratifier la convention du Conseil de l'Europe n'a pas modifié cette situation"*. (CE, *Proposition (CEE) de Directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Exposé des motifs)*, supra note 179, p. 15 ("Exposé des motifs")).

[182] CE, *Proposition (CEE) de la Commission pour une Directive du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*, J.O.

l'approche du 1er janvier 1998,[183] date ultime de sa transposition dans la législation interne des Etats membres, constitue, y compris à l'extérieur de l'Union européenne, un des instruments majeurs de la protection des données à caractère personnel[184].

SOUS-SECTION 2 - CHAMP D'APPLICATION

La Directive vise à protéger les libertés et droits fondamentaux des individus, notamment leur vie privée, par le biais de la protection des données à caractère personnel, afin d'assurer en contrepartie la liberté des flux d'informations sur le territoire communautaire[185].

Les données bénéficiant de la protection dont celles relatives à une personne physique

---

Communications (1990) n°C277, p. 3; pour plus de développements, voir U.U. Wuermeling, *supra* note 119, pp. 420-425.

[183] Article 32 de la Directive européenne: "*Les Etats membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard à l'issue d'une période de trois ans à compter de l'adoption de la présente directive*", soit le 24 octobre 1995.

[184] La proposition de Directive du Parlement européen et du Conseil du 24 octobre 1996 concernant "*la protection des données à caractère personnel et de la vie privée dans le secteur des télécommunications, en particulier des réseaux numériques à intégration de services R.N.I.S. et des réseaux mobiles numériques*" (J.O. Communication (1996) n° C315), est également pertinente dans ce contexte mais comme ce texte est toujours en discussion, nous ne l'envisageons pas ici; pour plus de développements, voir K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note154, p. 199 et s.; M.P. Roch, *supra* note 116, pp. 86-88.

[185] Article 1, § 1, et 2, de la Directive européenne; pour une analyse détaillée de la Directive, voir M.H. Boulanger et C. de Terwangne, "Commentaires de la proposition de Directive", dans Lamy, *Droit de l'Informatique*, 1992; S. Louveaux, "Article-by-article guide to Directive 95/46/EC", dans *A Business Guide to Changes in European Data Protection Legislation*, Cullen International, 1996; M.H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreau et Y. Poullet, "La protection des données à caractère personnel en droit communautaire", (1997) J. des Trib. de Droit eur., p. 121 et s.

identifiée ou identifiable[186], quelque soit leur forme (données écrites sur support papier, électronique ou autre, sons et images véhiculant des informations personnelles[187]), et qui font l'objet d'un traitement[188].

---

[186] *"Ainsi les adresses électroniques personnalisées (contenant des éléments suffisants pour établir l'identité de leurs titulaires - nom, prénom ou initiales par exemple) entrent dans le champ de la directive. Il en est de même des adresses non "parlantes" mais dont on connait le titulaire. Les données de routage, l'empreinte électronique laissée lors de l'utilisation de services présents sur le net, ne sont pas porteuses d'identification à priori mais si les moyens d'identification, c'est-à-dire de rattachement entre une donnée et l'identité d'un individu, sont à la portée du détenteur de la donnée, celle-ci doit être considérée comme à caractere personnel. C'est notamment le cas s'il a été demandé à l'interrogateur de s'identifier une première fois, au départ de ses opérations dans un site donné. Ce l'est aussi pour le fournisseur d'accès puisque c'est lui qui a attribué une adresse IP (la donnée de routage) à l'utilisateur. De même, si un lien contractuel ou autre existe entre le fournisseur d'informations et celui qui détient la clef d'identification, les données peuvent être considérées comme couvertes par la directive dans le chef du fournisseur d'information"* (M.H. Boulanger et C. de Terwangne, "Internet et la vie privée", Conférence du CRID sur Internet face au droit, Namur, 21 et 22 novembre 1996, p. 7).

[187] Considérant (§ 14) de la Directive européenne: *"Compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données"*; l'utilisation de ce type de donnée sur le réseau Internet est donc susceptible de tomber dans le champ d'application de la directive; (M.H. Boulanger et C. de Terwangne, *supra*, note 186, p. 8); Comp.: C. Millard et R. Carolina, "Commercial Transactions on the Global Information Infrastructure: A European perspective" (1996) 15 The John Marshall J. of Computer Information L. 269, p. 281; en ce qui concerne les risques que présente Internet à l'égard des données personnelles, voir M.H. Boulanger et C. de Terwangne, *supra* note186, pp. 1-4.

Considérant (§15) de la Directive européenne: *"Les traitements portant sur des sons ou des images ne sont compris dans le champ d'application que s'ils sont automatisés ou si les données sur lesquelles ils portent sont contenues ou sont destinées à être contenues dans un fichier structuré selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause"*; le critère retenu est donc celui de la structuration du fichier contenant les données; U.U. Wuermeling, *supra* note 119, p. 433 en ce qui concerne l'application de la Directive à la vidéosurveillance, voir P. Thomas et M.H. Boulanger, *supra* note 2, p. 223, n° 14.

[188] Le *"traitement"* s'entend au sens large, de toute opération, même prise isolément, *"telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction"* (article 2. b. de la Directive européenne).

Cette définition qui conduit à une multiplication des traitements, soulève des interrogations dans

La Directive fait également prévaloir sur la notion de *"fichier"*, déterminante dans les premières législations basées sur une localisation des données[189], la notion de *"responsable de traitement"*[190] pour définir les critères de rattachement permettant de déterminer la législation nationale applicable aux traitements entrant dans le champ d'application de la Directive. Si le responsable du traitement est établi dans un Etat membre de l'Union européenne, c'est la loi nationale de cet Etat transposant les dispositions de la Directive qui s'appliquera aux traitements effectués par le responsable dans le cadre de ses activités, conformément à l'article 4. 1. a. de la Directive[191].

---

le contexte d'Internet dont la vocation première est de permettre la circulation et la consultation d'informations. *"Ainsi, faut-il informer les personnes concernées dès que l'on consulte un site contenant des données à leur sujet et même si l'on n'a retenu aucun élément intéressant ou pertinent suite à cette consultation? En outre, si la consultation des données n'est suivie d'aucune matérialisation - les données consultées ne sont ni copiées, ni enregistrées, ni imprimées - que faut-il notifier à l'autorité de contrôle puisque l'éphémère opération n'a laissé aucune trace? Et comment accorder aux personnes concernées un droit d'accès à une information qui est tout au plus conservée dans la mémoire humaine? Il y a donc un problème [pratique] à considérer la seule consultation comme constitutive de traitement. Par ailleurs, l'énumération reprise dans la définition de l'article 2. b. est sous-tendue par une chronologie des opérations retenues. Elle débute par la collecte des données et s'achève par la destruction de celles-ci. Or, la consultation n'est pas citée en début de liste, précédant l'opération de collecte. Elle apparait au contraire entre l'extraction et l'utilisation, la communication,... Il semble donc que ce qui est visé dans la directive (...) n'est pas la consultation dans le chef de celui qui fait une "lecture" des données, mais plutôt la possibilité d'opération offerte par le traitement, le fait de laisser consulter les données; C'est d'une "offre en consultation" qu'il s'agit plutôt. (...). La consultation peut donc être retenue comme partie d'un traitement (les données collectées, enregistrées, classées, voire modifiées sont ouvertes à la consultation, par exemple) mais on ne doit pas considérer comme constitutive d'un traitement, la seule "lecture" qui n'a aucune prolongation matérielle. Cependant, dès que cette prise de connaissance donnera lieu à un copiage, un encodage ou toute autre forme de collecte ou d'enregistrement, la directive lui sera appliquée"* (M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 8-9).

[189] Sur une disquette ou sur le disque dur d'un ordinateur identifié; voir U.U. Wuermeling, *supra* note 119, p. 430; Th. Zerdick, *supra* note 121, p. 66.

[190] Qui ne doit pas nécessairement être établi sur un territoire, ce qui tient compte jusqu'à un certain point de l'évolution technologique où, dans le cadre du cybermonde *"la réalité est transnationale (...) [et] circule sans domicile fixe"* (M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 9).

[191] *"Ainsi, si une entreprise danoise ouvre un site sur Internet présentant notamment ses cadres avec une brève identification, elle doit respecter la loi danoise de protection des données. Si un complexe hôtelier espagnol offrant un service de réservation via Internet demande aux intéressés d'enregistrer leurs coordonnées afin d'effectuer la réservation, la loi espagnole de protection des*

Le responsable du traitement établi en-dehors du territoire communautaire n'est, en principe, pas concerné par la Directive. Toutefois, afin d'éviter un contournement des prescriptions communautaires ou nationales par la délocalisation de l'établissement du responsable du traitement, l'article 4. 1. c. de la Directive européenne dispose que *"tout responsable établi à l'extérieur de l'Union mais qui recourt à des **moyens**, automatisés ou non, **situés sur le territoire d'un Etat membre**, dans le but de traiter des informations nominatives, doit se soumettre à la législation de protection des données de cet Etat"*. Il doit en outre désigner un représentant établi dans cet Etat. Pour garder à cette disposition - impraticable dans le contexte du réseau mondial[192] - une portée

---

données s'appliquera au traitement de ces informations (qu'elles concernent des Français, des Russes, des Américains ou des Japonais)" (M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 10).

[192] En raison du critère *"moyens localisés sur le territoire d'un Etat membre"* utilisé pour soumettre le traitement à la loi de cet Etat. *"Internet constitue [en effet] un espace où l'information est a-localisée même si les personnes et les sites s'identifient par des "adresses"; Ces adresses sont en fait des clefs, les serrures et ce qu'elles cachent n'étant pas nécessairement géographiquement stables. (...). Pour trouver le correspondant géographique d'un site Internet, deux solutions sont envisageables:*

- soit remonter à la localisation de (...) l'ordinateur qui assure le maintien de l'information sur le site en question. Il est cependant possible de confier à un intermédiaire la mission d'héberger l'information que l'on souhaite mettre à disposition sur Internet. Dans cette hypothèse, l'adresse électronique correspond à une boîte postale ouverte pour la circonstance mais ne révèle pas de lien direct avec la source de l'information.

- soit on peut identifier le responsable de l'information, celui qui l'a produite, et on retient le lieu de son établissement. (...) Cette solution offre l'avantage de la cohérence avec les critères de rattachement adoptés par la directive concernant les traitements effectués par un responsable établi sur le territoire communautaire. (...) Il n'est pas toujours évident de connaître le lieu d'établissement du fournisseur d'information (...). Par ailleurs (...), pour localiser [les forums et autres "lieux" de rencontre ou d'échange], recourt-on à l'établissement du modérateur ou "maître du forum" ? (M H. Boulanger et C. de Terwangne, *supra* note 186, pp. 10-11). Si les moyens peuvent être localisés sur le territoire communautaire, se pose la question de savoir si ces moyens sont utilisés pour effectuer un traitement . Au sens large ainsi défini, *"copier des données revient à les collecter, ce qui est en soi constitutif de traitement aux yeux de la Directive. En conséquence, celui qui par la voie d'Internet, télécharge des données nominatives à partir d'un site ouvert par un fournisseur d'informations établi dans un Etat membre, effectue par là-même un traitement pour lequel il a recouru à des moyens (automatisés in casu) rattachés au territoire communautaire. Dans cette situation, il est tenu de respecter la réglementation*

effective, une lecture téléologique semble s'imposer. Comme on l'a observé[193], la *ratio legis* de cet article est *"d'éviter que les individus soient privés, notamment par une manoeuvre artificielle, du bénéfice de la protection de l'ensemble de la Directive"*. Il semble ainsi que l'article 4. 1. c. de la Directive européenne vise non seulement l'hypothèse où un responsable de traitement cherche délibérément à contourner la Directive et, pour ce faire, délocalise son établissement vers un pays tiers à l'Union européenne, tout en recourant à des moyens localisés sur le territoire communautaire pour réaliser son traitement, mais également l'hypothèse où le flux transfrontière de données est le fait exclusif d'un responsable localisé dans un pays tiers[194], espérant ainsi

---

européenne et de désigner un représentant établi dans l'Etat concerné", ce qui parait excessif. (M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 12).

[193] Considérant (§ 20) de la Directive européenne: *"Considérant que l'établissement, dans un pays tiers, du responsable du traitement des données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive; (...)"* et l'exposé des motifs: *"[L'article 4] fixe les critères de rattachement permettant de déterminer quelle est la législation nationale applicable aux traitements entrant dans le champ d'application de la directive et ceci afin d'éviter (...) que la personne concernée soit démunie de toute protection, en particulier du fait d'un contournement de législation"* (CE, *Proposition (CEE) modifiée de Directive du Conseil relative à la protection des personnes à l'égard des traitements des données à caractère personnel et à la libre circulation de ces données du 15 octobre 1992*, COM (92) 422 final - SYN 287, p. 13).

[194] *"C'est le cas, dans le cadre d'Internet, d'une collecte de données effectuées par le biais de "cookies" [technique qui permet à un serveur Internet d'"imprimer" sur chaque navigateur des informations qu'il détermine, telle l'adresse de la dernière page web consultée ou la date d'expiration du cookie, et qui lui permet de reconnaître un utilisateur qui a interrogé son site précédemment ou de connaître les dernières pages web visitées par l'utilisateur, à l'insu de la personne concernée, au sein même de son poste de travail. Les articles 25 et 26 ne trouvent pas à s'appliquer dans cette hypothèse car les règles protectrices relatives aux flux transfrontières ne s'adressent qu'à l'émetteur d'un flux, et pour autant (...) que celui-ci se situe en territoire européen. Or, on ne peut voir dans la personne "visitée" par les cookies un véritable émetteur des données prélevées puisque l'opération se déroule à son insu, sans qu'il ait manifesté sa volonté d'effectuer ou de voir effectuer le transfert. Plutôt que d'un flux, c'est une collecte de données qui est réalisée par le "récepteur" lorsqu'il entre en possession des informations. Le régime - plus souple - des flux transfrontières n'étant pas d'application, c'est donc le régime complet de la directive qui va s'appliquer au traitement des données obtenues à l'aide de cookies (...). En effet, à partir du moment où le responsable du traitement recourt à des moyens localisés sur le territoire d'un Etat membre (collecte au sein du poste de travail de la personne concernée), il doit respecter l'ensemble des dispositions de la directive telles qu'intégrées dans la loi nationale de l'Etat en cause; Dès lors, pour être légitime au regard de la Directive, la collecte des données à caractère personnel par le biais de cookies doit être loyale et ne peut se faire de façon occulte. Une information appropriée doit être fournie aux personnes concernées et*

échapper aux règles protectrices de la Directive relatives au flux transfrontières de données personnelles[195].

Le critère d'application de la Directive ne se réduit dès lors pas à l'utilisation de *"moyens situés sur le territoire d'un Etat membre"*. Une analyse plus globale est requise afin de déterminer si le responsable du traitement est anormalement établi en-dehors du territoire communautaire alors que son activité de traitement est centrée sur l'Europe ou si le traitement envisagé échappe à toute protection, dont celle régissant les flux transfrontières de données personnelles[196].

SOUS-SECTION 3 - FLUX TRANSFRONTIERES DE DONNEES A CARACTERE PERSONNEL

Afin que ce système de protection ne soit pas anéanti par un simple transfert des données hors du champ d'application territorial des dispositions communautaires[197], l'article 25.1 de la Directive européenne dispose que *"les Etats membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve des dispositions nationales prises en application des*

---

le but poursuivi doit être légitime. Concernant la trace électronique, le responsable du site étranger visité par une personne située en Europe ne doit pas "recourir à des moyens localisés sur le territoire d'un Etat membre" pour obtenir de telles données. Il lui suffit d'enregistrer les données de routage qui lui sont parvenues suite à l'action du visiteur. Il peut dès lors être plaidé que l'article 4. 1. c. ne s'applique pas à lui et que, de ce fait, il ne doit pas respecter le prescrit de la directive. Il ne reste plus alors qu'à prévenir les utilisateurs d'Internet que leur action dans le réseau peut ne pas passer inaperçue, même si ceux-ci ne s'en aperçoivent pas. Ici encore, l'autoréglementation d'un secteur peut apporter une réponse opportune face à la limite de l'instrument législatif, et conduire à la transparence des pratiques". (M.H. Boulanger et C. de Terwangne, *supra* note 186, pp. 13 et 19).

195 Qui ne s'appliquent qu'à l'égard des opérations effectuées sur des données envoyées à l'étranger à partir d'un Etat membre de l'Union européenne; *infra* Sous - section 3 - Flux transfrontières de données à caractère personnel.

196 M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 13.

197 M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 16; P. Thomas et M.H. Boulanger, *supra* note 2, p. 227, n° 16.

autres dispositions de la présente directive, le pays tiers en question offre un niveau de protection adéquat", sauf consentement de la personne concernée ou nécessité contractuelle[198].

Contrairement aux Lignes directrices de l'O.C.D.E. et à la Convention du Conseil de l'Europe[199], le principe est donc l'interdiction du transfert vers les pays tiers de données personnelles faisant l'objet d'un traitement tant manuel qu'automatisé et dont les responsables relèvent du secteur public ou privé[200], sauf à démontrer le caractère adéquat de la protection offerte par ce pays[201].

Paragraphe 1 - Evaluation

Dans le cadre concret décris, comment s'opère le contrôle des flux transfrontières des données personnelles[202] qu'impose cette disposition ?

---

198 Article 7a) et b) de la Directive européenne; H. Maisl, "La directive communautaire du 24 octobre 1995 relative à la protection de la vie privée", (1995) 4 D.I.T. 43, p. 44; J.P. Maximer, *supra* note 34, p. 99: *"the other provisions are 7c) (to comply with law), 7 d) (to protect the data subject) and 7e) (to perform a task carried out in the public interest exercice of official authority) (...). Article 7 f) [for the legitimate interests of the controller by third-party or parties to whom the data are disclosed. (...) Those (...) legal concepts are considerably more indefinite; Adde:* U.U. Wuermeling, supra note 119, p. 440 et s.

199 *Supra* Section 1 - Les Lignes directrices de l'O.C.D.E. et la Convention du Conseil de l'Europe, *Sous-section 4 - Flux transfrontières de données à caractère personnel.*

200 La position commune arrêtée par le Conseil le 20 février 1995 abandonne la distinction formelle entre les règles applicables au secteur public et celles applicables au secteur privé (CE, *Position commune (CEE) No 1/95 arrêtée par le Conseil le 20 février 1995*, J.O.Communications (1995) n° C93, p. 19 ("Exposé des motifs"); sur cette distinction faisant antérieurement l'objet de la proposition de Directive du Conseil, voir K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, pp. 189-190; Comp.: U.U. Wuermeling, *supra* note 119, pp. 428-429 et 439.

201 Entre Etats membres de l'Union européenne, aucun Etat ne peut invoquer le manque de protection accordée aux données personnelles dans un autre Etat pour interdire ou restreindre leur transfert, puisque, par hypothèse, la protection est uniforme entre les Etats membres (article 1.2 de la Directive européenne).

202 Certains auteurs (M.H. Boulanger et C. de Terwangne, *supra* note186, pp. 18-19) distinguent

L'article 25.2. de la Directive européenne précise que l'appréciation du caractère adéquat de la protection du pays tiers doit tenir compte de "*toutes les circonstances relatives à un transfert ou à une catégorie de transferts*" et, en particulier, de différents facteurs, fonction du transfert considéré (tels la nature des données en cause, la finalité et la durée du traitement, les pays d'origine et de destination finale ainsi que les liens existant entre les intervenants, le type de réseau (ouvert ou fermé) utilisé), ou fonction du niveau de protection en vigueur dans le pays tiers, telles les règles de droit générales ou sectorielles en vigueur, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées[203].

---

dans l'évaluation 3 catégories de flux dans le contexte d'Internet:

- les flux "*passifs*" qui "*se rapportent aux informations simplement mises à la disposition du public sur un site du réseau, [et qui] peuvent être téléchargées et, de ce fait, faire [potentiellement] l'objet d'un transfert vers un pays tiers. Pour cette catégorie de flux, il importe, avant de déposer de l'information à caractère personnel sur un site, d'évaluer la protection offerte par chaque état connecté puisque chacun de ces Etats représente un pays de destination potentiel pour les données. Si un pays se révèle dépourvu de mesures de protection adéquates, l'accès aux données ou, à tout le moins, les possibilités de copiage et de transfert des données doivent être interdits à ces pays*";

- les flux "*actifs cachés*" qui "*concernent d'une part, les données de routage, la trace électronique laissée dans le sillage des démarches effectuées dans le réseau mondial et, d'autre part, les données discrètement transférées d'un système à un autre par l'action des cookies qui entrent dans le champ de l'article 4.1.c. de la Directive européenne*", *supra*, paragraphe 2 - Champ d'application);

- les flux "*actifs conscients*" qui "*correspondent à des transferts effectués sciemment par le responsable de traitement ou par la personne concernée elle-même [qui] peuvent être décidés à l'initiative de l'émetteur ou en réponse à une demande provenant du destinataire et qui tombent le plus souvent dans les catégories d'exceptions de l'article 26 de la Directive européenne*". Comp.: C. Millard et R. Carolina, *supra* note 187, p. 282; *infra* paragraphe 4 - Dérogations. A défaut, c'est la règle de principe qui sera appliquée à l'égard de ces flux (par exemple un fournisseur de service belge vendant son registre de clients à une société de marketing canadienne ou québécoise) et une évaluation devra être faite de la protection offerte par le pays tiers concerné.

[203] M.H. Boulanger et C. de Terwangne, *supra* note 186, p.17; P. Thomas et M.H. Boulanger, *supra* note 2, p. 228, n° 17.

La notion d'adéquation requiert donc une analyse de la législation du pays tiers casuistique (i), pragmatique (ii) et fonctionnelle (iii). Il ne s'agit en effet pas de faire une comparaison abstraite et légitime de deux instruments de protection: il faut tenir compte à la fois de la réalité du transfert ou de la catégorie de transferts considérés, et de la totalité des éléments qui peuvent assurer dans le pays tiers la protection des données transférées.

(i) Analyse casuistique[204]

Le niveau de protection doit être évalué en fonction des risques qui s'attachent au transfert ou à la catégorie de transferts envisagés[205].

(ii) Analyse pragmatique

L'article 25.2 précité de la Directive européenne renvoie également à une diversité de règles, normes, instruments ou systèmes de protection[206] à prendre en considération: si l'instrument législatif facilite l'évaluation de la protection assurée par le pays tiers aux données personnelles, d'autres règles - tels les codes professionnels, la jurisprudence,

---

[204] *Infra, Paragraphe 3 -Autorisation* (la procédure plus globale de constatation du niveau adéquat, conformément à l'article 25.6 de la Directive européenne).

[205] "*Ainsi, la communication d'une liste de délinquants sexuels à une association offrant des services sociaux ou le transfert de la liste des adhérents d'un parti politique à une société de marketing présentent des risques élevés d'atteinte aux libertés des individus, par le biais de l'utilisation de leurs données. En conséquence, il convient d'évaluer de manière sévère l'adéquation de la protection offerte dans le pays tiers. Par ailleurs, on sera moins exigeant en présence d'un flux de données moins sensibles telles que les nom, fonction et durée d'ancienneté des travailleurs, intervenant entre la filiale et la maison mère d'une société. Au regard des circonstances encadrant pareil flux, étant donné le degré moindre de dangerosité qu'il présente, on admettra plus rapidement qu'un système de protection étranger est satisfait*" (M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 17).

[206] Certaines mesures techniques, du type des PICS (Protocol for Internet Content Selection), peuvent même être considérées comme système de protection; U.U. Wuermeling, supra note 119, p. 426: "*(...) The final Directive seeks to provide a framework, rather than minute provisions, in order to give members states more independence. (...) The final Directive seeks to provide a broader choice of measures to meet the requirements*".

les principes du droit ou les statuts de sociétés - pouvant offrir une protection aux données à caractère personnel faisant l'objet du flux, peuvent également être retenus. Outre ces instruments, une protection adéquate requiert que l'effectivité des règles soit assurée: il convient donc d'être attentif tant au contenu des règles ainsi qu'à leur mise en oeuvre.

(iii) Analyse fonctionnelle

L'approche retenue ne vise pas nécessairement à tenter de retrouver dans les pays tiers les mêmes dispositions que celles énoncées par la Directive européenne, mais bien à s'assurer de la mise en oeuvre par les pays tiers des principes fondamentaux de protection des données. Il ne s'agit donc pas d'une approche textuelle qui conduirait à rechercher une similarité de réglementation. C'est plutôt une "*similarité fonctionnelle*"[207] au niveau des principes protégés et des moyens d'effectivité qui est recherchée.

Si une protection adéquate n'existe que pour certains secteurs spécifiques (par exemple, le secteur bancaire ou le secteur de la santé), précisément visés par ce flux, le niveau de protection devrait être considéré comme suffisant pour autoriser le transfert, nonobstant l'absence de protection générale.

Cette approche permet donc un meilleur respect des structures et des caractéristiques juridiques locales que la recherche d'une protection "*équivalente*" qui exigerait une similarité complète, ce que la Directive européenne n'impose pas[208].

---

[207] Voir J.R. Reidenberg, "Setting Standards for Fair Information Practice in the USA", (1995) 80 *Iowa Law Review*, 13.

[208] Voir G.M. Epperson, "Contacts for Transnational Information Services: Securing Equivalency of Data Protection" (1981) 22 Har. Int'l. L. J. 157, p. 164: "*Alternatively, an exporting state*

Paragraphe 2 - Notion de "protection adéquate"

La notion d'"*adéquation*" n'a pas à ce jour été explicitée par la Commission européenne et, à notre connaissance, n'a pas été consacrée par d'autres textes communautaires. Si cette notion suppose un référent par rapport auquel l'Etat européen pourra évaluer la protection offerte par le pays tiers, celui-ci n'est pas davantage défini par la Directive.

L'exposé des motifs n'apporte aucune précision quant au choix des termes *"niveau de protection adéquat"* plutôt que *"protection équivalente"*. Comme on l'a observé[209], *"cette expression est aussi floue que celle que l'on retrouve dans la Convention (...)"*. C'est donc à tort qu'il est parfois soutenu[210] qu'une protection *"adéquate"* serait nécessairement moins exigeante qu'une protection *"équivalente"*, telle que requise par les Lignes directrices de l'OCDE et la Convention du Conseil de l'Europe.

Les difficultés d'interprétation soulevées plus haut[211], surgissent à nouveau. Qu'entend-on exactement par *"niveau de protection adéquat"*? Ce critère signifie-t-il que le pays importateur doit être pourvu d'une législation en la matière ? L'existence de règles protectrices non assemblées dans un instrument unique et cohérent, satisfait-elle au critère du niveau de protection adéquat? En d'autres termes, de quelle marge de

---

adopting the functional approach would permit the export of data in any case in which the data are guaranteed sufficient protection, irrespective of the legal regime of the importing state. Thus, a state requires an equivalent level of protection abroad, but leaves open the means of ensuring that protection, be it by the law of the importing state, by contract or by other means".

209 K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des communautés européennes", *supra* note 154, p. 195.

210 U.U. Wuermeling, *supra* note 119, p. 452: *"An adequate level will not mean the same level as within the Member State because the Member State level is "equivalent" in the language of the Directive"*.

211 *Supra*, paragraphe 4 - Flux transfrontières de données à caractère personnel.

manoeuvre disposent les Etats membres[212]?

Si l'un des buts premiers de la Directive européenne est de développer une politique commune des Etats membres quant au flux transfrontières de données personnelles[213], il reste que des disparités pourraient se présenter[214] dans l'application de la légitimité du transfert transfrontalier.

L'article 25 de la Directive européenne dispose en effet que *"(...) le transfert (...) ne peut avoir lieu que si, **sous réserve des dispositions nationales prises en application des autres dispositions de la présente directive**, le pays tiers en question offre un niveau de protection adéquat"*. Le transfert de données à caractère personnel à partir d'un Etat membre de l'Union européenne, devra dès lors toujours respecter les prescrits de la loi au sein même de cet Etat, quelle que l'évaluation de l'adéquation de la protection offerte aux données par le pays tiers[215].

---

212 M.P. Roch, *supra* note 116, p. 85: *"The standards for transborder data flows to third nations are still very high, having long raised concerns among many businesses and commentators. However, a lack of strict standards would render the directives useless since businesses could simply "export" personal data to non-European nations and process these data outside the reach of European data protection directives and national data protection laws"*.

213 *"(...) la libre circulation des données entre les Etats membres, que la présente proposition de directive vise à instaurer, suppose que des règles communes soient adoptées en ce qui concerne les transferts vers les pays tiers"* (CE, *Proposition (CEE) modifiée de Directive du Conseil 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 (Exposé des motifs)*, COM (92) 422 final - SYN 287 (Buxelles, 30 juillet 1992), p. 35 ("Exposé des motifs").

214 Voir Y. Poullet, "The European Directive relating to the protection of physical persons with regard to the processing of personal data and its free circulation - a state of relative harmony", dans *A Business Guide to Changes in European Data Protection Legislation*, Cullen International, 1996; S. Simitis, "From the Market to the Polis. The EU Directive on the Protection of Personal Data" (1995) 80, Iowa L.R. 3, p. 463 et s.; P. Schwartz, "European Data Protection Law and Restrictions on International Data Flows", (1995) 80, Iowa L.R., pp. 487 et s.

215 Ainsi, une communication d'une agence de voyages belge vers un hôtel situé aux Etats-Unis, devra, par exemple, comme n'importe quelle communication à une personne située dans l'Union

En d'autres termes, certains Etats membres pourraient être dotés d'une législation plus exigeante que d'autres, notamment en matière de données sensibles[216]. Ces exigences pourraient les conduire à refuser tout transfert de ces données si certaines conditions[217] ne sont pas remplies, ce qui conduirait à des disparités dans la mesure où d'autres Etats membres pourraient, accepter le même transfert sans conditions particulières.

Il convient donc de distinguer dans l'approche de la notion de *"protection adéquate"*, les principes de fond qui constituent le *"noyau dur"* de la protection des données, le référant de la protection et se présentent donc pour le pays tiers comme des objectifs à atteindre, des règles d'effectivité qui constituent les moyens nécessaires à garantir la réalisation de cet objectif. Leur nature, leur qualification et leur nombre importent peu, pourvu que le résultat combiné de leur présence garantisse le respect des principes fondamentaux.

Sous-paragraphe 1 - Principes fondamentaux

1 - Principes de base de la protection

Comme indiqué[218], il est possible de dégager des Lignes directrices de l'O.C.D.E. et de la Convention du Conseil de l'Europe neuf principes (le *"noyau dur"*) que l'on qualifie

---

européenne, respecter les autres prescrits nationaux belges pris en application de la Directive européenne (respect du principe de légitimité, de la qualité des données, etc.). Le fait qu'il s'agisse d'une communication vers un pays tiers, n'altère en rien la protection qui doit être assurée au sein même de ce pays.

216 H. Maisl, *supra* note 198, p. 43: *"en tenant compte des marges de manoeuvre non négligeables laissées aux Etats, un niveau de protection satisfaisant est-il désormais possible, toute idée d'"alignement par le bas" étant écartée ?"*.

217 Tel le consentement écrit de la personne concernée pour les données médicales.

218 *Supra*, Section 1 - Les Lignes Directrices de l'O.C.D.E. Et la Convention du Conseil de l'Europe, *Sous-section 3 - Principes fondamentaux*.

parfois de pratiques équitables en matière d'information (*"fair information practices"*)[219], assurant à l'individu une protection de ses données à caractère personnel. Ces principes sont consacrées, à des degrés divers, par la Directive européenne. Il nous semble dès lors possible d'en dégager certaines exigences fondamentales de protection des données personnelles mise en oeuvre par la Directive au sein et hors de l'Union européenne. Ce n'est, rappelons le, pas une protection identique qui est exigée dans le pays vers lequel les données sont transférées, mais une protection garante d'un certain nombre de principes de base interdépendants[220].

i) Principe de collecte licite et loyale[221]

Ce principe est celui de la limitation en matière de contenu des données à caractère personnel. Les données personnelles doivent également être recueillies après que la personne concernée en ait été informée ou que son consentement[222] ait été obtenu.
En ce qui concerne les transferts de données personnelles vers des pays tiers, les données ne peuvent être collectées par des moyens illicites ou illégaux ou être envoyées dans un pays tiers pour des finalités non admises au sein même de l'Union européenne

---

219 K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des communautés européennes", *supra* note 154, p. 162 et s.

220 Comme le souligne l'exposé des motifs, l'ensemble de ces principes *"sont interdépendants et se recouvrent partiellement"* (OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, Paris: OCDE, 1981, p. 32 ("Exposé des motifs").

221 Ce principe est consacré à l'article 7 des Lignes directrices de l'O.C.D.E., à l'article 5.a de la Convention du Conseil de l'Europe et à l'article 6.1.a de la Directive européenne.

222 Voir K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, p. 165; U.U. Wuermeling, *supra* note 119, p. 437: *"it could, in some cases, cover the principle of open and direct collecting. For example the collecting of data from children of the subject could be treated as unfair"*; M.H. Boulanger et C. de Terwangne, *supra* note 186, *ibid*: "Ainsi, au Québec, on a remarqué que l'accès à certains serveurs s'adressant plus particulièrement aux enfants pouvait être conditionné par la fait de compléter un questionnaire relatif à leurs habitudes de vie ou à celles de leurs frères et soeurs ou de leurs parents".

ce, afin d'assurer le respect de la protection mise en oeuvre par la Directive.

ii) Spécification des finalités[223]

Ce principe exige que les données à caractère personnel ne soient collectées que pour des finalités précises, explicites[224] et légitimes. C'est dès avant la mise en oeuvre d'un traitement et au plus tard au moment de la collecte[225], que la finalité doit être déterminée[226]. La légitimité de la finalité est laissée à l'appréciation des parties[227], sous réserve du contrôle du juge ou d'une autorité de contrôle ad hoc.

Outre l'exigence de légitimité, le principe de finalité implique également que toute

---

223 Article 9 des Lignes directrices de l'O.C.D.E. , article 5.b de la Convention du Conseil de l'Europe et article 6.1.b de la Directive européenne.

224 U.U. Wuermeling, *supra* note 119, p. 437: "*The commission gives, as an exemple, that the description "for commercial purposes" would be too broad*"; (CE, *Explanatory Memorandum of the Commission of the European Communities*, COM (92) 422 final - SYN, p. 15).

225 K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, p. 167.

226 Puisqu'une notification reprenant notamment la ou les finalités du traitement doit être adressée à l'autorité de contrôle "*préalablement à la mise en oeuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une finalité ou des finalités liées*" (articles 18 et 19 de la Directive européenne).

227 L'article 7 de la Directive européenne précise que le traitement des données à caractère personnel n'est légitime qu'avec le consentement de la personne concernée à moins qu'il soit nécessaire à l'exécution d'un contrat ou de mesures précontractuelles prises à la demande de la personne concernée ou s'il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou à la sauvegarde de l'intérêt vital de la personne concernée. En outre, la communication de données à caractère personnel à une personne physique ou morale et à une autorité publique n'est licite que si elle est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le(s) tiers auxquel(s) les données sont communiquées ou à la réalisation de l'"*intérêt légitime*" poursuivi par le(s) tiers auxquel(s), les données sont communiquées, à condition que l'intérêt de la personne concernée ne prévale pas (article 6 (1) (b)). Sur l'expression "*intérêt légitime*" sujette à de multiples interprétations, voir J. Thyraud, "Commentaire article par article du projet de proposition de directive du Conseil des Communautés européennes à l'égard du traitement des données à caractère personnel", Conférence annuelle des commissaires à la protection de la vie privée, Paris, septembre 1990, p. 3.

utilisation des données soit compatible avec la finalité annoncée lors de la collecte des données[228]. La Directive ne précise pas ce qu'il faut entendre par *"utilisation compatible"* mais il semble que ces termes doivent être compris dans le sens d'une *utilisation correspondant à l'attente raisonnable des personnes concernées"* au vu de la finalité première annoncée[229]. Entrent également dans la notion d'attente raisonnable, les opérations effectuées sur les données en application de textes de loi[230].

Si les opérations effectuées ne sont pas compatibles avec l'objectif initial, il faut considérer qu'il s'agit d'un nouveau traitement de données dont il convient d'informer les personnes concernées. La nouvelle finalité doit, à son tour, être légitime.[231]

---

228 Article 6. 1. b de la Directive européenne.

229 *"Dans le cas où un auteur publie des articles par le biais d'un site Internet offrant cette possibilité, il peut raisonnablement s'attendre à ce que le gestionnaire du site utilise ses coordonnées pour le tenir au courant des manifestations (colloques, conférences, rencontres) organisées sur le thème traité, ou pour les transmettre à des éditeurs scientifiques. Celui qui recourt à des services bancaires peut raisonnablement s'attendre à ce que l'organisme bancaire utilise ses données personnelles pour le faire bénéficier d'opérations de marketing concernant les produits ou services financiers offerts par la banque en question. L'utilisateur d'Internet qui s'adresse à un fournisseur d'accès pour pénétrer dans le réseau peut s'attendre à ce que le fournisseur d'accès utilise les données se rapportant à ses interrogations pour lui proposer des conditions spéciales d'abonnement tenant compte, par exemple, de la fréquence des appels. Ces utilisations secondaires doivent donc être considérées comme compatibles avec les finalités initiales des traitements"* (M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 15).

230 Lois pénales ou fiscales, par exemple. *"Ainsi, l'individu qui ouvre un compte en banque doit s'attendre à ce que les données relatives à ce compte soient communiquées aux autorités compétentes si une enquête à son égard est menée pour cause de suspicion de participation à des opérations de blanchiment d'argent"* (M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 15).

231 *"Ainsi, les coordonnées des abonnés téléphoniques sont reprises dans les annuaires dans le but de permettre l'identification du numéro d'appel d'un correspondant recherché. La vente de ces coordonnées par l'organisme de télécommunications à des sociétés privées à des fins de (télé)-marketing correspond à un traitement différencié car il s'agit d'une utilisation incompatible avec la finalité première; Elle doit donc être notifiée aux abonnés"* (M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 15.

Ce principe se rapproche du principe de qualité et de proportionnalité[232], selon lequel la collecte de données personnelles doit être limitée à ce qui est strictement nécessaire, c'est-à-dire pour des objectifs socialement acceptables, à l'exception des données "*sensibles*", c'est-à-dire celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que les données relatives à la santé et à la vie sexuelle. Compte tenu des risques inhérents à ces données[233], la légitimité de la finalité doit s'apprécier de façon rigoureuse afin que le traitement de ces données sensibles soit limité à des situations précises[234]. En terme de transfert, la nature de ces données crée ainsi des exigences à l'égard du niveau de protection requis.

Ce principe prévient enfin le cas où l'organisme collecteur viendrait à modifier indûment les finalités pour lesquelles les données personnelles ont été collectées[235].

iii) Limitation de l'utilisation[236]

Ce principe exige la limitation de l'utilisation des données à caractère personnel aux seuls traitements dont les finalités sont compatibles avec les finalités qui ont été

---

232 M.D. Kirby, *supra* note 118, p. 42; *infra, iv) Qualité et proportionnalité des données.*

233 M.P. Roch, *supra* note 116, p. 83: "*The data subject must have given written permission for the processing of these data. Religious, political, and similar organizations may, of course, continue to keep a member data base, provided that such data are not disclosed to third parties. In addition, data concerning criminal convictions may only be kept by "judicial and law-enforcement authorities".*

234 Article 6 de la Convention du Conseil de l'Europe et article 8 de la Directive européenne qui limite le traitement de données sensibles à certaines circonstances particulières; pour plus de développements, voir U.U. Wuermeling, supra note 119, p. 435; Th. Zerdick, *supra* note 121, p. 67.

235 Tel que dégagé par le Juge Kirby; *infra, iii) limitation de l'utilisation.*

236 Article 10 des Lignes directrices de l'O.C.D.E., article 5.b de la Convention du Conseil de l'Europe et article 6.1.b de la Directive européenne.

déterminées, rendues explicites et légitimes lors de la collecte initiale ainsi que la non-communication des données à autrui, même pour des fins compatibles (confidentialité)[237] sauf si la personne concernée y consent ou si une règle de droit le permet pour des raisons tenant à la gestion administrative, aux nécessités judiciaires, de poursuites ou d'enquêtes[238]. En termes de transfert de données vers des pays tiers, ce principe se traduit par l'obligation faite au responsable du traitement que les données ne soient transférées que pour une finalité légitime et déterminée et qu'elles ne soient réutilisées[239] ou communiquées que dans une mesure compatible avec le transfert initial.

iv) Qualité et proportionnalité des données[240]

En vertu de ce principe, les données traitées doivent être limitées aux seules données nécessaires à la réalisation de la finalité poursuivie. Les données doivent en effet être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles ont été collectées et sont utilisées. Par ailleurs, ces données doivent être exactes et, si nécessaire, mises à jour par le responsable du traitement, en particulier dans le cadre des processus décisionnel.

---

237 K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, p. 167: "*ce critère de compatibilité, proposé par les Lignes directrices de l'OCDE et la Convention européenne, doit certainement s'apprécier à la lumière de toutes les circonstances et reposer sur une analyse de la raisonnabilité de lien entre les anciennes et les nouvelles finalités*".

238 M. D. Kirby, *supra* note 118, p. 55.

239 "*Un exemple significatif est celui du prestataire de télé-achat qui collecte des données sur les utilisateurs du service qu'il propose. Il pourrait s'en servir, d'une part, pour opérer la transaction de télé-achat et, d'autre part, pour mieux cibler les consommateurs en fonction des produits qu'il pourrait leur proposer, ou encore, pour revendre des listes de consommateurs intéressés par tel ou tel produit à des sociétés de marketing*" (P. Thomas et M.H. Boulanger, *supra* note 2, p. 225, n° 15).

240 Article 8 des Lignes directrices de l'O.C.D.E., article 5.c et 5.d de la Convention du Conseil de l'Europe et article 6.1.c et 6.1.d de la Directive européenne.

Ce principe complète également celui de la participation individuelle par lequel l'individu concerné se voit reconnaître un droit d'accès et de rectification.

v) Garanties de Sécurité[241]

Les mesures de sécurité mises en oeuvre dans le pays de destination doivent permettre de garantir une certaine protection contre la destruction accidentelle ou non autorisée, la perte accidentelle, ainsi que contre l'accès, la modification, ou la diffusion non autorisés. Ces mesures sont en effet de nature à assurer la qualité des données. Comme on l'a en effet observé[242], *"l'effacement, la perte, la destruction criminelle ou la modification erronée des données personnelles peuvent porter atteinte au citoyen fiché, la prise de décision, aboutissement ultime de l'utilisation des renseignements, risque en effet d'être affectée par des données erronées ou en raison simplement de l'absence de données"*.

Les mesures de sécurité d'ordre matériel tels que le verrouillage des portes et les cartes d'identification), structurel (tel que les niveaux d'accès aux données) et informationnel (tel que le cryptage et la surveillance) sont souvent tributaires de l'avancée technologique du pays concerné[243]. Certains pays peuvent souffrir d'un retard technologique tel qu'il y est difficile, voire impossible, d'y assurer la sécurité et la confidentialité des données, le transfert de données s'en trouvant d'autant altéré.

---

241 Article 11 des Lignes directrices de l'O.C.D.E., article 7 de la Convention du Conseil de l'Europe et article 17 de la directive européenne

242 K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, p. 169.

243 U.U. Wuermeling, supra note 119, p. 450: *"The controller must choose a level of security having regard to the state of art and the cost of their implementation. Further, the "state of art" must be defined on a European Union level. Otherwise, it would cause different levels of protection in the Member States. A European Union -wide definition of the "state of art" might be given by security guidelines prepared by the Commission based on the decision on information technology security"*.

vi) Transparence[244]

Le traitement de données à caractère personnel, en particulier dans un contexte de réseaux ouverts[245], signifie un risque de perte de contrôle de la personne concernée sur ses propres données. Une certaine protection peut cependant être obtenue grâce au principe de transparence dans le traitement des données qui repose sur la connaissance par la personne concernée, de l'identité du responsable du traitement, des finalités et de leur éventuel changement ainsi que de leur éventuel transfert vers un pays tiers.

Ce droit d'information va plus loin que celui prévu par les Lignes directrices de

---

[244] Article 8 de la Convention du Conseil de l'Europe, article 12 des Lignes directrices de l'O.C.D.E. et articles 10 et 11 de la Directive européenne. Ce dernier article prévoit que lors de la première communication des données à autrui, le responsable du traitement, sauf exception clairement délimitée l'obligation d'informer la personne concernée de cette communication ainsi que de la finalité du traitement et des catégories de données sur lesquelles il porte. La personne concernée peut alors s'objecter à la communication ou à tout autre traitement pour des raisons légitimes tenant à sa situation particulière, sauf en cas de disposition contraire du droit national. Le responsable du traitement est alors tenu de cesser le traitement contesté (article 14 de la Directive européenne).

[245] Voir M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 15: "*La maîtrise par chacun des informations qui le concernent et du sort qui leur est réservé risque fort (...) d'être plus virtuelle que réelle. Vu le nombre d'acteurs qui interviennent dans un réseau ouvert (...) et les possibilités de réutilisation des données disponibles, comment réellement contrôler qui détient l'information et dans quel but elle est utilisée ? Comment connaître l'identité de tous ceux qui téléchargent les données à caractère personnel présentes sur les sites ? Et surtout, comment vérifier que les traitements effectués par ces personnes sont compatibles avec les finalités de départ ou que leurs finalités nouvelles sont légitimes ?*

Par ailleurs, on constate en contrepartie que, par ses possibilités techniques, Internet permet d'informer les personnes concernées à bien moindre coût et bien plus rapidement (...). D'autre part, la présentation des sites peut être configurée de telle sorte que l'information relative au responsable du traitement et aux finalités poursuivies apparaisse d'entrée de jeu sur l'écran. En outre, les possibilités d'interactivité donnent au consentement des personnes concernées une portée nouvelle, dans la mesure où ces dernières peuvent moduler leur consentement à voir les données enregistrées et traitées, en fonction des opérations qu'elles veulent effectuer sur le site visité et au fur et à mesure de leurs investigations. Elles peuvent déterminer les utilisations des données qu'elles acceptent, en cochant les cases correspondant aux utilisations consenties ou refusées parmi une liste proposée au départ de la consultation, par exemple. L'interactivité donne aux techniques d'opting-in ou d'opting-out une dimension immédiate et effective. La notion de consentement elle-même prend une signification nouvelle".

l'O:C.D.E., la Convention du Conseil[246] et nombre de législations nationales[247], puisqu'il existe même lorsque les données n'ont pas été collectées auprès de la personne: celle-ci devra être informée de l'identité du responsable du traitement et des finalités poursuivies *"dès l'enregistrement des données ou au plus tard lors de la première communication des données à un tiers"*, sauf si elles ont été collectées *"à des fins de statistique, de recherche historique ou scientifique ou si l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés"*[248].

Le principe de transparence implique également la possibilité pour la personne concernée de savoir si des informations à son sujet sont traitées par un responsable de traitement visé et d'obtenir, sur son initiative, une copie - sous forme compréhensible - des données faisant l'objet du traitement et d'en obtenir, le cas échéant, la rectification, l'effacement ou le verrouillage[249]. La Directive comporte une disposition originale par rapport aux conventions internationales et à la plupart des législations nationales antérieures: elle reconnaît le droit à la personne concernée de connaître l'origine des données enregistrées[250].

vii) Participation individuelle

Ce principe résulte de la nécessité pour la personne concernée d'obtenir une information sur les données traitées par le responsable du traitement et d'exercer un certain contrôle

---

246 Voir U.U. Wuermeling, supra note 119, pp. 443-444; M. P. Roch, *supra* note 116, p. 74.

247 Telle la loi française (H. Maisl, *supra* note 198, p. 44).

248 Article 11 de la Directive européenne; sur les exceptions au droit d'information (article 13 de la Directive européenne), voir U. U. Wuermeling, *supra* note 119, pp. 447-448.

249 Article 13 des Lignes directrices de l'O.C.D.E., article 8 de la Convention du Conseil de l'Europe et article 12 de la Directive européenne.

250 Article 12.a de la Directive européenne; voir U.U. Wuermeling *supra* note 119, p. 446.

sur son "*image informationnelle*", via un droit d'accès[251] et de rectification[252]. Cette double perspective est la pierre angulaire des législations nationales ou européennes de protection des données personnelles[253].

La Directive européenne porte le principe de la participation individuelle au-delà de la connaissance par la personne concernée des données et, le cas échéant, de leur rectification, et permet, dans certains cas (en particulier, lorsque la légitimité d'un traitement est contestable), une participation à la décision de traitement, soit sous la forme d'un consentement préalable, soit sous la forme d'une opposition[254].

- Le consentement

Il s'agit d'offrir aux individus le choix de donner, négocier ou refuser leur consentement, lors de la collecte, au traitement d'une ou de plusieurs données les concernant. Ce consentement doit être libre et "*éclairé*"[255], ce qui signifie que la

---

[251] Qui doit être aisé, sans délai excessif et, s'il n'est gratuit, à un prix raisonnable; voir U.U. Wuermeling *supra* note 119, pp. 446-447.

[252] Le principe de la transparence peut être considéré comme une condition préalable au principe de la participation individuelle (OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, supra* note 220, p. 35 ("Exposé des motifs").

[253] K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, p. 173; O.C.D.E., *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données decaractère personnel, supra* note 220, p. 36.

[254] Articles 7 et 14 de la Directive européenne.

[255] L'article 2 h) de la Directive européenne définit le "*consentement de la personne concernée*" comme "*toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement. Un consentement ne sera informé que si la personne concernée dispose des informations suivantes: les finalités du traitement et les catégories de données collectées, le cas échéant, l'identité du responsable du traitement ou son représentant, de même que le destinataire des données personnelles et l'existence d'un droit d'accès aux données le concernant et de*

personne concernée doit avoir une connaissance suffisamment précise de tous les éléments inhérents au traitement[256]. Le consentement répond au risque lié au contrôle des finalités[257] dans la mesure où en accordant son consentement, l'individu prend connaissance des finalités du traitement, participant par là-même à leur détermination et leur contrôle.

- L'opposition

La possibilité est offerte aux personnes concernées de s'opposer, pour des motifs légitimes[258], au traitement de certaines données les concernant[259]. Cette opposition sera exercée soit *a priori*, lors de la collecte par la signification du refus, soit *a posteriori* après avoir eu connaissance de l'existence d'un traitement.

---

rectification de ces données". La proposition de Directive précisait que ce consentement peut être retiré à tout moment sans toutefois entraîner d'effets rétroactifs (CE, *Proposition (CEE)de Directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Exposé des motifs)*, *supra* note 179, p. 20.

256 Soulignons que la plupart des législations nationales prévoient déjà l'obligation de mentionner dans la notification d'un traitement de données à caractère personnel auprès de l'autorité de contrôle, la (les) finalité(s) du traitement, les catégories de données collectées, l'identité du maître du fichier ou, le cas échéant, du gestionnaire des données et l'existence d'un droit d'accès et de rectification ainsi qu'en cas de transfert, même occasionnel, à l'étranger, les catégories de données concernées et, pour chacune d'elles, le pays de destination.

257 *Supra, ii) spécification des finalités.*

258 L'exposé des motifs de la proposition de Directive précisait à cet égard que *"les raisons légitimes visées dans cette disposition sont l'absence d'une justification légale d'un certain traitement des données à caractère personnel, par exemple parce que les conditions (...) du projet de directive concernant la légitimité de ce traitement ne sont pas remplies pour un traitement de données déterminé"* (CE, *Proposition (CEE) de Directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Exposé des motifs)*, *supra* note 179, p. 29); U.U. Wuermeling, *supra* note 119, p. 448: *"The COE Convention gives the right to obtain if the data have been processed contrary to law. The UN Guidelines grant the right to object if the processing is unlawful, or not necessary. The OECD regulation is unclear, because the right to object is granted if the "challenge is successful". That would only be the case if the processing is unlawful"*.

259 Notamment à des fins de prospection; l'article 14.b de la Directive européenne prévoit en effet un droit d'opposition sans justification dans le domaine du marketing.

viii) Responsabilité[260]

Toute personne (*"Responsable du traitement"*) effectuant, au sein d'un organisme public ou d'une entreprise, un traitement sur des données à caractère personnel[261] doit pouvoir être tenue responsable du dommage subi par la personne concernée suite à un traitement illicite ou une action incompatible avec les principes fondamentaux de protection des données[262]. Ce principe est donc le corollaire du principe de transparence: l'identification préalable du responsable ultime des traitements *"a aussi pour but d'éviter aux divers responsables d'une institution publique ou d'une entreprise d'obvier à leurs obligations en prenant prétexte de l'organigramme de leur mandant"*[263], privant la personne concernée de l'exercice de ses droits. Le principe de responsabilité implique également la possibilité pour tout individu d'exercer un droit de recours en cas de dommage ou de méconnaissance de ses droits, afin que des sanctions appropriées soit

---

[260] Article 14 des Lignes directrices de l'O.C.D.E., articles 8.d et 10 de la Convention du Conseil de l'Europe et articles 22 et 23 de la Directive européenne.

[261] OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, *supra* note 220, p. 37: *"le maître du fichier décide du choix des données et des activités de traitement de l'information. C'est pour son compte que les données sont traitées. En conséquence, il est essentiel qu'aux termes du droit interne de la responsabilité devant la loi, du respect des règles et des décisions concernant la protection de la vie privée incombe au maître du fichier, qui ne devrait pas être relevé de cette obligation pour la simple raison que le traitement des données est effectué pour son compte par un tiers, tel qu'un centre de traitement à façon"*.

[262] U.U. Wuermeling, supra note 119, p. 451: *"There are three main questions arising with regard to liability clauses: first, whether the liability is a strict liability or whether there is a special exemption; second, what sort of damage is covered; and third, if there is any limitation on the amount of compensation. The liability clauses in the Directive (...) provides strict liabilities. However, there is a possibility for the user to prevent the liability if he proves that he has taken reasonable care. (...) Under the Directive it is left to the Member States to decide whether they want to grant the possibility for such an exemption if a user can prove that he is not responsible for the event giving rise to the damage"*; sur les devoirs du responsable du traitement et sa responsabilité à l'égard de l'autorité nationale de protection des données, voir M.P. Roch, *supra* note 116, p. 81 et s.

[263] K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, p. 172 citant M.D. Kirby, *supra* note 118, p. 60.

adoptées[264].

ix) Détention limitée[265]

La durée du traitement est limitée par le principe même de finalité[266]. Les données ne peuvent en effet être conservées *"sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles ont été initialement collectées ou pour lesquelles elles sont traitées ultérieurement"*[267].

La durée de conservation des données liée à leurs finalités permet ainsi d'éviter la création d'immenses banques de données qui, dépassées et non corrigées, pourraient poursuivre indéfiniment la personne concernée et la pénaliser. Comme on l'a observé[268], certaines données préjudiciables, telles les condamnations pénales, *"doivent aussi disparaître au nom du droit à l'oubli"*.

2 - Autres critères

La Directive européenne identifie un certain nombre de *"traitements à risques"* requérant un niveau de protection plus adéquat, notamment en ce qui concerne leur transfert vers un Etat tiers à l'Union européenne.

---

264 *Infra*, Sous-paragraphe 2 - Règles d'effectivité.

265 Article 8 des Lignes directrices de l'O.C.D.E., article 5.e de la Convention du Conseil de l'Europe et article 6.1.e de la Directive européenne.

266 L'article 25.2 de la Directive européenne mentionne conjointement *"la finalité et la durée du ou des traitements envisagés"*.

267 Article 6.1.e de la Directive européenne.

268 K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, p. 171 citant la CNIL, *Dix ans d'informatique et libertés*, Paris, Economica, 1988, p. 18 ("Bilan de la CNIL").

Le lien existant entre les différents acteurs impliqués dans le transfert de données vers un pays tiers, influencera le niveau de risque lié au transfert lui-même. Si le flux s'inscrit dans le cadre d'une relation commerciale ou professionnelle générale ou dans le cadre de relations entre une société-mère et ses filiales, le risque de perte de contrôle par la personne concernée de ses propres données semble moindre dès lors qu'il est possible de retrouver la trace de ses données auprès du responsable du traitement européen. Les finalités, telle la gestion du personnel ou de la clientèle pour une société et ses filiales, sont également souvent liées entre elles.

En revanche, certaines circonstances influenceront le risque lié au transfert et auront ainsi une incidence sur le niveau de protection requis d'un pays tiers. Ainsi, le marketing direct, activité commerciale par laquelle l'individu peut recevoir une lettre d'une personne qu'il n'a jamais rencontrée et à qui il n'a jamais donné ses coordonnées[269], soulève de délicates questions relatives à l'absence de protection existante des données à caractère personnel. Un niveau de protection jugé comme "*adéquat*" pourrait exiger que toute utilisation de données personnelles à des fins de marketing direct implique le droit pour la personne concernée de s'y opposer[270].

De même, l'article 15 de la Directive européenne accorde une protection particulière à la personne concernée lorsque ses données personnelles font l'objet d'une *"décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains*

---

[269] H.M., "Marketing direct et données personnelles, définition d'une déontologie", (1995) D.I.T., p. 72: *"on entendra ici par marketing direct toute technique de marketing-communication, personnalisée, utilisant des fichiers ou bases de données nominatives , en vue d'établir un dialogue interactif et mesurable avec une cible identifiée"*.

[270] Comme indiqué (*supra*, I - Principes de base de la protection, *vii) Participation individuelle*); ce droit est consacré à l'article 14.b de la Directive européenne.

aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc". Ainsi, lorsque l'objectif du transfert des données vers un pays tiers est précisément de prendre une décision individuelle automatisée, une protection particulière devrait être accordée à l'individu afin de protéger ses intérêts légitimes[271].

Enfin, l'article 25.2 de la Directive européenne identifie un certain nombre de facteurs à prendre en considération lors de l'évaluation de l'adéquation de la protection dans un pays tiers, qui influencent le niveau de protection requis:

- de l'Etat de destination finale

Une protection considérée comme "*adéquate*" peut être privée d'effet si le pays tiers offrant cette protection permet le transfert ultérieur des données vers un autre Etat qui en est dépourvu. Le risque de voir certains pays tiers dotés d'un niveau de protection adéquats être utilisés comme simples lieux de transit des données, devrait toutefois être limité dans la mesure où le pays tiers analysé doit être le pays de destination finale des données. En pratique, il n'est cependant pas toujours évident d'identifier l'Etat de destination finale, en particulier dans le contexte de réseaux ouverts[272].

En outre, après avoir été considéré comme un pays de destination finale, un pays tiers peut être amené à transférer des données vers un troisième pays de manière parfaitement légitime. Il convient dès lors que des mécanismes de protection du pays tiers règlent cette question, en conditionnant les transferts vers un autre Etat à l'engagement par ce dernier d'une protection qui puisse également être considérée comme "*adéquate*" aux termes de l'article 25 de la Directive européenne pour le type de transfert envisagé.

---

[271] Pour plus de développements, voir U.U. Wuermeling, supra note 119, p. 449.

[272] M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 17 et s.

Cette condition semble en effet la seule garante d'une protection réellement adéquate.

- de l'Etat d'origine

En ce qui concerne les données provenant des Etats membres à destination de pays tiers, la Directive européenne requiert que les Etats membres adoptent une position commune quant à la protection offerte par ces pays. On peut toutefois douter de l'influence que le pays d'origine des données pourrait exercer sur le niveau de protection requis par un pays tiers. En revanche, si les données proviennent d'un pays tiers, le critère prend son sens. En effet, certaines données auraient notamment pu être collectées sans le consentement de la personne concernée, ce qui n'aurait pas été permis si la Directive avait été d'application.

Sous-paragraphe 2 - Règles d'effectivité

Une fois les risques identifiés et les principes de base déterminés, il reste à s'assurer qu'ils trouvent une mise en œuvre concrète[273]. Il n'est pas possible de décrire, dans le cadre de la présente étude, toutes les règles d'effectivité de la protection. Il s'agit plutôt d'établir des points de repères pour leur évaluation et d'analyser les conditions dans lesquelles elles peuvent garantir *in concreto*, pour les personnes concernées, le respect des principes de base.

Est ainsi recherchée la reconnaissance de certains droits pour la personne concernée, consacrés par un instrument porté à la connaissance des responsables du traitement et des intéressés et susceptibles d'un recours en cas de non-respect.

1 - Instrument créateur de droits

---

[273] L'article 25.2 précité de la Directive européenne précise en effet "*les règles de droit, générales ou sectorielles, (...) qui y sont* ***respectées***".

La Directive européenne vise essentiellement à protéger la personne concernée et à lui assurer une certaine maîtrise de son "*image informationnelle*". Cette protection est mise en oeuvre, d'une part, en accordant un certain nombre de droits à la personne concernée (droit d'accès, de rectification, d'opposition, etc.) et, d'autre part, en imposant au responsable du traitement une série d'obligations (d'information, de notification, de sécurité, de qualité des données, etc.). Le régime de protection mis en place par un pays tiers doit donc être créateur de droits à l'égard de la personne concernée.

Quant aux instruments permettant d'assurer cette protection, l'article 25.2 précité de la Directive européenne énumère de façon non limitative: "*les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées*".

La Directive européenne n'entend donc pas réserver la source de la protection adéquate au seul modèle législatif. Il peut s'agir aussi bien d'une loi globale ou sectorielle, d'un règlement administratif, d'une coutume ou d'une normalisation technique des codes de conduite sectoriels ou propres à une entreprise. Un pays tiers ne disposant pas de loi générale de protection des données, peut ainsi assurer une protection adéquate par des règles professionnelles ou des codes de conduite (sous certaines conditions[274]), ou même par une "*privacy policy*"[275] pour autant que l'engagement explicite du responsable du traitement et le degré de précision des protections offertes créent unilatéralement ou contractuellement un droit pour les personnes concernées ou leurs représentants d'agir devant les juridictions[276]. En outre, des sanctions prises par une autorité indépendante

---

[274] *Infra*, Chapitre 3 - Les codes de conduite, Section 1 - la Directive européenne.

[275] Une "*privacy policy*" s'entend de la déclaration publique faite individuellement par un responsable du traitement, contenant les principes de protection des données qui sont suivis par le responsable du traitement.

[276] Office of Fair Trading aux Etats-Unis, par exemple.

peuvent réprimer le non-respect d'une "*privacy policy*".

Il convient donc de ne rejeter *a priori* aucun de ces instruments, définis de façon non exhaustive, mais à en évaluer soigneusement l'effectivité en tenant compte des traditions culturelles et juridiques non européennes. Leur adéquation dépendront de l'existence de certains droits pour la personne concernée, de la légitimité de leur auteur et de leur caractère contraignant.

2 - Publicité

L'effectivité de la protection mise en place dans un pays tiers dépend largement de la possibilité pour le responsable du traitement, d'une part, et les personnes concernées, d'autre part, de prendre connaissance de leurs droits et obligations respectifs. Une connaissance efficace est généralement assurée par la publicité de l'instrument créateur de droits.

La forme de publicité importe peu, pourvu qu'elle le soit dans un langage compréhensible[177] pour les intéressés, ce qui leur permettra également de contrôler le respect de leurs droits par le responsable du traitement[178].

3 - Possibilité de recours et sanctions

Si la Directive européenne témoigne d'une large ouverture dans l'acception de la source utilisée pour assurer une protection adéquate, elle exige néanmoins que cette protection soit effectivement appliquée. Les sanctions réprimant un non-respect des principes

---

[177] Par exemple, une "*privacy policy*" dont le texte est distribué aux guichets des agences du responsable du traitement.

[178] Lorsqu'un responsable de traitement adopte et publie un code de conduite ou une "*privacy policy*", il lui devient difficile d'enfreindre ce code publiquement ou à l'insu des personnes concernées.

consacrés par cette source, doivent donc être prévues pour que puisse s'exercer, le cas échéant, le recours de la personne concernée. L'adéquation de la protection pourrait également dépendre de l'existence de moyens de contrôle garantissant directement ou indirectement le respect des principes fondamentaux (existence d'une autorité de contrôle, nomination d'un *"détaché à la protection des données"*, etc.).

Les moyens de sanction s'entendent, au sens large, des diverses procédures de dissuasion, de réparation ou de répression mises en place pour combattre les déviances aux comportements attendus pour assurer le respect des droits reconnus[279].

Ainsi, les modes de sanction privilégiés par la Directive européenne, c'est-à-dire les sanctions judiciaires, civiles ou pénales, ne doivent pas en faire oublier d'autres, tels l'amende administrative, l'exclusion d'une association, le refus d'un certificat, le boycottage d'une société, la recommandation, la menace de saisine des autorités administratives, etc., en provenance d'acteurs divers et dont l'efficacité est parfois supérieure à celle des sanctions classiques.

En outre, la sanction judiciaire ne se réduit pas au seul prononcé de condamnations pénales ou de dommages et intérêts à titre de réparation. Elle peut également s'accompagner de mesures de publicité, d'interdiction de traitement, de verrouillage, d'effacement ou de destruction de données.

Il est essentiel que la personne concernée puisse recourir, sans coût excessif, aux procédures institutionnalisées mises en place afin d'obtenir la reconnaissance et le

---

[279] U.U. Wuermeling, supra note 119, p. 450: " *(...) Article 10 of the COE Convention (...) requires Member states to establish appropriate sanctions and remedies for breach of domestic data protection legislation. The O.E.C.D. Guidelines recommend that States make provisions for sanctions and remedies not only to ensure the protection of personal data - like the COE Convention - but also to deter actions which may interfere with their free circulation* ".

respect de ses droits.

L'effectivité se conçoit d'une combinaison de ces trois critères. L'instrument a pour objet d'assurer le versant "*général*" de l'effectivité (affirmation et mise en oeuvre des principes), la publicité vise à assurer une prise de connaissance effective des droits énoncés par l'instrument, tandis que les moyens de contrainte et de recours visent tant la prévention[280] que la résolution des problèmes individuels.

Paragraphe 3 - Autorisation

Conformément à l'article 25 de la Directive européenne, l'évaluation - au cas par cas - de l'adéquation de la protection offerte par les pays tiers et la prise de décision quant à l'autorisation d'un transfert déterminé ou d'une catégorie de transfert reposent en première instance sur les Etats membres et sur la Commission européenne.

La Directive ne précise pas quelle autorité sera chargée de l'évaluation. Le pouvoir décisionnel devrait donc revenir à l'agence de protection des données au sein de chaque Etat membre puisque celle-ci connaît des traitements de données, y compris les transferts à destination de pays tiers, effectués sur son territoire[281]. Eu égard au nombre de transferts de données à caractère personnel à destination de pays tiers, ainsi qu'au nombre d'acteurs impliqués dans ces transferts, aucun Etat membre, quelle que soit la

---

[280] Les sanctions peuvent en effet exercer un effet dissuasif qui les renvoie au premier objectif.

[281] La Directive européenne prévoit en effet un régime de notification préalable à la création des traitements à l'autorité de contrôle, assorti de deux exceptions: l'exonération ou la simplification de la déclaration lorsqu'il existe dans l'organisme en cause un "*détaché à la protection des données*" (solution inspirée du droit allemand), le contrôle préalable pour les traitements susceptibles de présenter des risques particuliers, qu'ils émanent du secteur public ou privé (H. Maisl, *supra* note 198, p. 44); pour plus de développements, voir M.P. Roch, *supra* note 116, p. 71; U.U. Wuermeling, supra note 119, p. 453 et s.; C. Millard et R. Carolina, *supra* note 187, p. 280.

manière dont il choisit de mettre en oeuvre l'article 25 de la Directive européenne, ne pourra garantir que chaque demande d'autorisation de transfert soit examinée en détail. Les Etats membres pourraient donc rationaliser leur évaluation en mettant en place des mécanismes de prise de décisions, même temporaires, à l'égard de plusieurs transferts.

De tels mécanismes visant non seulement à uniformiser l'évaluation des Etats membres mais encore à leur simplifier autant que possible la prise de décision, sont prévus par la Directive européenne. Ils ont pour objet d'identifier les pays tiers au sein desquels la protection des données personnelles peut être considérée comme adéquate afin d'autoriser toutes ou certaines catégories de transferts envisagées[282].

A cet égard, l'article 25.6 de la Directive européenne établit une procédure qualifiée de "*constatation*" par laquelle la Commission européenne établit des "*white lists*" de pays tiers considérés comme assurant une protection adéquate, en raison de leur législation interne ou de leurs engagements internationaux[283].

Ces "*white lists*" devraient cependant être constituées avec une extrême prudence et n'être que provisoire ou émise à titre d'indication, sans préjudice de cas présentant certaines spécificités. En d'autres termes, l'inclusion d'un pays dans cette liste devrait s'opérer sur la base d'évaluations de cas particuliers plutôt que sur la base d'une

---

[282] Pour tous les transferts de données médicales, par exemple.

[283] La question se pose de savoir quels engagements internationaux sont visés ici. Si la ratification de la Convention du Conseil de l'Europe paraît constituer une présomption de protection adéquate (dans la mesure où elle implique que les pays concernés aient adopté une législation protectrice), il n'en est sans doute pas de même pour l'adhésion aux Lignes Directrices de l'O.C.D.E., dont la force contraignante est moindre; *supra*, Section 1 - Les Lignes directrices de l'O.C.D.E. et la Convention du Conseil de l'Europe.

évaluation abstraite de textes légaux[284]. Une difficulté peut en effet se présenter pour les pays n'offrant pas une protection uniforme dans tous les secteurs public et privé ou pour les pays fédéraux dont la protection diffère entre entités fédérées. Par ailleurs, l'absence de mention d'un pays tiers sur une "*white list*" ne devrait pas signifier d'office que la protection offerte par ce pays est inadéquate mais plutôt qu'aucun avis n'a encore été émis officiellement à ce sujet.

Outre ces mécanismes fédérateurs, l'article 25.3 de la Directive européenne impose aux Etats membres et à la Commission de "*s'informer mutuellement*" lorsque l'un d'eux estime que le niveau de protection n'est pas adéquat. La constitution de "*black lists*" de pays tiers, quel que soit le transfert envisagé, peut donc s'en trouver favorisée[285], les Etats membres étant alors invités à prendre toutes les mesures nécessaires pour empêcher tout transfert vers ces pays dont la protection est considérée comme inadéquate. L'article 25.4 de la Directive ne précisant pas de quelles mesures il est question ici, il pourra s'agir tant d'une norme législative interdisant ce type de transfert que de sanctions (amendes, etc.) en cas de violation de l'interdiction.

La Commission peut, quant à elle, engager des négociations avec ces pays afin de remédier à cette inadéquation ou constater qu'un pays tiers assure un niveau de protection adéquat "*en raison de la législation interne ou de ses engagements internationaux*"[286]. L'objectif de la Directive européenne n'est pas en effet d'exporter

---

[284] L'article 25 prône d'ailleurs une approche au cas par cas (*supra*, Paragraphe 1 - Evaluation).

[285] U.U. Wuermeling, supra note 119, p. 453: "*(...) the Commission will prepare a negative list of transfers for negotiations about regulations to secure adequate protection. Some countries might not able to meet the requirement for all transfers*"; voir à ce sujet, J.R. Reidenberg, "Data Protection Measures in the United States", (1995) 80 Iowa L. R., p. 497.

[286] Article 25.6 de la Directive européenne. Cette dernière disposition ne définit cependant pas les termes "*législations*" et "*instruments internationaux*" qui semblent se référer aux Lignes

son modèle réglementaire au-delà des frontières communautaires mais de garantir aux personnes bénéficiant au départ de sa protection, le maintien d'une protection adéquate pour les traitements de données soumis à la Directive, en particulier lorsque celles-ci sont transférées vers des pays tiers à l'Union européenne. Ainsi, le responsable d'un traitement au sein d'un Etat tiers pourrait, sans modifier les règles de protection qu'il observe habituellement, réserver aux seules personnes originairement bénéficiaires de la protection la *"protection adéquate"* prévue par l'article 25 de la Directive. Cette distinction pourrait s'effectuer tant par le biais d'un code de conduite ou d'un contrat, que par la nomination d'un représentant établi sur le territoire européen, soumis aux dispositions d'un Etat membre prises en exécution de la Directive et responsable vis-à-vis de ces bénéficiaires, sous réserve de l'effectivité de la protection assurée par ces moyens.

Soulignons que la constitution de *"white lists"* ou de *"black lists"* doit être conforme à la procédure de constatation prévue par l'article 31.2 de la Directive[287]. Ainsi, la Commission prendra des mesures appropriées en fonction des avis émis par un Comité consultatif composé des représentants des Etats membres et présidé par un représentant de la Commission[288]. Si la Commission est du même avis que le Comité, elle adoptera

---

directrices de l'O.C.D.E. et à la Convention du Conseil de l'Europe autorisant la voie de l'autoréglementation dans la mise en oeuvre des principes fondamentaux en matière de traitement et de communication des données personnelles. Comme l'a observé K. Benyelkhlef ("Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, p. 196), *"une protection éparse et diffuse, parce qu'assurée dans une multitude d'instruments législatifs (ou réglementaires, voire administratifs) ou l'autoréglementation satisfait-elle au critère de protection adéquat ?"*

[287] Cet article renvoit à l'article 14, 8, § 2, du Traité de Rome qui prévoit une procédure de vote à la majorité qualifiée.

[288] La mission de ce Comité est directement liée au pouvoir réglementaire que se réserve la Commission en vertu de l'article 27 de la Directive. L'article 31.2 dispose que *"le représentant de la Commission soumet au Comité un projet de mesures à prendre. Le Comité émet son avis sur ce projet, dans un délai que le président peut fixer en fonction de l'urgence de la question en cause"*

sans délai les mesures proposées qui seront d'application immédiate. En revanche, les mesures proposées par le Comité qui ne sont pas approuvées par la Commission, seront communiquées au Conseil qui prendra une décision à la majorité qualifiée, endéans les trois mois. A défaut, la Commission adoptera immédiatement les mesures envisagées en ne recevant l'aval ni du Comité, ni du Conseil.

Par ailleurs, est constitué un Groupe de protection des personnes à l'égard du traitement des données à caractère personnel qui, conformément à l'article 30.1.b. de la Directive européenne[289], est chargé de donner son avis sur le niveau de protection existant dans les Etats tiers. Ce Groupe à caractère consultatif et indépendant est composé d'un représentant des autorités de contrôle désignées par chaque Etat membre[290], ainsi que

---

[289] "Le groupe a pour mission:

a) d'examiner toute question portant sur la mise en oeuvre des dispositions nationales prises en application de la Directive, en vue de contribuer à leur mise en oeuvre homogène.

b) de donner à la Commission un avis sur le niveau de protection dans la communauté et dans les pays tiers.

c) de conseiller la Commission sur tout projet de modification de la présente Directive, sur tout projet de mesure additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur tout autre projet de mesures communautaires ayant une incidence sur ces droits et libertés;

d) de donner un avis sur les codes de conduite élaborés au niveau communautaire".

Le § 6 de l'article 30 oblige le groupe à établir un rapport annuel sur l'état de la protection des personnes physiques à l'égard du traitement des données personnelles dans la communauté et dans les pays tiers. Ce rapport est communiqué à la Commission, au Parlement européen et au Conseil.

[290] Il s'agit, en vertu de l'article 28 de la Directive européenne, des autorités publiques indépendantes chargées de surveiller l'application dans chaque Etat membre des dispositions prises en application de la Directive. Elles disposent, pour ce faire, de moyens d'investigations (tels les pouvoirs d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de leur mission de contrôle) et de pouvoirs effectifs d'intervention contre la constitution et l'utilisation de fichiers qui ne seraient pas conformes aux dispositions de la Directive (tels celui de rendre des avis préalablement à la mise en oeuvre du traitement et d'assurer une publication appropriée de ces avis ou la destruction de données ou

des autorités créées pour les institutions ou organismes communautaires et d'un représentant de la Commission.

L'on peut regretter que le Groupe de protection des données à caractère personnel et le Comité consultatif[291] soient rattachés, par le biais de leur présidence, à la Commission, et non au Parlement européen, créant un risque de dépendance que l'on ne peut négliger[292]. Il n'est donc pas exclu que les décisions prises soient également de nature politique[293].

Paragraphe 4 - Dérogations

L'article 26 de la Directive européenne prévoit plusieurs exceptions à l'interdiction de

---

d'interdire temporairement ou définitivement un traitement ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques). Elles disposent également du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la Directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire.

[291] Comme l'a observé K. Benyekhlef ("Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, p. 199) "*on peut se demander si la mission octroyée au Comité consultatif ne pourrait pas être remplie par le groupe de protection des données à caractère personnel. Une multiplicité d'institutions aux fonctions souvent mal définies, ne contribue certes pas à assurer l'objet ultime poursuivi par ce projet de directive, à savoir la protection de la vie privée informationnelle dans un contexte équilibreur respectant le principe de la libre circulation de l'information*"

[292] S. Simitis, "Les propositions pour une directive relative à la protection des données nominatives - une première appréciation", Conférence annuelle des Commissaires à la protection de la vie privée, Paris, septembre 1990, pp. 7-8: "*(..) mais la construction choisie par les propositions est loin d'être la seule alternative. Même si l'on se prononce pour une réduction des tâches de l'autorité prévue à des fonctions consultatives, il faut que son indépendance soit garantie. Seule une autorité clairement séparée des gouvernements nationaux et de la Commission offre la garantie d'une analyse critique et objective des développements en matière de traitement de données nominatives, de l'application des règles communautaires et des réformes nécessaires. Au lieu de l'incorporer dans la Commission, il faut la rattacher au Parlement*".

[293] On peut en effet douter que les Etats membres décident de déclarer inadéquate la protection assurée par voie réglementaire dans le seul secteur public par un partenaire commercial aussi puissant que les Etats-Unis, le Japon, l'Australie ou le Canada.

transfert de données à caractère personnel vers des pays tiers n'assurant pas un niveau de protection adéquat[294], liées à un transfert spécifique ou à l'existence de clauses contractuelles appropriées.

Sous-paragraphe 1 - Dérogations spécifiques

L'article 26 de la Directive européenne dispose que *"par dérogation à l'article 25 et* ***sous réserve de dispositions contraires de leur droit national régissant des cas particuliers****, les Etats membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2 peut être effectué (...)".*

Si ces dérogations prévues pour répondre aux inquiétudes de certains secteurs, principalement bancaire et du tourisme, seront en pratique largement appliquées, elles pourraient cependant voir leur effet limité par les législations que les Etats membres peuvent adopter interdisant, dans des cas particuliers, les transferts de données personnelles, nonobstant l'existence de l'une des dérogations suivantes:

1 - *La personne concernée a indubitablement donné son consentement au transfert envisagé.*

La personne concernée doit donner son consentement non seulement au traitement de

---

[294] U.U. Wuermeling, *supra* note 119, *ibid*: *"In Holland and U.K. codes of conduct have only an illustrative function"*; H. Maisl, *supra* note 198, p. 44 : *"La directive, comme les lois nationales, est un texte général. Des textes d'application sont nécessaires, secteur par secteur, pour adapter la réglementation. La CNIL autorité de contrôle française assure ce rôle par ses normes simplifiées ou par ses recommandations; récemment, elle a encouragé l'élaboration d'un code de déontologie des professionnels du marketing direct (DIT 95/1); des règles de conduite auxilliares de la loi, viennent concrétiser celles-ci dans certains secteurs avec le concours des professions concernées et l'accord de l'autorité de contrôle (cf. H. Maisl, DIT 94/3)".*

ses données, mais aussi au transfert. Ce consentement doit être "*éclairé*"[295], ce qui signifie que la personne concernée doit avoir conscience qu'il s'agit d'un flux transfrontalier, doit connaître le pays de destination des informations[296] et les risques spécifiques qu'entraîne ce transfert à destination d'un pays n'assurant pas une protection adéquate. En outre, le consentement doit être "*incontestable*", c'est-à-dire clair et non équivoque. On peut dès lors s'interroger sur la validité d'un consentement donné sous forme d'adhésion à des conditions générales, ne portant pas spécifiquement sur un transfert particulier.

2 - *Le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concerné ou le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.*

Non seulement le traitement mais aussi le transfert doivent être nécessaires à l'exécution de mesures précontractuelles ou d'un contrat. Ne répondrait dès lors pas à ce critère ou

---

[295] *Supra*, Paragraphe 2 - Notion de "Protection adéquate", Sous-paragraphe 1 - Principes fondamentaux, 1 - Principes de base de la protection, *vii) Participation individuelle;* article 2 h) de la Directive européenne, le consentement est "*toute manifestation de volonté libre, spécifique et informée (...)*"; l'exposé des motifs précise également: " *le transfert vers un pays tiers n'assurant pas un niveau de protection adéquat peut être effectué si la personne concernée a donné son consentement au transfert envisagé (...) Dans ce cas, la personne est informée du transfert ou de la possibilité de transfert vers un ou des pays tiers, n'assurant pas un niveau de protection adéquat*" (CE, *Proposition (CEE) modifiée de Directive du Conseil relative à la protection des peronnes physiques à l'égard des traitements des données à caractère personnel et à la libre circulation de ces données du 15 octobre 1992*, *supra* note 193, p. 36).

[296] P. Trudel , "Introduction au droit du commerce électronique sur l'Internet", (1995) 55 R. du B. 521, p. 539; *Adde*: U.U. Wuermeling, supra note 119, p. 453: "*the codes represent guidance, acceptance in voluntary, and recommendations are not binding*".

la délocalisation de la gestion des ressources humaines d'une société puisque s'il est nécessaire de traiter ces données, le transfert vers le pays tiers ne paraît pas, en soi, nécessaire à l'exécution du contrat.

En revanche, tel serait le cas des transferts de données personnelles dans le secteur bancaire et du tourisme dès lors que la plupart de ces transferts sont nécessaires à l'exécution d'un contrat conclu entre le banquier ou l'agence de voyage et son client (exécution de virements, réservation de voyages, etc.) ou dans son intérêt[297]. Ces dérogations pourront également être invoquées dans le cadre d'un contrat de travail au sein d'une société multinationale, dans la mesure où la gestion du personnel, par exemple, est réalisée au sein de la maison mère établie en-dehors de l'Union européenne[298].

La personne concernée devra également être informée des risques qu'entraîne un transfert de ses données vers un pays n'assurant pas une protection adéquate afin d'"*assurer à [son] égard un traitement loyal des données*"[299]. Si le transfert est nécessaire à l'exécution d'un contrat, les données peuvent en effet être utilisées dans le pays tiers à des fins différentes de celles considérées dans le pays d'origine. Pour cette raison, la personne concernée devrait également être informée de l'identité des destinataires ou catégories de destinataires à qui les données sont transférées, cette information ne se déduisant pas du transfert. La personne concernée ne sera en effet pas nécessairement informée de l'identité de la banque chargée de l'exécution d'un virement dans un pays tiers. Elle pourrait, par contre, être informée de l'identité d'une agence de voyages à l'étranger avec laquelle sa propre agence entretient des liens particuliers si

---

[297] telle une filiale faisant parvenir son fichier du personnel à la maison mère localisée au Canada (voir M.H. Boulanger et C. de Terwangne, *supra* note 186, p. 18).

[298] La gestion doit réellement s'opérer dans un pays tiers et le transfert doit être réellement "*nécessaire*". Il ne peut s'agir dès lors d'une délocalisation des fichiers dans le but d'éviter le régime de protection mis en place par la Directive européenne.

[299] Articles 10 (c) et 11.1 (c) de la Directive européenne.

ses données y sont transférées lors de la réservation d'un voyage.

3 - *Le transfert est nécessaire ou rendu obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.*

Selon l'interprétation de la notion "*d'intérêt public*" que donneront les Etats membres, cette exception prévue pour faciliter les échanges internationaux vers des pays tiers, pourrait notamment couvrir les échanges entre administrations fiscales ou douanières, entre services compétents en matière de sécurité sociale ou dans la cadre d'une procédure en justice instruite dans un Etat tiers.

4 - *Le transfert est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée.*

L'étendue de cette dérogation dépendra de la définition donnée à "*l'intérêt vital*" de la personne concernée. Les considérants (§ 31) relatifs à l'article 7.d de la Directive européenne indiquent que cette notion vise les traitements effectués "*en vue de protéger un intérêt essentiel à la vie de la personne concernée*". Dans le cadre d'un transfert de données vers un pays tiers, il semble que cette disposition n'autorise le flux de données à caractère personnel qu'en cas d'extrême urgence, lorsque le transfert de certaines données est de nature à sauver la vie d'une personne en danger. Rappelons que s'il s'agit de données "*sensibles*", les conditions prévues aux articles 7 et 8 de la Directive européenne doivent également être respectées.

5 - *Le transfert intervient au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du*

- *public et ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.*

Cette dérogation se justifie par le fait qu'à partir du moment où les données sont dans le domaine public, il n'y a plus de raison d'interdire leur transfert vers un pays tiers, même si la protection offerte dans ce dernier n'est pas jugée "*adéquate*".

Selon les considérants (§ 58) de la Directive, le transfert ne pourra jamais être autorisé pour la totalité ou des catégories de données personnelles contenues dans le registre public[300] mais seulement pur certaines données précises. En outre, lorsque la consultation n'est permise qu'à ceux ayant un "*intérêt légitime*", le transfert ne devrait pouvoir être effectué "*qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires*". Cette dérogation est donc limitée aux personnes situées dans un pays tiers qui disposeraient d'un droit de consultation si elles se trouvaient dans un Etat membre de l'Union européenne.

Sous-paragraphe 2 - Clauses contractuelles

Dans le cas où le pays tiers n'assure pas une protection adéquate et que les dérogations spécifiques prévues à l'article 26.1 de la Directive européenne ne trouvent pas à s'appliquer, un transfert de données personnelles vers un pays tiers peut néanmoins être autorisé "*lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées*". Cet accord contractuel conclu entre le transmetteur et le destinataire garantirait le respect par la société réceptrice des

---

[300] Constituent des registres public, les registres de la population ou les registres de commerce ouverts au public, de même que les annuaires, par exemple téléphoniques.

principes fondamentaux énoncés dans la législation de l'Etat exportateur[301].

L'article 26.2 de la Directive européenne prévoit dans cette hypothèse une procédure d'information de la Commission et des autres Etats membres par l'Etat accordant cette autorisation. En cas d'opposition de leur part, "*dûment justifiée au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes*"[302], la Commission, après l'avis d'un Comité consultatif[303], prendra des mesures appropriées, telle l'interdiction du transfert. L'Etat membre prendra également les mesures nécessaires pour se conformer à la décision de la Commission.

En 1992, le Conseil de l'Europe, conjointement avec la Commission Européenne et la Chambre du Commerce internationale, a entrepris la rédaction d'un contrat-type applicable aux flux transfrontières de données à caractère personnel[304] et ayant pour

---

301 K. Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", *supra* note 154, pp. 178-179: "*La France fournit une exemple pratique de cette approche contractuelle. (...). Fiat-France avait décidé de transmettre à son siège social à Turin des informations nominatives "ayant pour finalité la connaissance permanente des cadres supérieurs et la gestion optimale des carrières dans un contexte international" [CNIL, Délibération n° 89-79 du 11 juillet 1989 relative à la transmission d'informations relatives aux cadres supérieurs de la société Fiat-France à la société Fiat à Turin (Déclaration ordinaire n° 893-947) p. 1]. Il ne s'agissait pas d'une transmission unique, mais bien de l'établissement d'un système informatique ayant pour objet une transmission continue d'informations nominatives. La CNIL a d'abord constaté l'absence de toute législation relative à la protection des données à caractère personnel en Italie. Elle a ensuite exigé, par conséquent, que la société Fiat, à Turin, s'engage par voie contractuelle à respecter les principes fondamentaux en matière de gestion de l'information personnelle ("noyau dur") consacrés par la loi française [n° 78-17 relative à l'information, aux fichiers et aux libertés, J.O. et rectif. 25 janvier 1978] et la convention européenne*".

302 Article 26.3 de la Directive européenne.

303 Etabli par l'article 31 de la Directive européenne.

304 Conseil de l'Europe, "*Contrat type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de données et rapport explicatif*", (Strasbourg, 1992) T-PD (92) 7, révisé le 2 novembre 1992.

objet de faciliter les échanges de données à caractère personnel entre différents pays assurant un degré de protection aux données transférées au moins équivalent à celui du pays exportateur. La voie contractuelle ne saurait néanmoins assurer à la personne concernée une protection exclusive et définitive en raison des inconvénients qu'elle comporte. L'existence de clauses contractuelles entre pays exportateur de données et pays destinataire constituent dès lors des mesures complémentaires s'inscrivant dans un cadre législatif ou réglementaire plus global.

Le principal inconvénient résulte du principe de la relativité des contrats. Le contrat constitue en effet pour les véritables bénéficiaires, c'est-à-dire la personne concernée et l'autorité chargée de la protection des données, une *res inter alios acta*[305] qu'ils ne peuvent, en principe, pas invoquer en cas d'utilisation erronée ou abusive des données personnelles. Il convient donc de leur rendre ces clauses opposables en les insérant dans des conditions générales ou en recourant à des mécanismes telle que la stipulation pour autrui[306].

Par ailleurs, l'autorité nationale de protection de données établie dans un Etat membre ne disposera, hors de ses frontières, d'aucune autorité permettant d'assurer une protection efficace des données de la personne concernée[307].

Il semble dès lors prudent d'insérer dans le contrat des dispositions garantissant à la personne concernée la possibilité d'invoquer ces clauses et de les opposer à

---

[305] Voir la doctrine de "*privity*" dans les pays de common law.

[306] Ou encore la constitution d'un fonds de garantie auprès d'une tierce partie indépendante qui serait appelée dans le cas de non-respect du contrat, (OCDE, Série PIIC, Paris, OCDE, 1994 cité par Y. Poullet, "O.C.D.E.: Protection des données et de la vie privée", (1995) D.I.T., p. 84).

[307] Sauf une clause contractuelle par laquelle l'autorité de contrôle dispose de droits d'inspection.

l'exportateur des données[308] (qui, par hypothèse, est plus facile à localiser puisqu'il est situé sur le même territoire que la personne concernée) ainsi que l'exercice d'un recours auprès des autorités judiciaires ou de l'autorité nationale de protection des données établies dans le pays exportateur. A défaut, les clauses contractuelles ne semblent pas suffisantes pour offrir, conformément à l'article 26.2 de la Directive européenne, des garanties suffisantes *"au regard de la protection de la vie privée (...) et de l'exercice des droits correspondants"*.

Paragraphe 5 - Mise en oeuvre

Comme on l'a observé[309], *"the basic approach of the Directive to serve as a "framework" for data protection [rather than minute provisions], and consequently using broader definitions*[310]*, leaves a wide margin of manoeuvre for the Member States, which may lead to a "watering down" of the level of protection in the implementation process and thus hinder the harmonization-process of the right to privacy"*[311].

---

[308] Voir J.R. Reidenberg, "Setting standards for Fair Information Practice", *supra* note 207, p. 3; *Adde*: A.C.M. Nugter, *supra* note 149, pp. 308-309.

[309] Th. Zerdick, *supra* note 121, p. 68; *Adde*: U.U. Wuermeling, *supra* note 119, p. 426: *"During its development the Directive changed from precise provisions to a framework regulation. (...) The final Directive simply gives a broader choice of measures to meet the requirements. In some cases Member States may ass their own regulations on the basis of their legal traditions"*.

[310] Th. Zerdick, *supra* note 121, p. 68:" *Apart from this, the Directive is far more detailed than Convention 108: For example, the right to access extends not only to the contents of the information stored but also to the source and recipient of data*"; U.U. Wuermeling, *supra* note 119, p. 458: " *Some of the provisions in the Directive were taken from the CoE Convention and some ideas arose out of the OECD and UN Guidelines. However, there are two main differences between the Directive and other international regulations: first, the legal effect; and second, the extent of the detailed provisions and limited exceptions*".

[311] U.U. Wuermeling, *supra* note 119, p. 427: *"The Directive intends to ensure an equal level of protection in national laws. However, it is questionable whether the Directive will reach this goal. (...) It is clear that data protection in the European Union will never reach the same standard because at least the interpretation of the balance of interests clauses depend on the value of data protection in the societies of each Member State. Furthermore, the national habits to meet the legal provisions will cause differences. The Directive tries to solve such problems by*

La transposition de la Directive dans les législations des Etats membres entraînera la révision de plusieurs de leurs dispositions. Un des principaux changements qui devrait intervenir porte sur l'obligation pour tout responsable de traitement qui informatise des données relatives à des personnes physiques, d'en informer ces personnes, même lorsque les données n'ont pas été collectées auprès d'elles[312]. Outre l'identité du responsable du traitement et des finalités poursuivies, la personne concernée doit également être informée de l'origine des données enregistrées[313].

En revanche, dans la mesure où la Directive renforce l'obligation d'information des personnes, l'obligation de déclarer la constitution ou le traitement des données personnelles auprès de l'autorité nationale de contrôle devrait, sous réserve de ceux présentant des risques particuliers, s'en trouver allégée[314].

Les Etats tiers à l'Union européenne devront également changer certains de leurs propres standards s'ils veulent bénéficier des échanges transfrontières de données

---

introducing a Working Party at the European Union. However, it has not been given sufficient power. Only the European Court of Justice has the power to rule on a harmonised interpretation of the Directive. The rules on "direct effect" of Directives might be used , however, that is not enough to replace every difference in implementation and interpretation of the Directive. Especially in the private sector, the instrument of direct effect does not work. There is only an obligation for judges to interpret the present law, as far as possible, in the light of a directive. Finally, the process of obtaining a decision by the European Court of Justice is far too slow for the pressing need (...) The question of whether and to what extent the Directive provides an equivalent standard is quickly raised in Member States where the national law already provides sectoral regulations. If those regulations fall below the level of Directive, they must be amended".

312 A ce jour, la plupart des législations dont la loi française, ne comporte d'obligation d'informer les personnes que lorsque les données sont recueillies auprès d'elles ("Informatique et libertés: ce qui va changer dans la loi française", (1995) 11 Droit et affaires, p. 1).

313 Ce que les lois allemande et anglaise n'imposent pas; pour plus de développements, voir U.U. Wuermeling, *supra* note 119, pp. 446 et 459.

314 Solution inspirée du droit allemand (H. Maisl, *supra* note 198, p. 44).

personnelles en provenance ou à destination des Etats membres[315].

SECTION 3 - LA LEGISLATION FEDERALE CANADIENNE

La Loi fédérale canadienne sur «*la protection des renseignements personnels*», adoptée en février 1985[316], a pour objet de compléter la législation canadienne en matière de protection des renseignements personnels relevant des institutions fédérales et de droit

---

315 U.U. Wuermeling, *supra* note 119, pp. 445 et 460: "*Country outside the EU have to change their own standards, if they want to avoid obstacles in the exchange of personal data with countries of the European Union. (...) The Directive has not only an impact on Member States but also impacts on non Member States, like the U.S., that wish to transfer data to or from a European Union country. They must ensure an adequate level of protection if they want to exchange personal data. The third country regulations in the Directive raise the issue of whether there is adequate protection in a specific transaction. If third countries do not change their general law in order to provide adequate protection, it is debatable whether contractual regulations between partners of transactions are capable of meeting the requirements of the Directive*". Pour plus de développements, voir M.P. Roch, *supra* note 116, p. 93 et s.; S.A. Millar, "FTC Expores Consumer Protection in Cyberspace", (1996) The multimedia L. Report 4, p. 5. Dans le cadre du Groupe de protection des données à l'égard du traitement des données à caractère personnel, prévu à l'article 29 de la Directive, des travaux ont été entrepris en matière de transferts de données vers des pays tiers. Toutefois aucune position n'a été rendue publique jusqu'à ce jour. Par ailleurs, dans le cadre des négociations d'accession des pays de l'Europe centrale et de l'Europe de l'Est à l'Union, la Commission, encourageant les contacts entre les représentants de ces pays et les comités des autorités nationales de protection des données, recueille des informations sur le développement dans ces pays de législations en matière de protection des données.

316 L.C.R. 1985, c. P-21, [ci-après *Loi fédérale*]; D. Johnston, D. Johnston et S. Handa, *supra* note 19, p. 195: "*As with the federal Privacy Act, several provincies have enacted specific legislation to "protect the privacy of individuals with respect to personal information about themselves held by [government] institutions and to provide individuals with a right of access to that information. Privacy legislation designed to protect individual information held by government also applies at the municipal level"; Freedom of Information Act*, S.N., 1981, c. 5 (Terre-Neuve), *Freedom of Information Act*, S.N.S., 1990, c. 11 (Nouvelle-Ecosse); *Loi sur le droit à l'information*, S.R.N.B., 1973, c. R-10.3, telle qu'amendée (Nouveau-Brunswick), *Freedom of Information and Protection of Privacy Act*, 1987, S.O., 1987, c. 25, telle qu'amendée et *Loi de 1989 sur l'accès à l'information municipale et la protection de la vie privée*, S.O., 1989, c. 63 (Ontario), *Loi sur la liberté d'accès à l'information*, L.M., 1985-1986, c. 6 Chap. F175, telle qu'amendée (Manitoba), *Access to Information Act*, R.S.Y., 1986, c. 1 (Yukon), et *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* L.R.Q., c. A-2.1 (Québec); *infra* Section 4 - La législation Québécoise, *Sous-section 2 - La Loi sur l'accès*.

d'accès des individus aux renseignements personnels qui les concernent[317].

SOUS-SECTION 1 - CHAMP D'APPLICATION

La Loi fédérale s'applique aux renseignements personnels relevant des institutions fédérales[318]. Par "*renseignement personnel*, l'article 3 de La loi entend "*les renseignements quels que soient leur forme et leur support, concernant un individu identifiable*". Il s'agit, selon la Loi aussi bien des renseignements auxquels le public a déjà accès (situation de famille, adresse, âge, empreintes digitales) que des renseignements "*sensibles*" (race, origine nationale ou ethnique, couleur, religion, dossier médical, groupe sanguin, idées ou opinions personnelles)[319]. L'information doit être détenue par une institution fédérale, à savoir "*tout ministère ou département d'Etat relevant du gouvernement du Canada, ou tout organisme figurant à l'annexe de la Loi*" (l'Office des produits agricoles, le Centre canadien d'hygiène et de sécurité du travail, la Commission nationale des libérations conditionnelles, etc.).

En ce qui concerne les renseignements personnels en provenance de l'Union Européenne, la Loi s'applique *a priori* à la condition toutefois qu'ils aient été

---

[317] Article 2.1 de la Loi fédérale; sur cette dernière loi (L.R.C. 1985, c. A-1), voir L. Doré, "Panorama de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels" dans *Développements récents en droit de l'accès à l'information (1991)*, Coswanville, éd. Yvon Blais, 1991, pp. 29 - 66 et p. 68.

[318] D. Johnston, D. Johnston et S. Handa, *supra* note 19, *ibid*: "*(...) it only applies as between an individual and government institutions. It does not extend to private parties* [*S. 60 (1) c) does, however, give the Privacy Commissioner the power to extend his/her investigations to "persons or bodies, other than government institutions, that come within the legislative authority of Parliament*]. *Over the past few years, in addition to serving a watchdog role over government, in his annual report, the Privacy Commissioner has reported on the state of privacy law generally, including privacy between private* parties".

[319] Certaines catégories sont exclues, tels les renseignements concernant le poste ou les fonctions d'un employé d'une institution fédérale et ceux concernant un individu décédé depuis plus de 20 ans.

préalablement versés dans un fichier de renseignements personnels d'une institution fédérale.

SOUS-SECTION 2 - PRINCIPES FONDAMENTAUX

L'existence des principes de base dans une législation d'un pays tiers à l'Union européenne vise à assurer la garantie d'un niveau de protection qui pourrait être considéré comme adéquat au sens de l'article 25 de la Directive européenne. Il convient donc de vérifier la présence de ces principes dans la législation fédérale canadienne.

i) Principe de collecte loyale et licite

Aucun principe de collecte loyale et licite des données, ni de finalité légitime n'est inscrit dans la Loi fédérale[320].

ii) Spécification des finalités

Les données personnelles ne doivent être utilisées que pour une finalité déterminée. Ce principe est affirmé à l'article 7 de la Loi selon lequel "*à défaut de consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution, de même que pour les usages qui sont compatibles avec ces fins*".

La Loi n'exige pas la légitimité de la finalité poursuivie. L'article 4 de la Loi fédérale précise que l'institution fédérale ne peut collecter que des renseignements qui ont un lien direct avec ses programmes ou ses activités. Toutefois, cette obligation ne concerne pas directement la finalité du traitement. En outre, les programmes et activités de l'institution doivent d'abord être légitimes afin d'assurer la légitimité de la finalité.

---

320 Elle prévoit seulement que dans la mesure du possible, les renseignements personnels devraient être recueillis directement auprès de l'individu concerné (article 5 de la Loi fédérale).

iii) Limitation de l'utilisation

Les données personnelles ne peuvent être utilisées qu'aux fins pour lesquelles elles ont été recueillies ou préparées[121]. Néanmoins, dans certaines circonstances, les données peuvent être divulguées[122] en l'absence du consentement de la personne concernée. L'article 8 (2) (par. a) de la Loi[123] dispose en effet que les renseignements personnels peuvent être communiqués aux fins auxquelles ils ont été recueillis ou préparés, ou pour les usages qui sont compatibles avec ces fins. Semble seule constituer une fin compatible, celle invoquée à l'appui de l'utilisation ou de la divulgation de renseignements personnels à laquelle la personne concernée par les renseignements pourrait raisonnablement s'attendre lorsque ceux-ci ont été obtenus auprès d'elle[124]. La communication peut également se fonder sur une loi (par. b) ou une décision judiciaire (par. c).

La Loi fédérale ne précise toutefois pas que cette même finalité doit être respectée en cas de réutilisation des données personnelles pour un nouveau traitement.

iv) Qualité et proportionnalité des données

---

121 *"dont le partage de ce renseignement au sein même de l'organisme l'ayant recueilli. Il est cependant possible de se servir d'un renseignement à une fin compatible avec l'objectif initial de la collecte (...)"* (Le Commissaire à la protection de la vie privée, *Rapport annuel 1995-1996*, Groupe Communication du Canada, 1996, p. 63).

122 *"Ainsi un organisme fédéral peut communiquer des renseignements en vertu d'un accord ou d'une entente liant d'autres paliers de gouvernement à un organisme étranger. Ce partage doit cependant être décrit publiquement afin que la population puisse comprendre comment le gouvernement fédéral utilise et communique les renseignements qui la concernent. Cette information permet un consentement éclairé de la part de la population"* (Le Commissaire à la protection de la vie privée, *Rapport annuel 1995-1996*, *supra* note 321, *ibid.*

123 Cet article énumère les cas d'autorisation de communication de renseignements personnels qui relèvent d'une institution fédérale.

124 *Supra*, Section 2 - la Directive européenne, *Sous-section 3 - Flux transfrontières de données à caractère personnel*, Paragraphe 2 - Notion de "protection adéquate", Sous-paragraphe 1 - Principes fondamentaux, 1 - Principes de base de la protection, *iii) limitation de l'utilisation*.

Comme indiqué[125], l'article 4 de la Loi fédérale précise que seuls les renseignements qui ont un lien direct avec ses programmes ou ses activités peuvent être collectés par une institution fédérale. Ce *"lien direct"* semble correspondre à l'obligation de la Directive européenne de ne traiter que des données nécessaires à la poursuite de la finalité du traitement.

En outre, l'article 6 (2) de la Loi fédérale dispose que l'institution fédérale doit veiller, autant que possible, à ce que les renseignements utilisés soient à jour, exacts et complets[126]. Ce principe correspond aux exigences de la Directive européenne énumérées à l'article 6 (2).

v) Garanties de sécurité

Aucune garantie de sécurité n'est prévue par la Loi fédérale contre d'éventuels pertes, destructions ou accès non autorisés[127].

---

[125] *Supra, ii) Spécification des finalités.*

[126] Article 6 (2) de la Loi fédérale.

[127] Aussi, dans le cadre de l'aménagement de l'autoroute canadienne de l'information, le Comité consultatif sur l'autoroute de l'information (CCAI) a recommandé que:

"Rec. 10-14 The federal governement should take a leadership role in developing privacy, integrity and authenticity services on the Information Highway, through the creation of a uniform public key infrastructure (PKI) to meet federal governments needs.

Rec. 10.15 The Department of Justice and other departments should review and suggest changes to federal legislation and statutes to provide greater certainty to the areas of digital signature and public key infrastructure services". (Information Highway Adivsory Council, Final Report *Connection, Community, Content, Challenge* (Ottawa: Supply and Services Canada, september 1995) (Chair D. Johnston), pp. 145 et 146 [ci-après *IHAC Final Report*]; *Adde*: Ministère des Communications, *La société canadienne à l'ère de l'information: Pour entrer de plain-pied dans le XXIe siècle*, Ottawa, Ministère des Approvisionnements et Services, 1996, p. 27).

Le CCAI considère en effet que *"the governement can play a leadership role by leveraging Canada's private sector strengths in the security field to deplay the PKI, which in turn acts as a catalyst for private sector security service introduction (...) It is likely that broad-based security will be actieved through several PKIs, to be built by different public and private entities. (...) An unfragmented "electronic market" on the Information highway, offering maximum consumer*

vi) Transparence

L'institution fédérale chargée de recueillir des renseignements personnels est tenue, en vertu de l'article 5 (2), d'informer la personne concernée des fins auxquelles ces renseignements sont destinés. Aucune disposition de la Loi fédérale ne mentionne toutefois l'obligation d'informer la personne concernée du changement de finalité du traitement.

Par ailleurs, un répertoire de renseignements personnels est tenu par l'administration[328]. Ce répertoire vise à faire connaître aux individus l'existence de fichiers de renseignements personnels ainsi que leur contenu. Un ministre est chargé de la diffusion de ce répertoire dans tout le territoire du Canada, "*toute personne [ayant] le droit d'en prendre normalement connaissance*".

---

choice, will be possible only if PKI interoperability standards issues are fully addressed". (IHAC, Final Report, ibid).

Le CCAI recommande dès lors:

"*Rec. 10.16 The government and the private sector should continue to work together to develop compatible PKI policies to ensure interoperability and uniform privacy protection for users.*

Rec. 10.18 The government and the private sector should continue to work in partnership to ensure PKI cross-certification between major national and international trading partners" (IHAC Final Report, *ibid*, p. 146)".

Le CCAI encourage également "*the government*", *itself a PKI user, to take the lead in establishing a common independent Canadian certification authority (Rec. 10.14) and act as catalyst for the introduction of private sector services requiring security*" (IHAC Final Report, *ibid*, p. 51; voir également D. Johnston, D. Johnston et S. Handa, *supra* note 19, pp. 138-139.

Sur le commerce électronique au sein de l'administration publique, l'élaboration et la mise en oeuvre de politiques et de normes juridiques qui appuieront le commerce électronique dans le secteur privé, voir Ministère des Communications, *La société canadienne à l'ère de l'information: Pour entrer de plain pied dans le XXIe siècle*, *ibid*, pp. 30-31; IHAC Final Report, *ibid*, p. 144.

[328] Article 11 de la Loi fédérale.

Un droit d'accès est également octroyé à tout citoyen canadien et tout résident permanent pour les renseignements personnels les concernant et versés dans un fichier de renseignements personnels[129]. Ce fichier regroupe tous les renseignements personnels qui ont été, sont ou peuvent être utilisés à des fins administratives et qui sont marqués de façon à pouvoir être retrouvés par référence au nom d'un individu ou à un numéro, symbole ou autre indication identificatrice propre à cet individu[130]. Le droit d'accès est également accordé aux mêmes personnes pour les autres renseignements personnels relevant d'une institution fédérale dans la mesure où la personne concernée peut fournir des indications suffisantes pour les localiser[131].

Le droit d'accès s'exerce par le biais d'une demande écrite adressée à l'institution fédérale compétente. L'institution est tenue d'y donner suite dans les trente jours[132] et, en cas de refus de communication, doit motiver sa réponse[133] et mentionner le droit pour la personne concernée de déposer une plainte auprès du Commissaire à la protection de la vie privée[134]. L'accès est accordé soit par la permission de consulter les renseignements, soit par la délivrance de copies[135]. L'accès aux renseignements personnels est également garanti par l'obligation qui repose sur les institutions

---

129 Article 12 (1) a de la Loi fédérale.

130 Article10 (1) de la Loi fédérale.

131 Article 12 (1) b de la Loi fédérale; sur l'annulation de "*fichiers inconsultables*" voir L. Doré, *supra* note 317, p. 71.

132 Une prorogation maximale de 30 jours est permise si le traitement de la demande entrave sérieusement le fonctionnement de l'institution fédérale, s'il est nécessaire d'effectuer des consultations ou de traduire les renseignements (article 15 de la Loi fédérale).

133 C'est-à-dire indiquer à l'auteur de la demande "*soit le fait que les renseignements n'existent pas, soit la disposition précise de la Loi sur laquelle se fonde le refus ou sur laquelle il pourrait vraisemblablement se fonder si les renseignements existaient*" (L. Doré, *supra* note 317, p. 71).

134 Articles 13 à 16 de la Loi fédérale.

135 Article 17 de la Loi fédérale.

fédérales, de conserver ces renseignements pendant une période suffisamment longue, pour permettre précisément à la personne concernée d'exercer son droit d'accès[136].

Toute personne disposant d'un droit d'accès, peut demander la correction des renseignements erronés ou incomplets qui lui ont été communiqués[137]. Elle peut également exiger que toute personne ou organisme à qui les renseignements ont été transmis, soit informée des corrections ou de la mention qu'une correction a été demandée mais non effectuée.

Si la Loi prévoit un droit d'accès et de rectification pour tout citoyen canadien et tout résident permanent[138], elle n'accorde pas de droits similaires aux ressortissants européens, par exemple, dont les données seraient transférées au Canada et seraient contenues dans un fichier de renseignements personnels détenu par une institution fédérale.

vii) Participation individuelle

L'article 7 de la Loi fédérale prévoit qu'"*à défaut du consentement de l'individu concerné*", les renseignements personnels ne peuvent servir qu'aux fins pour lesquelles ils ont été recueillis et pour les usages qui sont compatibles avec ces finalités. Ce principe répond aux exigences de conformité du traitement avec les finalités déclarées, mais ne permet pas à la personne concernée de contrôler les finalités du traitement ni de

---

136 Article 6 (1) de la Loi fédérale.

137 Article 12 (2) de la Loi fédérale.

138 Sauf exceptions visant à protéger les intérêts nationaux (articles 20-23 de la Loi), les intérêts privés (articles 25-28 de la Loi) et les opérations du gouvernement (articles 19 et 27 de la Loi), voir L. Doré, *supra* note 317, pp. 73-76.

s'opposer au traitement de renseignements personnels.

Un droit d'opposition n'est pas inscrit en tant que tel dans la Loi fédérale. L'article 5 (1) précise seulement que l'institution fédérale est tenue de recueillir auprès de l'individu lui-même, chaque fois que possible, les renseignements personnels destinés à des fins administratives, "*sauf autorisation contraire de l'individu*". Cette disposition ne semble cependant pas constituer un véritable droit d'opposition.

viii) Responsabilité

Aucune responsabilité de la personne en charge d'un traitement de données personnelles n'est mentionnée dans la Loi fédérale.

ix) Détention limitée

Comme indiqué[339], si l'article 6 (1) de la Loi prévoit que les institutions fédérales sont tenues de conserver les renseignements personnels pendant une période suffisamment longue pour permettre à la personne concernée d'exercer son droit d'accès, la Loi fédérale ne prévoit cependant pas que les données fassent l'objet d'une détention limitée au temps nécessaire pour la réalisation de la finalité.

---

[339] *Supra, vi) Transparence.*

SOUS-SECTION 3 - REGLES D'EFFECTIVITE

Les principes de base de protection des données doivent être complétés par des règles d'effectivité qui mettent en place les moyens de garantir *in concreto* le respect pour la personne concernée de ces principes fondamentaux. L'évaluation de l'adéquation de la protection offerte par la législation fédérale dépendra dès lors également de l'effectivité de la protection: reconnaît-on des droits pour la personne concernée, dans un instrument créateur de droits, porté à la connaissance des responsables du fichier et de la personne concernée, ces droits étant susceptibles d'un recours en cas de non-respect ?

Comme indiqué[340], un droit d'accès consacré dans un texte de loi, porté à la connaissance du public, est accordé à tout citoyen canadien ainsi que tout résident permanent désireux de se faire communiquer des renseignements personnels les concernant, accompagné d'un droit de rectification des données[341]. Cependant, la Loi fédérale ne permet pas aux individus de s'opposer à la communication des données personnelles.

La Loi fédérale prévoit également un droit de recours en cas de non-respect de ces droits. Ainsi, toute personne qui s'est vue refuser la communication de renseignements personnels ou dont les renseignements ont été utilisés pour des fins autres que celles pour lesquelles ils ont été recueillis et sans son consentement, peut déposer une plainte écrite auprès du Commissaire à la protection de la vie privée[342]. Celui-ci peut également

---

340 *Supra, vi) Transparence.*

341 Article 12 de la Loi fédérale.

342 Le Commissaire à la protection de la vie privée est nommé sur résolution du Parlement pour une période de sept ans; D. Johnston, D. Johnston et S. Handa, *supra* note 19, p. 195: "*In addition to the Federal Privacy Commissioner, provincies may also have their own privacy commissioners who also serve as government watchdogs. Our constitution does not expressly deal with the*

enquêter d'initiative sur toute question relative à l'application de la Loi ou sur les activités de collecte, d'utilisation, de communication, de rétention et de destruction des renseignements personnels. A la suite de cette enquête, le Commissaire présente ses conclusions et ses recommandations qui peuvent être incorporées au rapport qu'il doit soumettre une fois l'an au Parlement ou faire l'objet de rapport spéciaux[343].

L'article 68 de la Loi fédérale précise que quiconque contrevient à l'action du Commissaire à la protection de la vie privée dans l'exercice de ses pouvoirs est coupable d'une infraction et passible, sur déclaration sommaire de culpabilité, d'une amende d'au plus mille dollars.

L'individu qui s'est vu refuser l'accès à des renseignements personnels et qui n'a pas obtenu satisfaction après enquête du Commissaire à la protection de la vie privée, peut intenter un recours en révision de la décision de refus devant la Cour Fédérale[344]. Ce droit de recours dont le dépôt d'une plainte est le préalable nécessaire, doit s'exercer dans les quarante-cinq jours suivant le compte-rendu du Commissaire[345].

---

power over privacy rights. Consequently, both the provincies and the federal government have exercised authority over privacy matters in different contexts".

[343] Articles 35 et 37 de la Loi fédérale.

[344] Article 41 de la Loi fédérale; ces recours ne couvrent pas des délais échus ou des prorogations, à moins qu'elles ne constituent un refus présumé (articles 48, 49 et 51 de la Loi).

[345] La procédure est décrite à l'article 29 de la Loi fédérale.

SOUS-SECTION 4 - MISE EN OEUVRE

Si chaque principe de base identifié dans la Directive européenne comme garantissant un niveau de protection adéquat ne se retrouve en tant que tel dans la Loi fédérale (ni le principe de la collecte loyale et licite des renseignements, ni l'exigence de légitimité de la finalité poursuivie ne sont consacrés; il n'existe pas non plus de garanties de sécurité contre la perte, la destruction ou l'accès non autorisé aux données, ni de dispositions sur la responsabilité de la personne en charge d'un traitement de données personnelles; enfin, non seulement le consentement de la personne n'est pas requis lors de la collecte initiale, mais il n'existe pas non plus d'obligation d'informer la personne concernée du changement de la finalité du traitement), l'effectivité de la législation fédérale canadienne semble être assurée de façon satisfaisante[346].

On peut cependant déplorer l'inexistence de certains droits (essentiellement d'accès et de rectification) similaires pour les ressortissants européens, ce qui pourrait restreindre le transfert des données personnelles les concernant.

La "*protection adéquate*" de la Directive européenne n'exige cependant pas un niveau de protection "*équivalent*" dans le pays tiers[347], en sorte que, sous réserve de dispositions nationales plus strictes, un transfert de données à caractère personnel, dans le secteur public, à partir d'un Etat membre de l'Union européenne devrait pouvoir être autorisé sans conditions particulières.

---

[346] Voir Le Commissaire à la protection de la vie privée, *Rapport annuel 1987-1988*, Groupe Communication du Canada, p. 5.

[347] *Supra*, Section 2 - la Directive européenne, *Sous-section 3 - Flux transfrontières de données à caractère personnel*, Paragraphe 2 - Notion de "protection adéquate".

Il reste que, nonobstant les déclarations de la nécessité d'une intervention législative[348], le Canada ne dispose pas de normes nationales protégeant, comme l'exige la Directive européenne, les renseignements personnels détenus par les entreprises privées. Sous réserve des législations spécifiques[349] et des codes de conduite applicables dans le secteur privé[350], le Canada risque de souffrir d'une interdiction de transfert de données à

---

[348] Dans le cadre de l'aménagement de l'autoroute canadienne de l'information, le Comité consultatif sur l'autoroute de l'information (CCAI) considérait que "*to ensure the protection of privacy rights of Canadians in the information age, the council believes strongly in the need for national framework legislation to apply to government and private sector alike. (...) In order for consumers and users to benefit from electronic information networks, there is a need for coherent national standards as to what constitutes effective privacy protection in an electronic environment among business, consumer organizations and government. The Council believes that such a standard can best be achieved through legislation*" (IHAC Final Report, *supra* note 327, p. 140 et XIV. Le gouvernement a également reconnu la nécessité d'une loi-cadre pour protéger les renseignements personnels: "*comme on ne peut pas uniquement compter sur la technologie et les mesures de sécurité, le droit à la protection des renseignements personnels doit être reconnu dans la loi, surtout dans un monde électronique où il est très facile de recueillir et d'exploiter des renseignements sur une personne*" (Ministère des Communications, *La société Canadienne à l'ère de l'information: Pour entrer de plain-pied dans le XXI siècle*, *supra* note 327, p. 27).

[349] "*There are some special privacy situations which are governed by provincial law, such as privately owned credit reporting agencies. In Ontario, for example, the Consumer Reporting Act restricts those agencies that gather and distribute consumer credit information. The Act specifically limits the type of information which can be gathered, as well as to whom such information may be given. Any person about whom such information is being collected may request disclosure of this information. The Act also restricts anyone, who is not specifically listed under the Act, from "knowing[ly] obtain[ing] information from the files of a consumer reporting agency respecting a consumer...". While this Act is specifically aimed at controlling the privacy interests of individuals in a private party context, it is one of the few pieces of legislation that currently deals with private party privacy issues. As the I-way develops, and electronic databases become more prevalent, it seems likely that similar specific legislation will be enacted*" (D. Johnston, D. Johnston et S. Handa, *supra* note 19, p. 197).

[350] "*Most governments in Canada have legislated privacy protection pertaining to their own activities. However, in this regard, the private sector is virtually unregulated; only Quebec has enacted specific legislation governing its private sector. The Council believes strongly that there should be national legislation (Rec. 10.2) to establish for information practices on the Information Highway.*

In this regard, the Council endorses the efforts of the Canadian Standards Association (CSA) to develop a voluntary national code (Model Code for the Protection of Personal Information). The government should continue to collaborate with the CSA as well as business, consumer organizations and other levels of government to implement the code and develop effective independant oversight and enforcement mechanisms (Recs. 10.1 and 10.2)" (IHAC, Final

partir du territoire communautaire et, par conséquent, d'un désavantage commercial par rapport à d'autres pays [351].

Report, *supra* note 327, p. 50).

Le CCAI recommandait dès lors:

Rec. 10.1 The federal government should act to ensure privacy protection on the Information Highway. This protection shall embody all principles of fair information practices contained in the CSA draft Model Code for the Protection of Personal Information. To this end, the federal government should continue to participate in the development and implementation of effective national voluntary standards based on this model code.

Rec. 10.2 The federal government must take leadership in the implementation of these principles through the following actions:

a. in cooperation with other levels of government who share responsibility for various sectors of activity on the Information Highway, establish a federal - provincial - territorial working group to implement the privacy principles in all jurisdictions;

b. create a level playing field for the protection of personal information on the Information Highway by developing and implementing a flexible legislative framework for both public and private sectors. Legislation would require sectors or organizations to meet the standard of the CSA model code, while allowing the flexibility to determine how they will refine their own codes;

c. in cooperation with the CSA Working Group on Privacy and other interested parties, study the development of effective oversight and enforcement mechanisms;

d. establish a working group to coordinate the development, demonstration and application of privacy-enhancing technologies for the provision of government services and information; and

e. update and harmonize appropriate privacy protection policies, legislation and guidelines applicable to its own operations and to the delivery of government services and information. (...)

Rec. 10.4 Provincial and territorial governments should adopt measures to ensure that personal records, including education and training data, are protected from unauthorized collection, storage and use. (IHAC Final Report, *ibid*; sur l'état des législations provinciales, voir Le Commissaire à la protection de la vie privée, *Rapport annuel 1995 - 1996*, *supra* note 321, p. 35).

[351] Hong-Kong s'est doté d'une législation dans ce domaine en 1992; l'Australie envisage d'étendre l'application de sa Privacy Act, actuellement limitée aux documents fédéraux, au secteur privé.

SECTION 4 - LA LEGISLATION QUEBECOISE

SOUS-SECTION 1 - CADRE GENERAL

Le Code civil du Québec, entré en vigueur en 1994, consacre un chapitre spécifique sur les normes de conduite à adopter en matière de respect de la réputation et de la vie privée[352]. Ces dispositions reflètent en grande partie les Lignes directrices de l'O.C.D.E.[353], en ce compris le droit d'accès de tout individu à ses propres données, le droit de rectification de données inexactes et l'interdiction de communication des données à un tiers sans le consentement de la personne concernée.

Il a été toutefois considéré que ces dispositions générales du Code civil, malgré l'insertion du droit d'*habeas data*[354], n'apportaient pas une protection adéquate et suffisante à l'égard des citoyens de la province[355]. En effet, en l'absence de sanctions

---

352 Voir les articles 35 à 41 du Code civil du Québec, pour plus de développements, voir A. Ouimet, *supra* note 43, pp. 203 - 205.

353 Auxquelles le Canada a adhérées le 29 juin 1984; *supra*, Section 1 - Les Lignes directrices de l'O.C.D.E. et la Convention du Conseil de L'Europe, *Sous-section 1 - Cadre général.*

354 voir H.P. Glenn, "Les droits de la personnalité, le respect de la vie privée et le droit à l'image" dans G.A. Beaudoin, dir., Actes des journées strasbourgeoises de l'Institut canadien d'études juridiques supérieures, 1988: "*le nouveau Code civil (...) consacre la notion des droits de la personnalité et instaure un régime unique de ce nouveau droit d'habeas data (le contrôle des données nominatives par la personne sujet des données*".

355 Voir à ce sujet, "La protection de la vie privée eu égard aux renseignements personnels détenus dans le secteur privé", Barreau du Québec, Août 1991; Commission d'accès à l'information du Québec, *Rapport annuel 1994 - 1995*, Les publications du Québec 1995, p. 11; le Commissaire à la protection de la vie privée, *Rapport annuel 1995 - 1996*, *supra* note 321, pp. 19-21.

Sur la controverse quant à la nécessité d'une législation, voir H.P. Glenn, "Le droit en l'an 2000: L'envahissement des contrôles gouvernementaux et des technologies nouvelles dans la vie privée des citoyens, *supra* note 104, pp. 710 - 711: "*Je crois qu'il faut reconnaître d'abord que la plupart des échanges de données personnelles sont parfaitement légitimes, par le consentement même des personnes intéressées. Le consentement va même au-delà d'un premier échange, car*

spéeifiques, seuls les recours en responsabilité civile ou en injonction pouvaient être exercés afin d'assurer le respect de ces principes. En outre, des règles et procédures complémentaires permettant à la personne concernée de connaître les personnes qui détenaient des informations à son sujet semblaient nécessaires afin de faire valoir réellement et efficacement son droit au respect de sa vie privée et de sa réputation[156]. Ces règles furent consacrées par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et la Loi sur la protection de renseignements personnels dans le secteur privé.

---

nous savons tous (...) que la circulation des données personnelles est une condition essentielle de la plupart de nos institutions, publiques ou privées. C'est pourquoi je ne suis pas d'accord avec le Groupe de recherche informatique et droit qu'a conclu récemment que "[...] la légitimité des activités entourant la constitution des bases de données et de leur utilisation reste à fonder". Je crois au contraire que la légitimité se trouve dans l'acceptation massive et démontrée de ces banques de données de la part de tout le monde et dans la vie de tous les jours. Ce qui s'impose, par contre, c'est le moyen de prévenir les abus de notre système de liberté technologique. Ce moyen, c'est le droit que nous avons présentement, qui sanctionne la violation de la vie privée par le moyen de l'action en justice aboutissant à une décision individualisée et à un remède concret rendu par un officier de justice indépendant de toutes les parties. Le peu de recours à ce moyen de redressement est un autre exemple de l'acceptation par tout le monde des pratiques existantes (...) Encore une fois, nous avons l'habeas data au Québec, dans les domaines publics et privés. (...) Dans la mesure où l'habeas data est considéré comme sous-utilisé (...), il y a évidence encore que la circulation des données a eu lieu avec l'autorisation implicite des personnes intéressées. Devant la volonté évidente de l'individu d'ainsi définir sa personnalité, au nom de quoi, précisément, propose-t-on de prendre des mesures plus restrictives, plus globales et plus autoritaires ? Au nom de quoi, au juste, propose-t-on de convertir notre vie qui est privée en un ordre qui est public ?" Contra: K. Benyekhlef, La protection de la vie privée dans les échanges internationaux d'informations, *supra* note 39, p. 79-89.

[156] La Loi sur la protection des renseignements personnels dans le secteur privé, précise, en son article 1er, que "*la présente loi a pour objet d'établir, pour l'exercice des articles 35 à 40 du Code civil du Québec en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil du Québec*"; voir Commission d'accès à l'information du Québec, "Pour quand la protection des renseignements personnels dans le secteur privé ?", (1991) 7 L'accès 1; Commission d'accès à l'information du Québec, "La protection des renseignements personnels dans le secteur privé: un mouvement international", (1992) 8 L'accès 1.

SOUS-SECTION 2 - LA LOI SUR L'ACCES AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (LOI SUR L'ACCES)[357]

Paragraphe 1 - Champ d'application

La Loi sur l'accès s'applique aux documents détenus par les organismes publics dans l'exercice de leurs fonctions[358], quelle que soit l'origine des renseignements nominatifs[359]. Les données concernant des personnes situées dans un Etat membre de l'Union européenne et transférées à un organisme public situé au Québec tombent dès lors sous le champ d'application de la Loi sur l'accès.

Certaines conditions doivent être réunies pour que la Loi trouve à s'appliquer. Il doit exister un document (écrit, graphique, sonore, visuel, informatisé ou autre[360]), détenu par un organisme public[361] ou pour son compte dans l'exercice de ses fonctions. Chargée d'entendre en révision des demandes formulées à l'encontre des décisions des organismes publics, la Commission d'accès à l'information du Québec consulte les actes

---

357 L.R.Q., c. A - 2.1, [ci-après *Loi sur l'accès*]; quoique adoptée en juin 1982, la loi québécoise n'est entrée en vigueur, dans ses principales dispositions, que le 1er juillet 1984.

358 Article 1, § 1 de la Loi sur l'accès.

359 La notion de "*renseignements nominatifs*" est définie à l'article 54 de la Loi; pour une étude jurisprudentielle, voir Y. D. Dussault, "Le point sur deux sujets complexes inhérents à la Loi sur l'accès: les renseignements fournis par un tiers et la notion de renseignements nominatifs" dans *Développements récents en droit de l'accès à l'information (1991)*, Coswanville, éd. Yvon Blais, 1991, pp. 107-122.

360 Article 1, § 2 de la Loi sur l'accès.

361 Les articles 3 à 7 de la Loi sur l'accès définissent l'organisme public comme étant le Conseil exécutif, le Conseil du trésor, l'Assemblée nationales, le gouvernement, les ministères, les organismes gouvernementaux, municipaux, et scolaires ainsi que les établissements de santé et de services sociaux. La Loi exclut de son champ d'application les tribunaux judiciaires ainsi que certains documents déjà publics et détenus à des fins de consultation publique.

instituant les organismes publics afin de déterminer ses fonctions précises[362] et d'établir le lien entre ces fonctions et la détention du document.

Paragraphe 2 - Principes fondamentaux

Sous-paragraphe 1 - Principes de base de la protection

Outre les principes de l'accès à l'information et de la confidentialité des données, objets du titre même de la loi, celle-ci véhicule un certain nombre de principes fondamentaux, correspondants à la notion de "*protection adéquate*" au sens de l'article 25 de la Directive européenne.

i) Principe de collecte loyale et licite

En vertu de l'article 65 de la Loi sur l'accès, quiconque, au nom d'un organisme public, recueille un renseignement nominatif auprès de la personne concernée ou d'un tiers, doit au préalable s'identifier et l'informer de l'identité et l'adresse de l'organisme public au nom duquel la collecte est faite, de l'usage du renseignement, des catégories de personnes qui auront accès aux renseignements, etc. Cet article met ainsi en oeuvre le principe d'une collecte loyale et licite des données à caractère personnel, qui ne peut s'effectuer à l'insu de la personne concernée.

ii) Spécification des finalités

La même disposition de la Loi sur l'accès exige une information de la personne concernée quant à l'usage auquel le renseignement est destiné, ce qui implique non seulement que la finalité des données collectées soit explicite mais aussi qu'elle ait été déterminée au préalable. Quant au principe de légitimité de la finalité, on peut supposer que puisque la Loi s'applique aux documents détenus par un organisme public dans le

---

[362] Voir, par exemple, Boucher c. Office du crédit agricole du Québec, [1986] C.A.I. 372, 375-76, cité par P.A. Comeau et A. Ouimet, "Freedom of Information and Privacy: Québec's Innovative

cadre de ses fonctions, la légitimité des finalités poursuivies est garantie par la légitimité même de l'acte instituant l'organisme public et déterminant ses fonctions[363].

iii) Limitation de l'utilisation

La limitation de l'utilisation des données aux seuls traitements dont les finalités sont compatibles avec celles qui ont été déterminées lors de la collecte initiale est également garantie par le lien nécessaire entre la détention du document et les fonctions de l'organisme public[364].

iv) Qualité et proportionnalité des données

Le principe de qualité des données implique de limiter les données traitées au seules données nécessaires à la poursuite de la finalité poursuivie. Ce principe est inscrit à l'article 64 de la Loi sur l'accès en vertu duquel *"nul ne peut, au nom d'un organisme public, recueillir un renseignement nominatif si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en oeuvre d'un programme dont il a la gestion[365]"*. En outre, la Loi précise qu'*"un organisme public doit veiller à ce que les renseignements nominatifs qu'il conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis"*[366].

v) Garanties de sécurité

Role in North America", (1995) 80 Iowa L.R. 3.

363 Ce principe renvoit à l'article 7 de la Directive européenne qui admet le traitement de données à caractère personnel, s'il est *"nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis"* ou s'il *"est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées"*.

364 *"Le document doit être détenu par un organisme public ou pour son compte, dans l'exercice des fonctions de l'organisme"* (article 1 § 1 de la Loi sur l'accès).

365 Pour des cas d'application, voir Commission d'accès à l'information du Québec, "Rapport annuel 1991-1992", (1992) L'accès 1, p. 3.

366 Article 72 de la Loi sur l'accès.

Les mesures de sécurité à respecter permettent de garantir une certaine protection des données, notamment contre l'accès, la modification ou la diffusion non autorisés. Bien qu'aucune disposition spécifique n'exige de la part de l'organisme public détenant des documents contenant des données nominatives, un niveau de sécurité déterminé, on peut supposer que des mesures soient prises à cet égard[367] dans la mesure où l'article 76 de la Loi exige que la déclaration auprès de la Commission d'accès à l'information[368] mentionne *"les mesures de sécurité prises au sein de l'organisme pour assurer le caractère confidentiel des renseignements nominatifs et leur utilisation suivant les fins pour lesquelles ils ont été recueillis"*. Cette disposition ne semble cependant pas pouvoir à elle seule garantir un niveau de sécurité pour les données à caractère personnel, sauf le renvoi au principe de responsabilité en cas de manquement à cette exigence.

---

[367] Par exemple, les mesures de sécurité présentées par la Commission d'accès à l'information à l'intention des organismes du réseau de la santé et des services sociaux (Commission d'accès à l'information du Québec, "Informatisation des dossiers contenant des renseignements confidentiels: la CAI adopte des mesures de sécurité" (1992) 7 L'accès 1.

[368] Requise lors de la constitution d'un fichier de renseignements personnels; voir M.P. Bouchard, "Loi sur l'accès québécoise: principes, structures et recours, à la lumière des législations d'autres juridictions provinciales", dans *Développements récents en droit de l'accès à l'information (1991), Coswanville*, éd. Yvon Blais, 1991, p. 8.

vi) Transparence

L'article 76 de la Loi sur l'accès requiert que tout établissement d'un fichier fasse l'objet d'une déclaration auprès de la Commission d'accès à l'information. Cette exigence, couplée avec celle de l'article 65 portant sur l'information à fournir à la personne concernée lors de la collecte d'un renseignement personnel, contribue à assurer une certaine transparence pour la personne quant à l'usage de ses données.

Le principe de transparence, tel qu'identifié[369], exige également que la personne puisse prendre connaissance des données la concernant et obtenir, le cas échéant, la rectification, l'effacement, ou le verrouillage. Ce droit constitue l'un des principaux volets de la Loi sur l'accès qui accorde à toute personne un droit d'accès aux documents des organismes publics[370], soit par le biais d'une consultation des documents, soit par l'obtention d'une copie de ceux-ci. L'accès à un document est, en principe, gratuit.

A ce principe existent certaines exceptions, la plupart facultatives, prévues par la Loi sous six classifications générales, en ce qui concerne les renseignements ayant une incidence sur les relations intergouvernementales, sur les négociations entre organismes publics, sur l'économie, sur l'administration de la justice et la sécurité publique, sur les décisions administratives ou politiques et sur la vérification[371].

---

[369] *Supra*, Section 2 - la Directive européenne - *Sous-section 3 - Flux transfrontières de données à caractère personnel*, Paragraphe 2 - Notion de Protection adéquate, Sous-paragraphe 1 - Principes fondamentaux, 1 - Principes de base de la protection *vi) Principe de transparence*.

[370] L'accès à un document est, en principe, gratuit Article 9 de la Loi sur l'accès. *"Toutefois, des frais n'excédant pas le coût de sa transcription, de sa reproduction ou de sa communication peuvent être exigées du requérant"* (article 11, § 2 de la Loi sur l'accès).

[371] Voir Chapitre II, Section II de la Loi intitulée *"Restrictions au droit d'accès"*. Ces restrictions sont proches de celles prévues à l'article 13 de la Directive européenne; pour plus de développements, voir M.P. Bouchard, *supra* note 368, pp. 9-22 et Y. D. Dussault, *supra* note 359, pp. 91-107.

Quant au droit de rectification, l'article 89 de la Loi précise que *"toute personne qui reçoit confirmation de l'existence dans un fichier d'un renseignement nominatif la concernant peut, s'il est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi, exiger que le fichier soit rectifié*[372]". Dans le cas où le renseignement nominatif est en fait une opinion émise par un tiers au sujet de l'individu, celui-ci n'a pas droit d'en obtenir la correction. Il peut cependant exiger de l'organisme public qui conserve ce renseignement qu'il y adjoigne la demande de rectification, de façon à ce que toute personne qui consulterait ce fichier ait accès à l'opinion et à la demande de rectification.

vii) Participation individuelle

En principe, un organisme public ne peut communiquer à un tiers un renseignement personnel à moins que sa divulgation ne soit autorisée par la personne concernée[373]. Si l'individu dispose ainsi d'un certain contrôle de son "*image informationnelle*" par le biais de son consentement à la transmission des informations, il n'en dispose cependant pas en ce qui concerne l'utilisation initiale de ses données, son consentement n'étant pas requis lors de la collecte des données.

Le principe de consentement à la communication des données n'est cependant pas absolu. Certaines communications de renseignements nominatifs sont légalement permises sans le consentement de la personne concernée dans des cas et selon certaines modalités précisément énoncées, notamment lorsque la communication est nécessaire à l'application d'une convention collective, d'un décret, d'un arrêté, d'une directive ou

---

372 Bien que la loi ne parle que de la rectification des données, il nous semble que dans les cas où la collecte, la communication ou la conservation ne sont pas autorisées par la loi, il s'agit plutôt d'un droit d'obtenir que les données soient supprimées plutôt que d'un droit de demander la rectification de celles-ci.

373 Article 53 de la Loi sur l'accès.

d'un règlement qui établissent des conditions de travail ou lorsque la communication est nécessaire à l'exercice d'un mandat confié par l'organisme public à la personne ou l'organisme qui reçoit l'information[374].

viii) Responsabilité

En vertu de l'article 167 de la Loi sur l'accès, et sauf cas fortuit ou force majeure, la personne concernée pourra obtenir de l'organisme public qui conserve les renseignements personnels, réparation du préjudice subi pour manquement à la confidentialité des données, aux principes régissant soit la collecte, la conservation et l'utilisation des renseignements, soit l'établissement et la gestion des fichiers, soit le respect des droits de la personne concernée par les renseignements.

ix) Détention limitée

Le principe de la détention limitée des données est consacré à l'article 73 de la Loi sur l'accès qui précise que *"lorsque l'objet pour lequel un renseignement nominatif a été recueilli est accompli, l'organisme doit le détruire, sous réserve de la Loi sur les archives"*. A l'exception des données personnelles dont la conservation est requise en vertu d'une loi, la durée de détention des données est donc fonction de la finalité poursuivie. Toutefois, si le renseignement nominatif qui n'a plus d'utilité pour l'organisme public, fait l'objet d'une demande d'accès, le responsable de l'accès de l'organisme doit veiller à sa conservation jusqu'à ce que le demandeur ait épuisé ses recours[375].

Sous-paragraphe 2 - Autres critères

Contrairement à la Directive européenne qui identifie un certain nombre de *"traitements à risque"*, nécessitant un niveau de protection renforcée, la Loi sur l'accès ne contient

---

374 Voir les articles 67 et suivants de la Loi sur l'accès.

375 Article 102.1 de la Loi sur l'accès.

pas de dispositions particulières portant sur les données sensibles. Ceci n'implique cependant pas qu'il n'existe aucune protection en la matière, des règles particulières, telles celles existant dans le domaine de la santé, pouvant être consacrées par des législations spécifiques.

Paragraphe 3 - Règles d'effectivité

La Loi sur l'accès prévoit un certain nombre de garantie assurant la mise en oeuvre concrète des principes énoncés.

Les droits de la personne concernée et les obligations de l'organisme public responsable du fichier dans le secteur public sont consacrés par un texte loi, porté à la connaissance des intéressés[376]. Par ailleurs, tout individu dispose non seulement d'un droit de révision auprès de la Commission d'accès à l'information[377] en cas de refus d'une demande, formulée par écrit[378], d'accès aux documents[379] mais également d'un droit de recours si elle souffre d'un préjudice à la suite de la décision d'un organisme public de ne pas

---

376 Voir en ce qui concerne le rôle de la Commission en matière de prise de connaissance par les personnes concernées de leurs droits, *infra*, *Sous-section 3 - la Loi sur la protection des renseignements personnels dans le secteur privé*, Paragraphe 3 - Règles d'effectivité, Sous-paragraphe 2 - la commission d'accès à l'information; pour plus de développements, voir D.H. Flaherty, *Protecting Privacy in Surveillance Societies: the Federal Republic of Germany, Sweden, France, Canada and the United States*, Chapel Hill, The University of North Carolina Press, 1989.

377 *Infra*, *Sous-section 3 - La loi sur la protection des renseignements dans le secteur privé*, Paragraphe 3 - Règles d'effectivité, Sous-paragraphe 2 - La Commission d'accès à l'information.

378 Article 135 de la Loi; Commission d'accès à l'information du Québec, *supra* note 365, *ibid.*

379 La demande de révision doit être faite dans les 30 jours suivant le rejet, explicite ou présumé, de la demande d'accès ou de rectification (article 135 de la Loi sur l'accès). Le rejet d'une demande se présume si aucune réponse écrite n'a été reçue dans les délais légaux (articles 52 et 102 de la Loi sur l'accès). La demande de révision de la décision de l'organisme public de communiquer un document malgré l'opposition du tiers concerné doit être formulée dans les 15 jours de l'avis donné par l'organisme au tiers (article 136 de la Loi sur l'accès).

corriger, à sa demande, les données qui la concerne[380]. L'effectivité de la protection offerte aux renseignements personnels est ainsi assurée par la Commission d'accès à l'information qui, avant même l'adoption de la loi 68 et intervenue, à diverses reprises, dans le secteur privé[381].

Des sanctions pénales sont également prévues à l'égard de quiconque refuse ou entrave sciemment l'accès à un document ou à un renseignement ou qui accorde sciemment l'accès à un document ou à un renseignement dont la loi ne permet pas la communication[382].

SOUS-SECTION 3 - LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVE (LOI 68)[383]

Paragraphe 1 - Champ d'application

Première législation d'Amérique du Nord visant à réglementer la détention et l'utilisation de données à caractère personnel dans le secteur privé[384], la Loi 68[385]

---

380 Article 166 de la Loi sur l'accès.

381 La Commission d'accès à l'information s'inquiétait déjà en 1987 des passerelles de communication des renseignements personnels entre le secteur public régi par la Loi d'accès et le secteur privé non réglementé (Commission d'accès à l'information, *Une vie privée mieux respectée, un citoyen mieux informé*, Rapport sur la mise en oeuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, Les Publications du Québec, 1987; voir A. Ouimet, *supra* note 43, pp. 191 194).

382 Articles 158 et suivants de la Loi sur l'accès.

383 L.Q. 1993, c. 17 [ci-après *Loi 68*].

384 En 1986, le Groupe de recherche informatique et droit (GRID) publiait une étude portant sur les banques de données à caractère personnel constituées par le secteur privé québécois (Groupe de recherche informatique et droit (R.D. Bureau, R. Laperrière, J.P. Lemasson, J. Martin et J.P. Péladeau), *L'identité piratée*, Montréal, SOQUIJ (société québécoise d'information juridique) 1986; voir également P. Péladeau et R. Laperrière, *Le droit sur la protection des renseignements personnels - étude sur les bases privées de données à caractère personnel en droit canadien,*

s'applique à toutes les entreprises privées opérant dans la province, au sens de l'article

---

comparé et international, Montréal, SOQUIJ, 1986; J.P. Lemasson, J. Martin, P. Péladeau et R. Laperrière, *Les renseignements personnels et l'ordinateur enquête sur la situation des bases de données à caractère personnel dans le secteur privé québécois*, Montréal, SOQUIJ, 1986; P. Mackay, P. Péladeau et R. Laperrière, *Droit, informatique et vie privée: bibliographie sélective, canadienne et internationale*, Montréal, SOQUIJ, 1986. Ces recommandations soulignaient "*la nécessité d'une intervention publique dans le secteur privé, sous la forme de l'adoption de normes générales inspirées de celles de l'O.C.D.E., et d'une législation spécifique consacrant les droits des citoyen(ne)s à l'information, au consentement, à la contestation des données, traitements, divulgations et décisions, et assurant la promotion des droits démocratiques au débat public, au contrôle des développements technologiques et à la maîtrise sociale de l'informatisation. Elles préconisent que la mise en oeuvre de ces normes et politiques soit confiée à un organisme public spécialisé ayant notamment pour mission d'offrir une expertise publique, de faire respecter la loi et d'assurer une coordination des efforts d'auto-réglementation des secteurs privés et une participation adéquate des représentants du public, des entreprises, des groupes intermédiaires et de l'Etat*" (R. Laperrière, *La protection des renseignements personnels dans le secteur privé*. Résumé du mémoire soumis à la Commission de la culture de l'Assemblée nationale du Québec, GRID, 10 février 1988, p. 2 et version révisée (4 mars 1993)).

En 1989, le Comité interministériel sur la protection de la vie privée eu égard aux banques de données personnelles recommandait "*que le gouvernement du Québec prenne l'initiative d'une intervention publique visant à protéger les droits des personnes à leur vie privée dans le secteur privé en occupant le champ de compétence du Québec en la matière*" (Ministère de la Justice, *La vie privée: zone à accès restreint*, Synthèse du rapport du Comité interministériel sur la protection de la vie privée eu égard aux banques de données à caractère personnel, Québec, avril 1989). La principale divergence du Comité interministériel à l'égard des recommandations du GRID portait sur l'opportunité de créer un organisme de contrôle pour le secteur privé distinct de la Commission d'accès à l'information (R. Laperrière, "La protection des renseignements personnels dans le secteur privé au Québec et le projet de loi 68", Conférence de l'UQUAM sur la protection des renseignements personnels: bilans et enjeux, Montréal, 16 avril 1993, p. 2).

La nécessité d'adopter une loi pour régir les activités informationnelles du secteur privé a été évoquée, à diverses reprises, par la Commission d'accès à l'information et par la Commission de la culture de l'Assemblée nationale du Québec (Commission de la culture, *La vie privée, un droit sacré*, Québec, Assemblée nationale, juin 1988) et par le Groupe de travail du Ministère des Communications (Rapport du Groupe de travail sur la commercialisation des banques de données des organismes publics, Ministère des Communications du Québec, Québec, 1991, *supra* note 74). Pour une analyse critique du projet de loi 68, voir R. Laperrière, "La protection des renseignements personnels dans le secteur privé au Québec et le projet de loi 68", *ibid*, p. 4 et s.; R. Laperrière, *Le projet de loi 68 sur la protection des renseignements personnels dans le secteur privé*. Mémoire soumis à la Commission de la culture de l'Assemblée nationale du Québec, Québec, février 1993.

385 Adoptée le 15 juin 1993 par l'Assemblée nationale du Québec; voir L. Dandurand, "L'accès à l'information dans un débat démocratique" (1996) 16 Paroles de droit (Bulletin de la Fondation canadienne des droits de la personne) 5; V. Steeves, "Humaniser l'espace cybernétique: la vie privée, la liberté d'expression et l'autoroute de l'information", (1995) 28 Droits de la personne 1, p. 3.

1525 du Code civil du Québec[386] qui directement ou indirectement recueillent, détiennent, utilisent ou communiquent à des tiers des renseignements personnels, quelle qu'en soit l'origine. Sont ainsi protégées les données relatives à toute personne résidant ou non au Québec.

La Loi exclut toutefois de son champ d'application les données à caractère personnel collectées, détenues, utilisées ou communiquées à des fins journalistiques[387], ce qui pourrait poser problème au regard de la Directive européenne. Celle-ci s'applique en effet à ce type de traitement, sauf exceptions spécifiquement prévues par les Etats membres[388].

Par *"renseignement personnel"*, l'article 2 de la Loi 68 entend toute information qui peut être directement ou indirectement rattachée à un individu identifié ou identifiable, quelle que soit la nature du support et quelle que soit la forme sous laquelle elle est accessible (écrite, graphique, sonore, visuelle, informatisée ou autre)[389]. Dans cette mesure, toute personne qui exploite une entreprise et recueille à cette fin des renseignements personnels, est automatiquement assujettie aux prescriptions de la Loi sur la protection des renseignements personnels dans le secteur privé.

---

386 *"Constitue l'exploitation d'une entreprise l'exercice par une ou plusieurs personnes, d'une activité économique organisée, qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services"*.

387 Article 1 de la Loi 68.

388 Les Etats membres peuvent prévoir des exemptions et dérogations à certains principes uniquement dans la mesure où celles-ci s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression.

389 Article 1, § 2 de la Loi 68. Cette définition est identique à celle contenue dans la Loi sur l'accès du secteur public (*supra*, *Sous-section 2 - La loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, Paragraphe 1 - Champ d'application).

Paragraphe 2 - Principes fondamentaux

Sous-paragraphe 1 - Principes de base de la protection

i) Principe de collecte loyale et licite

Ce principe de limitation en matière de contenu est prévu à l'article 5 de la Loi 68 en vertu duquel "*les renseignements doivent être recueillis par des moyens licites*", c'est-à-dire pas à l'insu de la personne concernée.

ii) Spécification des finalités

L'article 4 de la Loi 68 impose aux entreprises privées qui, en raison d'un intérêt légitime et sérieux constituent un dossier sur autrui, d'y inscrire *"l'objet"*. Si la Loi ne définit pas ce qu'il faut entendre par l'objet d'un dossier, on peut raisonnablement penser que celui-ci à trait à l'utilisation qui sera faite des renseignements. Il s'agit donc bien d'une obligation de détermination des finalités poursuivies.

La Loi ne précise pas davantage ce qu'il faut entendre par *"un intérêt légitime et sérieux"* autorisant la constitution d'un dossier[390]. L'exigence de légitimité de la finalité reste donc imprécise en l'absence de moyens de contrôle de cette légitimité expressément énoncés.

Précisons en ce qui concerne la détermination de la finalité, qu'en vertu de l'article 9 de

---

[390] Que mentionne l'article 37 du Code civil. "*Ne devraient être légitimes que les dossiers constitués et les renseignements collectés du consentement exprès de la personne concernée, ou en vertu d'une autorisation spécifique de la loi, ou pour donner effet à une relation d'affaires directe avec la personne concernée*" (R. Laperrière, "La protection des renseignements personnels dans le secteur privé au Québec et le projet de Loi 68", *supra* note 384, pp. 10-11); voir H.P. Glenn, "Le droit en l'an 2000: L'envahissement des contrôles gouvernementaux et des technologies nouvelles dans la vie privée des citoyens", *supra* note 104, p. 710.

la Loi, une entreprise ne peut refuser de fournir des biens ou des services ou d'acquiescer à une demande relative à un emploi en raison du refus de la personne concernée de fournir un renseignement personnel, sauf si ce renseignement est nécessaire à la conclusion ou à l'exécution du contrat, si la collecte est autorisée par la loi ou encore si l'entreprise a des motifs raisonnables de croire que la demande de biens, de services ou d'emploi n'est pas licite[391]. La nécessité de l'information pour la conclusion ou l'exécution d'un contrat ainsi que l'existence d'une loi, peuvent dès lors servir à fonder la collecte de données à caractère personnel dans le cadre contractuel de fourniture de biens et services ou d'un contrat d'emploi.

La Loi exige que l'objet soit explicite dans la mesure où la personne qui recueille des informations personnelles auprès de la personne concernée, est tenue d'informer celle-ci de l'objet du dossier au moment de sa constitution[392].

iii) Limitation de l'utilisation

L'exigence de limitation de l'utilisation des données à caractère personnel aux seules fins compatibles avec les finalités qui ont été déterminées, légitimes et rendues explicites lors de la collecte initiale est précisée à l'article 13 de la Loi 68 qui dispose qu'*"une entreprise, ne peut sans le consentement de la personne concernée, utiliser les renseignements personnels contenus dans un dossier à des fins non pertinentes avec*

---

391 Nous retrouvons ici certains critères énoncés à l'article 7 de la Directive européenne en vertu duquel le traitement de données à caractère personnel peut être effectué notamment s'*"il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci"* ou s'*"il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis"*.

392 Article 8 de la Loi 68; R. Laperrière, "La protection des renseignements personnels dans le secteur privé au Québec et le projet de Loi 68", *supra* note 384, p. 10 *"Contrairement à la loi d'accès qui vise à contrôler les renseignements et leur ordonnancement en fichiers dans le secteur public, le projet de loi 68 ne vise que les dossiers et les renseignements qu'ils contiennent. Aucune norme ne vient régir la constitution et la question des fichiers, non plus que les traitements (...). Presque rien ne permet de contester les traitements, les critères et raisonnements sur lesquels ils sont fondés, et les décisions automatiques auxquels ils conduisent"*.

l'objet de ce dossier, à moins que la présente loi ne le prévoit".

iv) Qualité et proportionnalité des données

En vertu de l'article 5 de la Loi 68, la personne qui recueille des renseignements personnels afin de constituer un dossier sur autrui ou d'y consigner de tels renseignements, ne doit recueillir que des renseignements nécessaires à l'objet du dossier. Est ainsi consacré le principe de proportionnalité des données qui implique de limiter les données traitées au seules données nécessaires à la poursuite de la finalité poursuivie.

En outre, toute personne qui exploite une entreprise doit veiller à ce que les dossiers qu'elle détient sur autrui soient à jour et exacts, au moment où elle les utilise pour prendre une décision relative à la personne concernée. Si une mise à jour constante des dossiers n'est pas requise, celle-ci pouvant intervenir au moment de la prise de décision, en pratique, les entreprises veilleront à mettre régulièrement à jour les informations qu'elles détiennent sur une personne afin de pouvoir prendre rapidement leurs décisions la concernant.

Soulignons que ce principe, énoncé à l'article 11 de la Loi 68, pourrait avoir une portée limitée dans la mesure où une mise à jour ne semble pas exigée en cas de détention de données à caractère personnels à des fins d'archivage ou de statistiques ou, en cas de détention de fichiers à des fins de cession à des tiers par des entreprises qui ne sont pas chargées de prendre une décision. Même si aucune décision ne doit être prise dans ces cas, il est essentiel que les données soient exactes et mises à jour.

v) Garanties de sécurité

L'article 10 de la Loi 68 dispose que *"toute personne qui exploite une entreprise et recueille, détient, utilise ou communique des renseignements personnels sur autrui doit*

prendre et appliquer des mesures de sécurité propres à assurer le caractère confidentiel des renseignements". La loi prévoit donc l'adoption de mesures de sécurité visant à garantir une certaine protection des données, notamment contre l'accès, la modification ou la diffusion non autorisés.

vi) Transparence

L'exigence de l'information de la personne concernée est reprise à l'article 8 de la Loi 68 qui précise que la personne qui recueille des renseignements personnels auprès de la personne concernée doit, lorsqu'elle constitue un dossier sur cette dernière, l'informer de l'objet du dossier, de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise, de l'endroit où sera détenu son dossier ainsi que de ses droits d'accès ou de rectification. Par ailleurs, la source des renseignements doit être indiquée lorsque la personne qui constitue un dossier sur autrui ou qui y consigne des renseignements personnels, recueille de tels renseignements auprès de tiers, lequel exploite une entreprise. Une certaine transparence quant à l'origine des renseignements est donc requise[393].

Le principe de transparence, tel qu'identifié[394], exige également que la personne puisse elle-même prendre connaissance des données la concernant et obtenir, le cas échéant, la rectification, l'effacement ou le verrouillage. Ce droit est reconnu par l'article 27 de la Loi 68 qui consacre le droit pour toute personne non seulement d'obtenir confirmation de l'existence de renseignements à son sujet, mais également d'en obtenir la

---

[393] La Loi va plus loin que la Directive européenne à cet égard puisque celle-ci ne requiert une information sur la source des renseignements que si cette information peut être considérée *"nécessaire pour assurer à l'égard de la personne concernée un traitement loyal des données"* (articles 10 et 11 de la Directive européenne).

[394] *Supra*, Section 2 - La Directive européenne, *Sous-section 3 - Flux transfrontières de données à caractère personnel*, Paragraphe 2 - Notion de protection adéquate, Sous-paragraphe 1 - Principes fondamentaux, 1 - Principes de base de la protection, *vi) Transparence*.

communication[395]. La personne concernée dispose du droit de rectification de renseignements inexacts, incomplets ou équivoques[396]. L'entreprise qui procède à une rectification doit la notifier à toute personne qui a reçu communication des renseignements au cours des six mois précédant la rectification, ainsi qu'à celles qui ont fournis les renseignements personnels[397].

Les droits d'accès et de rectification s'exercent par simple demande écrite. Le droit d'accès est en principe gratuit, des frais raisonnables pouvant cependant être exigés pour la transcription, la reproduction ou la transmission de renseignements personnels[398]. Enfin, selon l'article 29 de la Loi, la personne qui exploite une entreprise et qui détient des dossiers sur autrui doit prendre les mesures nécessaires notamment pour assurer l'exercice des droits d'accès et de rectification. Elle doit, par exemple, porter à la connaissance du public le lieu où les dossiers sont accessibles et les moyens d'y accéder. La mise en oeuvre effective des droits de la personne concernée est ainsi légalement consacrée.

vii) Participation individuelle

Ce principe est consacré par la place prééminente accordée dans la Loi 68 au consentement de la personne concernée qui, "*manifeste, libre, éclairé et donné a des fins spécifiques*" est requis non seulement pour la communication de données

---

[395] La Loi prévoit certaines restrictions au droit d'accès notamment lorsque, de l'avis d'un professionnel de la santé, la consultation du dossier médical causerait un préjudice grave pour la santé de l'individu; ou lorsque la divulgation de renseignements au sujet d'une personne risquerait de révéler des renseignements personnels au sujet de tiers (articles 37 et suivants de la Loi 68).

[396] Voir l'article 28 de la Loi qui renvoit à l'article 40 du Code civil du Québec.

[397] Article 40 du Code civil du Québec.

[398] Article 33 de la Loi 68.

personnelles à un tiers[399], mais également pour toute utilisation des données à des fins non pertinentes à l'objet du dossier[400]. Le consentement est également requis pour toute conservation et utilisation des données, une fois l'objet du dossier accompli, sous réserve du délai prévu par la loi ou par le gouvernement[401]. Toutefois, le consentement de la personne concernée n'est pas requis lors de la collecte et de l'utilisation initiale des données, ce qui limite sensiblement la réelle maîtrise de l'individu sur son "*image informationnelle*"[402].

La personne concernée se voit cependant reconnaitre un droit d'obtenir la suppression d'un renseignement périmé ou non justifié par l'objet du dossier, ou dont la collecte n'est pas autorisée par la Loi[403].

viii) Responsabilité

La Loi 68 ne contient aucune disposition portant sur l'obligation pour l'entreprise qui détient des renseignements personnels de réparer le préjudice résultant d'un traitement illicite ou d'une action contraire aux principes de base de la protection mise en place[404].

---

399 La Loi 68 prévoit toutefois des exceptions où il sera permis à la personne qui exploite une entreprise de communiquer à des tiers des renseignements personnels sans obtenir le consentement de la personne concernée. Mentionnons notamment la communication à une personne chargée de prévenir, détecter ou réprimer le crime et la communication de renseignements personnels dans des situations d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée (article 18 de la Loi 68).

400 Article 14 de la Loi 68.

401 Article 12 de la Loi 68.

402 Sur la validité du consentement, voir R. Laperrière, "La protection des renseignements personnels dans le secteur privé au Québec et le projet de Loi 68", *supra* note 384, p. 11.

403 Article 28 de la Loi et article 40 du Code civil du Québec.

404 En ce qui concerne le projet de Loi 68, R. Laperrière écrivait déjà: "*Il faudrait (...) s'assurer que les entreprises qui reçoivent et traitent des renseignements soient solidairement tenues envers les personnes concernées aux mêmes obligations que celles de qui elles les ont obtenues* (...)" (R. Laperrière, "La protection des renseignements personnels dans le secteur privé au Québec et le

Une personne ayant subi un dommage pourrait cependant invoquer le régime de droit commun en matière de responsabilité, conformément aux articles 35 à 40 du Code civil du Québec.

ix) Détention Limitée

L'article 12 de la Loi 68 limite l'utilisation des renseignements contenus dans un dossier, à l'accomplissement de l'objet du dossier accompli, sauf consentement de la personne concernée et sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement.

---

projet de Loi 68", *supra* note 384, p. 11).

Sous-paragraphe 2 - Autres critères

L'existence dans la législation d'un pays tiers d'une protection particulière pour les traitements considérés comme pouvant entraîner un risque particulier pour la personne concernée[405] peut exercer une influence sur l'adéquation de la protection offerte dans ce pays, si pas de manière générale, à tout le moins en ce qui concerne certaines catégories de transferts de données.

A cet égard, la Loi 68 prévoit des mesures particulières pour la communication à des tiers de listes de noms, d'adresses ou de numéros de téléphone de personnes physiques servant à des fins de prospection commerciale ou philanthropique[406]. Moyennant le respect de certaines conditions, une personne qui exploite une entreprise peut, sans le consentement des personnes concernées, utiliser à des fins de prospection commerciale ou philanthropique, une liste nominative de ses clients, de ses membres ou de ses employés. La Loi consacre cependant un régime, qualifié d'*"opting out"*, selon lequel les personnes inscrites sur une liste doivent se voir offrir à la première occasion, la possibilité de retrancher leur nom[407].

Si la Loi 68 ne contient pas de dispositions précises en ce qui concerne les données sensibles, à l'instar de la Loi sur l'accès, elle n'exclut nullement l'application de

---

[405] Que prévoit la Directive européenne, *supra*, Section 2 - La Directive européenne, *Sous-section 3 - Flux transfrontières de données à caractère personnel*, Paragraphe 2 - Notion de protection adéquate, Sous-paragraphe 1 - Principes fondamentaux, 2 - Autres critères.

[406] Articles 23 et suivants de la Loi 68.

[407] Ce régime est comparable à celui de l'article 14 de la Directive européenne qui nous paraît cependant plus large dans sa reconnaissance d'un droit d'opposition en cas de traitement de données à des fins de prospection; voir R. Laperrière, "La protection des renseignements personnels dans le secteur privé au Québec et le projet de Loi 68", *supra* note 384, pp. 11 et 12: *"Les exemptions à l'obtention du consentement de la personne pour la communication de renseignements à des tiers sont encore trop largement définies, à l'encontre du principe de la limitation des exceptions énoncé à l'article 4 des lignes directrices de l'O.C.D.E."*.

législations spécifiques, prévoyant des mesures de protection des renseignements personnels dans des secteurs particuliers.

Les règles existantes dans un pays tiers et régissant le transfert de données vers un autre pays peuvent également garantir, une certaine protection des données à caractère personnel visée par la Directive européenne. Un pays tiers considéré comme un pays de destination finale peut en effet être amené à transférer les données vers un troisième pays n'offrant pas une protection correspondant aux critères de la Directive européenne. La Loi 68 ne prévoit de garanties que pour les renseignements relatifs à des personnes résidant au Québec[408]. Afin que la législation québécoise puisse être considérée comme adéquate à cet égard, il conviendra dès lors soit de modifier cet article de manière à accorder une protection aux renseignements provenant de pays tiers, tels ceux de l'Union européenne, soit de prendre en considération dans l'analyse de l'adéquation de la protection offerte le fait que le Québec est le pays de destination finale.

Paragraphe 3 - Règles d'effectivité

Sous-paragraphe 1 - Droit de recours et sanctions

Les droits de la personne concernée et les obligations de toute personne exploitant une entreprise et détenant à cette fin des renseignements personnels sont consacrés par un texte de loi porté à la connaissance des intéressés. Afin de garantir l'effectivité des principes de protection énoncés dans la Loi 68, celle-ci prévoit un droit de recours de la

---

[408] Article 17 de la Loi 68; déjà à propos du projet de loi 68, R. Laperrière écrivait: "*Le projet ne contient aucune disposition pertinente au contrôle des flux transfrontières de données personnelles. (...) Il nous faudra alors démontrer non seulement que nous ne laissons pas couler nos renseignements sans protection à l'étranger, mais aussi que nous accordons aux renseignements étrangers que nous traitons une protection adéquate ou équivalente à celle dont ils bénéficient dans leur pays de provenance*" (R. Laperrière, "La protection des renseignements personnels dans le secteur privé au Québec et le projet de Loi 68", *supra* note 384, p. 12).

personne concernée auprès de la Commission d'accès à l'information du Québec[409], compétente pour entendre des différends résultant du refus d'acquiescer à une demande d'accès ou de rectification[410]. Elle peut notamment ordonner à une personne exploitant une entreprise de donner communication ou de rectifier un renseignement ou de s'abstenir de le faire[411]. Conformément à l'article 61 de la Loi 68, la personne concernée peut interjeter appel d'une décision de la Commission devant la Cour du Québec sur toute question de droit ou de compétence.

Dans le but d'assurer le respect de la loi, des sanctions pénales sévères sont prévues à l'encontre des entreprises et de leurs administrateurs, dirigeants ou représentants qui contreviendraient à ces dispositions[412].

Sous-paragraphe 2 - La Commission d'accès à l'information

Créée initialement lors de l'élaboration de la Loi sur l'accès aux documents des organismes publics[413], ses pouvoirs ont été étendus lors de l'adoption de la Loi sur la protection des renseignements personnels dans le secteur privé. Composée de quatre membres et d'un président nommés par l'Assemblée Nationale, la Commission dispose de pouvoirs de décision, de surveillance et de contrôle[414].

Lorsque la personne concernée n'est pas satisfaite de la réponse obtenue d'un organisme

---

409 *Infra*, Sous-paragraphe 2 - La Commission d'accès à l'information.

410 Article 42 de la Loi 68; rappelons que la Commission d'accès à l'information du Québec exerce déjà une compétence semblable en matière de documents et renseignements détenus par des organismes du secteur public.

411 Article 55 de la Loi 68.

412 Articles 91 à 93 de la Loi 68.

413 Voir l'article 103 de la Loi sur l'accès.

414 Voir les articles 122 et suivants de la Loi sur l'accès.

public ou d'une entreprise privée à la suite d'une demande, formulée par écrit, d'accès à des documents ou à des renseignements nominatifs, ou à la suite d'une demande de rectification de renseignements la concernant, elle peut demander à la Commission qui dispose à cet égard d'une compétence exclusive, de réviser cette décision[415]. Si la Commission ne dispose pas du pouvoir de divulguer les documents, elle peut néanmoins en donner l'ordre à l'organisme public[416]. Ses décisions sur des questions de droit ou de compétence[417] sont susceptibles d'appel auprès de la Cour du Québec[418].

La Commission assume également une fonction de surveillance de l'application de la législation dans le secteur tant public que privé. Elle est investie à cet égard de larges pouvoirs d'enquête[419]. Ainsi, elle pourra de sa propre initiative ou à la demande de la personne concernée procéder à une enquête ou charger une personne de procéder à une enquête sur toute question relative à la protection des renseignements personnels ainsi que sur les pratiques de l'entreprise en cette matière. Au terme de cette enquête, la Commission pourra recommander ou ordonner l'application de mesures correctives propres à assurer la protection des renseignements personnels.

---

415 Commission d'accès à l'information du Québec, *Rapport annuel 1991-1992*, Les publications du Québec, 1992, p. 1: "*Lors de la révision, l'organisme ne pourra ajouter de nouveaux motifs de refus à la réponse du responsable de l'accès [sauf circonstances exceptionnelles]. Il en ira de même si l'organisme porte en appel, devant la Cour du Québec, une décision de la Commission; (...) En d'autres termes, l'organisme a choisi les paramètres juridiques sur lesquels est fondé son refus et la portée du litige*"; sur la procédure, voir également M.P. Bouchard, *supra* note 368, p. 23.

416 "*Lorsque la commission d'accès ordonne à l'organisme public de faire quelque chose, cette décision devient exécutoire à l'expiration d'un délai de 30 jours, à moins qu'appel n'en ait été interjeté. Quant aux décisions enjoignant l'organisme public à s'abstenir de faire quelque chose, elles sont exécutoires dès le moment de leur transmission à l'organisme public*" (M.P. Bouchart, *supra* note 368, pp. 23-24).

417 Sous réserve des questions de faits recevant de sa compétence (article 146 de la Loi sur l'accès).

418 Article 147 de la Loi sur l'accès et article 61 de la Loi 68. La décision de la Cour est sans appel (article 154 de la Loi sur l'accès).

419 Voir articles 127 et suivants de la Loi sur l'accès et articles 81 et suivants de la Loi 68.

La Commission est également chargée d'étudier les déclarations de fichiers de renseignements personnels détenus par les organismes publics, les communications de renseignements nominatifs effectuées sans le consentement des personnes concernées ainsi que les demandes d'obtention de ces renseignements à des fins d'études, de recherches et de statistiques.

Enfin, la Commission joue un rôle actif dans l'information des personnes concernées de leurs droits et le respect par les organismes responsables de leurs obligations. Elle peut à cet effet initier des séminaires, conférences et autres activités et donner son avis sur les problèmes pratiques que rencontrent les organismes publics et les entreprises[420].

Paragraphe 4 - Mise en Oeuvre

Certaines failles peuvent être relevées dans la transposition des principes de base à l'assurance d'une protection adéquate au sens de la Directive européenne.

En effet, le principe de la légitimité de la finalité que consacre la Loi 68, ne fait l'objet d'aucune précision sur ce qui pourrait fonder cette légitimité[421] , ni sur les moyens de contrôle de celle-ci. En ce qui concerne la qualité des données détenues par des entreprises privées, l'exigence d'exactitude et de mise à jour n'est pas requise lorsque la société ne prend pas de décisions relatives aux personnes concernées. De même, rien dans la loi ne restreint la collecte ou la divulgation de données sensibles. Enfin, si la législation dans le secteur tant public que privé accorde une certaine maîtrise de l'individu sur ses données personnelles, notamment par le biais de son consentement à

---

[420] Voir notamment, Commission d'accès à l'information du Québec, "Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la santé et des services sociaux", (1992) 8 L'accès 22.

[421] Sous réserve du consentement "*éclairé*" de la personne concernée; voir H.P. Glenn "Le droit en l'an 2000: L'envahissement des contrôles gouvernementaux et des technologies nouvelles dans la vie privée des citoyens", *supra* note 104, pp. 710-711.

la communication de ses données, celui-ci n'est cependant pas requis lors de l'utilisation initiale des données ni, dans certaines circonstances, lors de la communication de ses données à des tiers. La Loi ne contient pas davantage de disposition pertinente au contrôle des flux transfrontières de données personnelles, ce qui pourrait poser problème au regard de la protection adéquate requise par la Directive européenne, notamment si le Québec n'est pas le pays destinataire des données.

L'effectivité de la législation du Québec, sous réserve de quelques modifications, semble cependant garantie dans le secteur tant public que privé[422], notamment par les larges pouvoirs accordés à la Commission d'accès à l'information du Québec[423].

CHAPITRE 3 - LES CODES DE CONDUITE

Les codes de conduite s'entendent généralement des règles professionnelles de protection des données ou encore du "*recours aux normes volontairement développées et acceptées par ceux qui prennent part à une activité*"[424].

Comme on l'a souligné[425], "*la nature première des règles autoréglementaires, c'est*

---

[422] "*Les articles 179 et 179.1 de la loi sur l'accès prévoient que la Commission d'accès à l'information doit, tous les cinq ans, faire rapport au gouvernement sur la mise en oeuvre de la loi, ainsi que sur l'opportunité de la maintenir en vigueur ou de la modifier. Ce rapport est par la suite déposé auprès de l'Assemblée nationale qui désigne une commission pour en faire l'étude, notamment en permettant aux personnes et organismes intéressés de se faire entendre sur cette question*" (M.P. Bouchard, *supra* note 368, p.26.

[423] *Adde*: R. Laperrière, "La protection des renseignements personnels dans le secteur privé au Québec et le projet de loi 68", *supra* note 384, p. 15.

[424] P. Trudel, "Les effets juridiques de l'autoréglementation", (1989) 19 Revue de droit de l'Université de Sherbrocke, p. 251.

[425] P. Trudel, "Introduction au droit du commerce électronique sur l'Internet", *supra* note 296, p. 539; *Adde*: U.U. Wuermeling, *supra* note 119, p. 453: "*The codes represent guidance, acceptance in voluntary, and recommandations are not binding*".

d'être volontaires, c'est-à-dire de ne pas être obligatoires au sens où l'est la règle de droit édictée par l'Etat. L'assujettissement à l'autoréglementation est généralement consenti par le sujet".

SECTION 1- LA DIRECTIVE EUROPEENNE

L'article 27.1 et 2 de la Directive Européenne encourage l'élaboration de codes de conduite "*destinés à contribuer en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales prises par les Etats membres en application de la (...) Directive*", et prévoit de manière optionnelle un contrôle de leur conformité à la norme "*supérieure*" par l'autorité nationale de protection des données personnelles[426]. Les codes de conduite se conçoivent donc comme un mode d'expression subordonné aux règles normatives édictées par l'autorité publique. Ils exercent une fonction complémentaire et non exclusive par rapport à une législation nationale existante[427].

Cette définition de la Directive européenne n'est pas partagée par certains Etats tiers, tels les Etats-Unis, le Japon, l'Australie et le Canada, dont le secteur privé est régi par

---

[426] Y. Poullet, "O.C.D.E.: protection des données et de la vie privée", *supra* note 306, p. 83: "*(...) diverses législations, en particulier celle des Pays-Bas, celle d'Irlande, du Royaume-Uni et d'Australie, appuient la promulgation de codes de conduite privés pris par des associations représentatives en application des législations de protection des données*"; U.U. Wuermeling, *supra* note 119, *ibid*: "*The OECD Guidelines promotes the idea of self regulations similar to the codes of conduct in Holland, Ireland and the U.K. (...) The self regulation in the meaning of the OECD Guidelines could be compensated by legislation*". Un contrôle des projets de codes communautaires peut également être exercé par le Groupe de protection des personnes à l'égard du traitement des données à caractère personnel (articles 27 et 30 de la Directive européenne).

[427] U.U. Wuermeling, *supra* note 119, *ibid*: "*In Holland and U.K., codes of conduct have only an illustrative function*"; H. Maisl, *supra* note 198, p. 44: "*La directive, comme les lois nationales, est un texte général. Des textes d'application sont nécessaires, secteur par secteur, pour adapter la réglementation. La CNIL [autorité de contrôle française] assure ce rôle par ses normes simplifiées ou par ses recommandations; récemment, elle a encouragé l'élaboration d'un code de déontologie des professionnels du marketing direct (DIT 95/1); des règles de conduite auxiliaires de la loi, viennent concrétiser celles-ci dans certains secteurs avec le concours des professions concernées et l'accord de l'autorité de contrôle (cfr. H. Maisl DIT 94/3)*".

des codes de conduite autosuffisants, c'est-à-dire ne se référant à aucune norme "*supérieure*", et ne faisant l'objet d'aucun contrôle externe spécifique autre que celui des cours et tribunaux. Si ces systèmes d'auto-réglementation justifient une protection des données personnelles plus souple et plus adaptée aux besoins du secteur, suffisent-ils à assurer une protection adéquate ?

Constituant l'un des instruments énumérés à l'article 25 de la Directive européenne assurant l'effectivité des principes de fond, les code de conduite doivent être créateurs de droits pour les personnes concernées et d'obligations pour le responsable du traitement ainsi que répondre à certaines conditions d'effectivité. Leur effectivité dépendra de leur mode d'élaboration, de la représentativité de l'association, de la connaissance de leur existence permettant à la personne concernée d'exercer un recours et du caractère contraignant et efficace des modes de contrôle et de sanction qui leur sont associés.

SOUS-SECTION 1- ELABORATION

La Directive européenne exige un mode ouvert d'élaboration afin que les codes de conduite ne résultent pas d'une décision unilatérale des seuls représentants du secteur, responsables du traitement, mais permettent à l'ensemble des acteurs intéressés de s'exprimer[428].

Ce processus ne doit pas constituer en une véritable négociation, mais peut prendre la forme d'une audition (*"hearing"*) des personnes intéressées, suivie d'une motivation des décisions prises par rapport aux positions exprimées lors de cette audition.

---

[428] Par exemple, les associations de consommateurs pour les codes de conduite relatifs au marketing direct (pour plus de développements, voir H.M., *supra* note 269, pp. 71 et 59) ou les employés pour les codes de conduite relatifs à la protection des données dans les relations de travail, etc.

SOUS-SECTION 2 - REPRESENTATIVITE

La proposition de Directive exigeait une représentativité au sein des organisations professionnelles et autres associations qui promulguent les codes[429] afin d'éviter qu'ils n'expriment des points de vue minoritaires. Cette condition a été abandonnée par la Directive qui prévoit des garanties tenant à la nécessaire conformité des codes de conduite aux dispositions nationales prises en exécution de la Directive. Il reste que cette condition de représentativité peut être souhaitable là où le code de conduite n'est pas une norme *"subordonnée"*.

SOUS-SECTION 3 - PUBLICITE

Tant les responsables du traitement que les personnes concernées doivent être en mesure de prendre effectivement connaissance de l'existence d'un code de conduite et des procédures de révision. Doivent ainsi être prévues par les sociétés qui adhèrent au code des références explicites, à son existence et à la possibilité d'en obtenir aisément une copie. La publicité du code de conduite permet en effet aux personnes concernées de s'en prévaloir et d'exercer un contrôle collectif (par voie de la presse, de l'opinion publique, de mouvements de consommateurs, etc) en cas de non-respect.

SOUS-SECTION 4 - CONTROLES ET SANCTIONS

Il est essentiel que le code de conduite prévoit des modes de contrôle et de sanctions propres ou externes pour autant, conformément à l'article 28 de la Directive

---

[429] Article 28.2 de la proposition (CEE) modifiée de Directive du Conseil relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel et à la libre circulation de ces données du 15 octobre 1992, *supra* note 193, *ibid*: *"Les projets de codes sont examinés par l'autorité nationale de contrôle, qui assure de leur bien fondé et de la représentativité des organisations professionnelles qui les ont préparés"*.

européenne, qu'elles émanent d'un organe indépendant[430] chargé de veiller au respect de l'application du code et qui pourrait recevoir les réclamations des personnes concernées[431].

SECTION 2 - LE CSA MODEL CODE CANADIEN

Afin d'instaurer un équilibre entre les avantages socio-économiques et le droit de la personne de contrôler les renseignements qui la concernent, certains secteurs ont tenté d'établir et de mettre en oeuvre des codes de conduite sectoriels sur l'information et le respect de la vie privée.

Ainsi, l'Association canadienne du marketing direct s'est dotée d'un code volontaire offrant aux consommateurs la possibilité de refuser la transmission ou la vente de leurs données à d'autres sociétés[432].

De même, le secteur bancaire dispose d'un code volontaire énumérant en dix sections les lignes directrices auxquelles les banques peuvent adhérer en matière de collecte, de conservation, de protection, d'utilisation et de rectification d'informations personnelles relatives à leurs clients. Son contenu et son application restent cependant lacunaires, notamment en ce qui concerne l'accès du client au renseignements personnels et le

---

[430] Par "*indépendant*", la Directive fait référence non pas à une indépendance organisationnelle mais à une indépendance fonctionnelle: mode de désignation des membres, publicité des rapports, accès aisé pour les personnes concernées (publicité de l'existence de cet organe, caractère non coûteux de cet accès, etc.).

[431] OCDE, série PIIC, Paris, OCDE, 1994, cité par Y. Poullet, "OCDE: protection des données et de la vie privée", (1995) D.I.T., p. 83 pour qui la question délicate du contrôle de l'application des codes de conduite nécessite une collaboration entre le secteur et l'autorité de contrôle compétente ainsi, le cas échéant, qu'entre autorités de contrôle.

[432] Le Commissaire à la protection de la vie privée, *Rapport annuel 1990-1991*, Groupe Communication du Canada, 1991, p. 1.

nombre de renseignements requis pour accorder un crédit[433].

Ces codes, n'ayant pas de force obligatoire, se sont inspirés des principes directeurs entourant la collecte, l'usage et la communication des renseignements personnels d'une norme industrielle nationale établie par l'Association canadienne de normalisation (CSA) pour la protection des renseignements personnels par le secteur privé[434] dont une loi destinée à en encadrer les principes est en cours d'élaboration.

S'inspirant des Lignes directrices de l'OCDE[435], cette norme volontaire vise à établir des principes concernant la gestion des renseignements personnels, préciser les exigences minimales que les organismes participants doivent respecter pour protéger les renseignements personnels qu'ils possèdent, sensibiliser la population canadienne à la façon dont devraient être protégés les renseignements personnels et fournir des critères permettant à la communauté internationale d'évaluer la protection accordée aux renseignements personnels au Canada.

---

433 "*The Canadian Bankers Associations Model Privacy Code for Individual Customers*", December 1990; Mentionnons également, à titre d'exemples, le Code de la Canadian Life and Health Insurance Association et de l'Insurance Bureau of Canada et de l'Institut canadien d'information sur la santé; voir Le Commissaire à la vie privée, *Rapport annuel 1995-1996*, *supra* note 321, p. 34; A. Ouimet, *supra* note 43, pp. 199-203

434 Le CSA Model Code [ci-après *Code ou Norme*] a été préparé par le Comité Technique CSA sur la protection de la vie privée, composé de représentants des usagers de l'information (data users), des populations concernées (data subjects), des gouvernements et d'organisations d'intérêt général (associations professionnelles par exemple), sous l'autorité du Comité directeur de normalisation sur les systèmes de gestion, et a été adopté par le Conseil canadien des normes comme norme nationale; Ministère des Communications, *La société canadienne à l'ère de l'informatique: Pour entrer de plain pied dans le XXIe siècle*, *supra* note 327, p. 28.

435 V. Steeves, *supra* note 385, p. 3. "*Le projet de Code de l'Association comprend deux dispositions supplémentaires. La première exige que la personne qui donne des renseignements personnels consente à leur collecte. La deuxième prévoir le droit de porter plainte contre l'organisme collecteur de données qui n'a pas respecté toutes ses lignes directrices, en plus d'exiger que les données soient exactes*".

SOUS-SECTION 1 - CHAMP D'APPLICATION

La Norme s'applique à tout renseignement personnel, au sens d' *"enregistrement de renseignements concernant un individu identifiable, quelle que soit sa forme"*[436]. Il vise donc non seulement les renseignements concernant des résidents canadiens, mais également toute donnée détenue sur le territoire canadien, quelle que soit son origine.

SOUS-SECTION 2 - PRINCIPES FONDAMENTAUX

Le Code définit les exigences minimales de protection des renseignements personnels que chaque secteur peut adapter soit en définissant la façon dont il souscrit aux dix principes mentionnés dans le code, soit en élaborant un code qui lui est propre, soit en modifiant les commentaires en vue de fournir des exemples qui leurs sont propres.

La Norme est basée sur dix principes interdépendants auxquels les organismes qui adoptent la Norme doivent adhérer dans leur totalité[437]. La nécessité d'appliquer ces dix critères de manière cumulative démontre que, pour être efficaces, ces principes doivent se combiner entre eux.

i) Principe de collecte loyale et licite

Le principe 4.4.2 du Code dispose que l'organisme ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder à leur collecte de façon honnête et licite[438]. Ce principe est ainsi conforme à l'article 6 de la Directive européenne qui énonce que *"les données à caractère personnel doivent être*

---

[436] Article 2.1 du Code.

[437] Principe 3.1 du Code.

[438] Principe 4.4.2 du Code.

traitées loyalement et licitement".

Conformément au principe de transparence, les organismes devraient préciser la nature des renseignements recueillis comme faisant partie intégrante de leurs politiques et pratiques concernant le traitement des renseignements.

ii) Spécification des finalités

Les finalités pour lesquelles des renseignements personnels sont recueillies doivent être déterminées par l'organisme préalablement ou au moment de la collecte, et au plus tard avant leur traitement, et précisées afin que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués. La Norme ne précise toutefois pas quand l'explication doit être écrite, la personne concernée étant par exemple invitée à remplir un formulaire spécifique, ou quand un simple exposé oral des finalités suffit.

En vertu du principe 4.3.3 du Code, un organisme ne peut, sous prétexte qu'il fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires à la réalisation des fins légitimes explicitement énoncées. L'exigence de légitimité prévue par la Directive européenne, ne semble pas pouvoir être déduite des termes *"fins légitimes"* qui s'inscrivent dans le cadre particulier de la relation contractuelle de fourniture de biens ou services. Le Code n'en donne aucune définition et ne prévoit aucun contrôle de la légitimité des finalités poursuivies.

iii) Limitation de l'utilisation

En vertu du principe 5 du Code, les renseignements ne doivent pas être utilisés ou communiqués à des autres fins que celles pour lesquelles il ont été recueillis, à moins

que la personne concernée n'y consente ou que la loi l'exige.

iv) Qualité et proportionnalité des données

En vertu du principe 4.4.1 du Code, tant la quantité que la nature des renseignements recueillis doivent être limitées à ce qui est nécessaire à la réalisation des fins déterminées.
En outre, les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins pour lesquelles ils sont utilisés, compte tenu des intérêts de la personne concernée.

Il n'est pas exigé qu'un organisme mette systématiquement à jour les renseignements personnels, à moins que cela ne soit nécessaire pour atteindre les fins pour lesquelles ils ont été recueillis.

v) Garanties de sécurité

La protection des renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées des données personnelles doit être prévue par l'organisme[439].

---

[439] Le Comité consultatif sur l'autoroute de l'information (CCAI) recommande également que "*The department should encourage the use of new technologies such as public key encryption and smart cards to permit greater personal control of information*" (...) "*The government, in partnership with the private sector and privacy advocates, must encourage the development of uniform policies, standards and practices for use by PKIs in Canada*" (IHAC Final Report, *supra* note 327, pp. 50 et 51). "*Under this scheme, enterprises would rely on an independent and trustworthy third party, a certification authority, to verify the electronic identity of persons accessing their system. A "certification network" known as the PKI, would link these Certification Authorities. This technology would harmonize security standards and enhance their reliability*" (D. Johnston, D. Johnston et S. Handa, *supra* note 19, p. 139); (*supra*, Chapitre 2 - La voie législative, Section 3 - La législation fédérale canadienne, *Sous-section 2 - Principes fondamentaux*, v) *Garantie de sécurité*.

Ces mesures de sécurité dont la nature variera en fonction de la sensibilité des renseignements recueillis, de la quantité, de la répartition et du format des renseignements ainsi que des méthodes de conservation, peuvent revêtir plusieurs formes, soit matérielle comme le verrouillage des classeurs et la restriction de l'accès aux bureaux, soit administrative comme les autorisations sécuritaires et l'accès sélectif, soit technique comme l'usage de mots de passe et le recours au chiffrement[440].
Ces mesures de protection[441] se couplent avec l'obligation faite aux organismes de sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels.

vi) Transparence

Un organisme doit mettre à la disposition de toute personne des renseignements précis sur ses politiques, ses pratiques et sa stratégie concernant la gestion des renseignements personnels la concernant. Ce principe est présumé être respecté par les organisations collectrices de données nominatives énonçant clairement leur politique et leurs pratiques en matière de traitement des informations au moyen de brochures offertes auprès de leur établissement, de renseignements adressés à ses clients, d'un accès en ligne ou d'un numéro de téléphone sans frais.

Les renseignements fournis doivent comprendre les nom, fonction et adresse de la personne responsable de la politique et des pratiques de l'organisme et à qui seront acheminées les plaintes et demandes de renseignements, le moyen d'accès aux

---

[440] Dans le cadre du développement de l'autoroute canadienne de l'information, la CCAI considère à cet égard que "*Companies should be free to develop their own security encryption systems on the Information Highway, but consumers will expect equivalent levels of service and protection. There is a balance to be struck* (...)" (IHAC Final Report, *supra* note 327, p. 144; D. Johnston, D. Johnston et S. Handa, *supra* note 19, p. 139).

[441] Dont le CCAI a indiqué que "*The government and the private sector should continue to work together to develop and ensure the widest acceptance of national and international security*

renseignements personnels que possède l'organisme, une description du type de renseignements personnels que possède l'organisme ainsi qu'une explication générale de l'usage auquel ils sont destinés, une copie de toute brochure ou autre document d'information expliquant la politique, les normes ou les codes de l'organisme et la nature des renseignements personnels communiqués aux organismes associés (par exemple, les filiales).

Un organisme doit informer toute personne qui en fait la demande, de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et de leur éventuelle communication à des tiers, et doit lui permettre de les consulter. Il lui sera ainsi possible de contester l'exactitude et l'état complet des renseignements et d'y faire apporter les corrections appropriées.

Les organismes sont également invités à indiquer la source des renseignements en leur possession. Si un organisme est dans l'impossibilité de fournir une liste précise des organismes à qui il a effectivement communiqué des renseignements au sujet d'une personne, il devrait fournir une liste de ceux à qui il pourrait effectivement avoir communiqué les renseignements.

Le délai de réponse de l'organisme collecteur à une demande de communication de renseignements doit être *"raisonnable"* et à un coût minime, sinon inexistant pour la personne concernée qui doit avoir accès aux informations *"sans effort démesuré"*. Afin d'être compréhensible, la communication de ces données doit revêtir une forme accessible au citoyen qui ne possède aucune compétence particulière en ce domaine.

Dans certains cas, l'organisme ne pourra être tenu de communiquer tous les renseignements qu'il possède au sujet d'une personne en raison du coût prohibitif de

---

standards" (IHAC Final Report, *supra* note 327, p. 146).

l'information à fournir, du fait que les renseignements personnels contiennent des détails sur d'autres personnes, sont protégés par le secret professionnel ou relèvent d'une procédure judiciaire, ou encore pour des raisons juridiques, de sécurité ou commerciales exclusives.

vii) Participation individuelle

En vertu du troisième principe du Code, toute personne doit être informée et consentir à la collecte, l'utilisation ou la communication de renseignements qui la concernent, à moins qu'elle ne soit pas apte à le faire. Dans ce cas, le consentement peut également être donné par un représentant autorisé, détenteur d'une procuration. Le principe 4.2.4 du Code prévoit également le consentement de la personne concernée pour toute nouvelle finalité poursuivie avant leur utilisation, sauf si les nouvelles fins auxquelles les renseignements sont destinés soit prévues par une loi. Le consentement de la personne concernée est donc la base de toute collecte et utilisation de renseignements personnels.

Contrairement à l'article 7.b. de la Directive européenne qui permet un traitement *"s'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci"*, le Code ne fait aucune référence à un quelconque contrat qui pourrait fonder le traitement de données sans le consentement de la personne concernée.

Il permet cependant de recueillir, d'utiliser et de communiquer des renseignements personnels à l'insu de la personne concernée et sans son consentement *"pour des raisons d'ordre juridique, médical ou de sécurité, pour l'application de la loi, pour la détection d'une fraude ou de sa répression, ou dans le cas d'une personne gravement malade ou souffrant d'incapacité mentale"*. Si certains de ces exemples correspondent

aux exceptions prévues par l'article 7 c, d, e, et f de la Directive européenne[442], il semble cependant que le champ d'application du Code est plus large quant à la possibilité de collecter, traiter et transférer les données sans le consentement de la personne concernée. Ainsi, la détection d'une fraude ou sa répression ne paraît pas relever d'une mission d'intérêt public dont serait investi le responsable du traitement.

En-dehors de ces exceptions, le consentement de la personne concernée, recueilli avant toute collecte, utilisation ou communication de renseignements personnels, variera selon le degré de *"sensibilité"* des données[443]. Ainsi, le consentement ne pourra n'être qu'implicite lorsque les renseignements sont *"moins sensibles"*[444], le Code ne précisant cependant pas ce qu'il faut entendre par données *"moins sensibles"*.

En pratique, le consentement peut revêtir soit être donné verbalement quand les renseignements sont recueillis par téléphone soit être donné au moment où le produit ou le service est utilisé, soit prendre la forme d'un formulaire de demande de renseignements à signer avec l'insertion d'une case que la personne pourra cocher si elle refuse que ses nom et adresse soit communiqués à d'autres organismes. A défaut, elle sera présumée consentir à ce que les renseignements soient communiqués à des

---

442 Qui prévoit la possibilité de traitement de données à caractère personnel sans le consentement de la personne concernée *"s'il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis"*, *"s'il est nécessaire à l'exécution d'une mission d'intérêt public dont est investi le responsable du traitement"*, *"s'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée"* ou *"s'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée"* (*supra*, Section 2 - La Directive européenne, *Sous-section 3 - Flux transfrontières*, Paragraphe 2 - Notion de "Protection adéquate", Sous-paragraphe 1 - Principes fondamentaux, 1 - Principes de base de la protection, *vii) Participation individuelle*.

443 Si les dossiers médicaux et les renseignements concernant le revenu sont toujours considérés comme *"sensibles"*, d'autres peuvent le devenir selon le contexte.

444 Principe 4.3.6 du Code.

tiers[445].

Le Code précise que le consentement peut être retiré à tout moment, sous réserve de restrictions prévues par une loi ou un contrat et sous réserve d'un délai raisonnable.

Enfin, l'organisme doit apporter les modifications nécessaires lorsqu'une personne démontre que des renseignements personnels sont inexacts ou incomplets.

viii) Responsabilité

Un organisme est responsable des renseignements personnels dont il a la gestion, c'est-à-dire des renseignements en sa possession, sous sa garde ou confiés à une tierce partie à fin de traitement. Dans ce dernier cas, l'organisme doit, par voie contractuelle ou autre, fournir un degré semblable de protection et doit désigner, à cette fin, une ou plusieurs personnes chargées du respect des principes susmentionnés, dont l'identité sera communiquée sur simple demande.

Ce principe de responsabilité, considéré comme fondamental au point d'être le premier principe du Code, ne correspond nullement à ce que les principes de base d'une protection adéquate requièrent au sens de la Directive européenne, à savoir la responsabilité de tout individu effectuant un traitement sur des données à caractère personnel en cas de dommage subi par la personne concernée suite à un traitement illicite ou une action incompatible avec les principes de base de la protection des données. En effet, le Code ne vise que la seule désignation d'un responsable qui devra s'assurer que les principes sont respectés.

---

[445] Cette option ressemble plus à un droit d'opposition qu'à un véritable consentement à la communication des données personnelles à des tiers.

Au contraire de la Directive européenne[446], le Code n'envisage pas le principe de responsabilité au niveau de la réparation d'un éventuel préjudice.

ix) Détention limitée

Le principe 5 du Code prévoit que l'organisme ne doit conserver les renseignements personnels que le temps nécessaire la réalisation des finalités déterminées.

Le Code impose également aux organismes d'élaborer des lignes directrices quant aux durées minimales et maximales de conservation et d'appliquer des procédures spécifiques pour la conservation des renseignements personnels. L'organisme doit conserver les renseignements personnels servant à prendre une décision au sujet d'une personne suffisamment longtemps pour permettre à la personne concernée d'exercer son droit d'accès à l'information après que la décision a été prise. Un organisme peut toutefois être soumis aux exigences prévues par la loi en ce qui concerne les périodes de conservation.

Enfin, l'organisme devrait détruire, effacer et dépersonnaliser les renseignements personnels qui ne sont plus nécessaires à l'égard des fins précisées. Les organismes concernés devraient à cet égard élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels.

---

[446] Voir article 23 de la Directive européenne qui dispose que *"toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi"*.

SOUS-SECTION 3 - REGLES D'EFFECTIVITE

Si le Code retranscrit les principes identifiés[447] dans les Lignes directrices de l'O.C.D.E., il reste à déterminer si les personnes concernées trouveront, par le biais de cette norme, une véritable protection quant au respect de leurs données personnelles. S'agit-il d'un véritable instrument créateur de droits pour la personne concernée, porté à la connaissance et susceptible de recours en cas de non-respect de ces droits?

Paragraphe 1 - Publicité

En vertu du principe de transparence susmentionné[448], le Code impose à l'organisme qui y adhère de mettre à la disposition de la personne concernée tout document ou moyen d'information de sa politique et de sa pratique en matière de gestion des renseignements personnels[449]. L'effectivité de la protection mise en place dans un pays tiers dépend en effet, dans une large mesure, de la possibilité pour les responsables du traitement et les personnes concernées de prendre connaissance de leurs obligations et droits respectifs[450].

---

447 *Supra*, Chapitre 2 - La voie législative - Section 1 - Les Lignes directrices de l'O.C.D.E. et la Convention du Conseil de L'Europe, *Sous-section 3 - Principes fondamentaux*.

448 *Supra*, *Sous-section 2 - Principes fondamentaux*, *vi) Transparence*.

449 Principe 4.8.2 du Code.

450 Le Comité consultatif sur l'autoroute de l'information (CCAI) a à cet égard recommandé:

"*Rec. 10.3. Industry Canada should:*

a. establish a working group that includes representation from the private sector, provincial, territorial and federal governments and consumer organizations for the purpose of increasing public awareness and understanding of privacy issues and personal privacy rights through the preparation and dissemination of educational materials; and

b. encourage the CSA to advance its privacy standard in international standards fora" (IHAC Final Report, *supra*, note 327, p. 142).

En outre, la publicité d'un code de conduite dans un langage compréhensible est de nature à garantir son respect par les responsables du traitement qui, y ayant adhéré, peuvent difficilement l'enfreindre[451].

Paragraphe 2 - Droit de recours

Le principe 10 énoncé du Code reconnaît la possibilité pour le particulier de contester non seulement l'exactitude des données le concernant mais également la conformité de la pratique d'un organisme avec les principes énoncés. Si un droit de recours lui est ainsi reconnu, aucune sanction n'est cependant prévue.

L'effectivité d'un tel recours auprès d'un responsable au sein de l'organisme[452] dépend du fait que cette personne dispose d'une indépendance fonctionnelle et structurelle ainsi que de réelles prérogatives d'investigations au sein de son organisation.

Le Code impose également aux organismes concernés d'informer de l'existence de recours facilement accessibles, les personnes qui introduisent une demande de renseignements concernant les politiques et pratiques de gestion des renseignements personnels suivies ou déposent une plainte[453] et d'y donner suite.

Si, dans le cadre de son examen interne ou externe, la plainte est jugée fondée l'organisme doit prendre les mesures appropriées et, le cas échéant, modifier ses politiques et ses pratiques pour assurer leur conformité aux principes du Code.

---

451 Principe 4.8.2 du Code.

452 Rappelons que le principe 1 du Code exige que l'organisme désigne une ou des personnes qui devra(ont) s'assurer du respect des principes y énoncés.

453 Certaines autorités réglementaires acceptent les plaintes relatives aux pratiques de gestion de l'information des entreprises relevant de leur compétence.

En cas de litige, l'organisme doit communiquer à la personne concernée les coordonnées des autorités de contrôle[454] dont l'indépendance[455] et l'accessibilité[456] assureront l'effectivité des voies de recours. L'effectivité des mesures prises par les autorités de contrôle dépendra de leur réelles possibilités d'action et de la qualité des législations, standards ou autres mécanismes de protection appliqués lors de leur contrôle.

Paragraphe 3 - Contrôle

Le Code prévoit plusieurs méthodes de contrôle du respect des principes énoncés, sous forme d'audits internes, externes ou sous la forme d'un contrôle technique des accès autorisés aux données personnelles (*"Audit Trails"*).

En l'absence de sanctions, l'effectivité des audits internes réalisées par les responsables de la protection et de la sécurité des données personnelles (*"Data Controller"*) au sein de l'entreprise, dépendra des larges pouvoirs d'investigations dont ils devraient disposer dans l'exercice de leur mission.

---

[454] Il s'agit des agences fédérales de réglementation telles que l'OSFI (Office of the Superintendent of Financial Institutions) ou la CRTC (Canadian Radio-Television and Telecommunications Commission), des agences provinciales de réglementation (Office of Superintendent of Insurance), des instances d'autorégulation telles que celles qui existent dans l'industrie du câble, des associations de commerce elles-mêmes (Canadian Direct Marketing Association) et au Québec, de la CAI (Commission d'Accès à l'Information) qui joue le rôle de médiateur et qui, si la médiation a échoué, jouit des prérogatives d'une Cour administrative.

[455] Ceci implique pour l'autorité de contrôle une indépendance dans sa composition, une transparence dans son mode de fonctionnement et des prérogatives suffisamment étendues qu'elle peut déléguer.

[456] Ceci implique que l'existence de l'autorité de contrôle soit rendue publique et que la saisine de cette autorité soit aisée, tant au niveau du prix que des délais et procédures.

L'effectivité des audits externes réalisées par des institutions[457] ou par des auditeurs externes à l'entreprise à partir des rapports établis par celle-ci (*"External Review of the Internal Audit"*) dépendra tant de leur compétence et indépendance[458] que de l'étendue de leur mandat[459], ainsi que du caractère public du résultat de l'audit[460].

Paragraphe 4 - Norme volontaire

Si le Code tend à assurer l'effectivité de sa mise en oeuvre[461], il s'agit seulement d'une norme volontaire tant au niveau de son adhésion qu'au niveau de son application.

Son respect par les entreprises privées sera cependant assurée par plusieurs facteurs. Outre le souci d'éviter toute publicité négative[462], les pressions concurrentielles[463], entre

---

457 Rappelons que dans le secteur public, ce rôle est confié au Commissaire à la protection de la vie privée dont les pouvoirs d'investigation sont fixés à l'article 37 de la Loi fédérale canadienne.

458 Il convient à cet égard d'être attentif aux procédures d'agréation des auditeurs qui ne peuvent être le seul fait des responsables de la protection et de la sécurité des données personnelles au sein des organismes ayant adhéré au Code.

459 Le mandat des auditeurs doit leur permettre de contrôler effectivement le respect des principes de protection des données, telle la qualité des données ou la spécification des finalités, ainsi que le suivi donné aux demandes de renseignement et aux plaintes.

460 C'est en effet le risque de perte d'un *"label"* ou la non-obtention d'un *"certificat"* qui confinera l'organisme à respecter les principes du Code auquel il a adhéré.

461 Voir notamment, le principe 4.1.4 du Code : *"Les organismes doivent appliquer des politiques et des pratiques destinées à donner effet aux principes, y compris : a) appliquer des pratiques servant à protéger les renseignements personnels; b) établir des pratiques pour recevoir les plaintes et les demandes de renseignements et y donner suite; c) former le personnel et l'informer des politiques et pratiques; d) rédiger des documents explicatifs concernant leurs politiques et pratiques"*.

462 Le fait pour une société de marketing direct de ne pas souscrire aux exigences du Code pourrait altérer son image de marque. En revanche, la mention de l'affiliation au Code dans un contrat peut faciliter les échanges avec les clients potentiels, rassurés par cette *"marque de crédibilité"*. En outre, en matière de collaboration entre autorités publiques et entreprises privées, le respect par ces dernières des dispositions du Code constitue une garantie déterminante pour ces autorités.

463 Si la plupart des concurrents sont affiliés au Code, l'entreprise, pour garder une certaine

provinces[464] et même internationales[465] seront de nature à inciter les entreprises à mettre en oeuvre les principes fondamentaux qui y sont énoncés[466].

SOUS-SECTION 4 - MISE EN OEUVRE

Le modèle du CSA Model Code[467] ne doit pas être négligé comme pouvant assurer un niveau de protection adéquat à l'égard des flux transfrontières de données.

En effet, excepté le principe de responsabilité, l'ensemble des principes fondamentaux identifiés dans la Directive européenne, y sont consacrés.

Il importe donc que le Code soit largement diffusé au sein des entreprises privées et auprès des personnes concernées et que celles-ci puissent bénéficier d'un recours en cas de non-respect des principes par les responsables.

---

crédibilité, sera tentée d'y adhérer et par voie de conséquence, sera tenu de respecter les principes qui y sont énoncés.

[464] Par exemple, un organisme d'assurance dont le siège social est sis au Québec et envoyant des données personnelles relatives à des citoyens québécois hors du Québec, sera tenu de *"prendre les mesures nécessaires pour que les informations ne soient pas utilisées à des fins différentes des objectifs initiaux"* (article 17 de la Loi 68).

[465] Par exemple, une compagnie de transport aérien ne pourrait pas, selon le *"UK Data Protection Registrar"*, envoyer des informations qu'elle détient sur ses employés au Royaume-Uni à son siège social sis en Ontario sans qu'une protection des données nominatives soit adéquatement assurée, notamment par l'adoption du Code.

[466] Le CCAI a également recommandé au gouvernement fédéral " *[to] continue to collaborate with the CSA as well as business, consumer organizations and other levels of governement to implement the code and develop effective independent oversight and enforcement mechanisms (Rec. 10.1 and 10.2)*" (IHAC Final Report, *supra* note 327, p. 50); *supra* Chapitre 2 - La voie Législative, Section 2 - La Directive européenne, *Sous-section 4 - Mise en oeuvre*.

[467] Le Code pourrait en effet devenir une norme standard (telle que la norme ISO-9000) de qualité par laquelle les entreprises privées assurent la protection des renseignements personnels. Voir à ce sujet, C. Bennett, "Privacy Codes, Privacy Standards and Privacy Laws: The Instruments for Data Protection and What They Can Achieve", (1995) Int'l L.R 5; P. Trudel, "De l'autoréglementation", (1989) 19 R.D.U.S. 249.

Enfin, les moyens de contrôle du respect de la protection exercé par un responsable au sein même de l'organisme et les recours auprès d'autorités internes et externes envisagés par le Code peut contribuer à assurer une effectivité non négligeable aux principes de base à la condition toutefois que soient assurés leur indépendance et leur réel pouvoir d'action[445].

---

[445] IHAC Final Report, *supra* note 327, p. 140: "*while voluntary standards are useful for engaging business in the protection of personal information, there remains the need for effective, independent oversight and for all parties to have the same rules*".

CONCLUSION

En pénétrant dans le droit positif, la vie privée, longtemps protégée par les moeurs et les usages sociaux, est entrée dans une sphère publique, celle de la protection juridique soumettant au public ce que le sujet entendait garder secret.

Plusieurs causes peuvent être assignées à l'accession des biens de la personnalité à la qualité de biens juridiques, dont celle du développement des techniques de fixation et de reproduction des sons et de l'image et celle de l'existence d'un "*marché d'échange patrimonial*" permettant au sujet de transférer à autrui un droit à l'exploitation patrimoniale des droits de la personnalité[469].

Contrairement à une opinion dominante dans la doctrine de plusieurs pays européens, le droit de la personnalité (Allemagne) et le droit au respect de la vie privée (France) ou à l'intimité et au secret (Italie) ne sauraient ainsi être des droits subjectifs, de nature exclusivement non patrimoniale.

En matière de technologie de l'information, la protection des droits de la personnalité qui a pour objectif la simple dignité de la personne, est confrontée à une large gamme d'instruments juridiques dont aucun n'est pleinement satisfaisant[470].

---

[469] F. Rigaux, "La liberté de la vie privée", *supra*, note 4, p. 546, n° 9.

[470] Voir le rapport intitulé "*La protection de la vie privée dans le secteur privé sous juridiction fédérale*" (cité dans (1996) 9 Justice, p. 17) qui approuve les innovations de la loi 68 mais ne peut indiquer si elles seront de nature à réduire efficacement les problèmes liés à la circulation incontrôlée de l'information entre les secteurs publics et privés et entre les provinces et les pays et qui examine l'élargissement de la loi fédérale canadienne au secteur privé ou l'adoption d'une loi spéciale régissant le secteur privé; sur la déclaration du ministre de l'industrie de mettre en place une loi fédérale obligeant les entreprises privées à respecter la vie privée de leurs employés et clients, voir le Commissaire à la protection de la vie privée, *Rapport Annuel 1995-1996*, *supra* note 321, p. 3.

Les moyens de reproduction évoluent en effet à une vitesse telle que les appréhender par les techniques législatives classiques conduit à figer des solutions qui ne tiennent pas compte de l'évolution technologique[471].

En outre, le multimédia et les autoroutes de l'information ne connaissant pas de frontières, les processus normatifs nationaux ou communautaires tiennent mal ou peu compte de la dimension internationale des enjeux. Une réponse aux risques d'atteinte aux libertés et droits fondamentaux de l'individu doit donc être recherchée en-dehors de ce cadre.

A l'instar de la Directive européenne, on peut encourager une approche auto-réglementaire[472], du type "*codes de conduite*", élaborés à différents niveaux, plus ou moins proches des services proposés.

---

[471] H.P. Glenn, "Le droit en l'an 2000: L'envahissement des contrôles gouvernementaux et des technologies nouvelles dans la vie privée des citoyens", *supra* note 104, p. 708: "*Ce droit fait par les juristes est toujours à la remorque de ce qui est fait par les scientifiques. Etant donné ce phénomène nécessaire de retard, le droit qui est censé contrôler est un droit qui contrôle l'ancienne technologie, une technologie souvent en pleine désuétude*"; P. Martens, *supra* note 53, p. 182.

[472] M.H. Boulanger et C. de Terwagne, *supra* note 186, pp. 4-5: "*Il convient de rappeler à cet égard que l'auto-réglementation est une des caractéristiques intégrantes d'Internet. Certains serveurs indiquent quelles sont les informations qu'ils détiennent au sujet d'un utilisateur. Sur base de l'interrogation de la fonction prévue à cet effet, ils émettent une hypothèse quant à l'identité de l'utilisateur, à la localisation du fournisseur d'accès, au type de machine de l'utilisateur ou au fait d'avoir visité le site récemment ... Les serveurs d'anonymisation offrent aux utilisateurs la possibilité de "se balader" relativement incognito sur le net. Ils fonctionnent globalement de la manière suivante: lors de l'envoi d'un premier message, le serveur d'anonymisation supprime les données permettant d'identifier l'utilisateur, attribue à celui-ci un nouveau "nom" et se charge, par la suite, de lui réexpédier les messages qui lui sont destinés. Il existe sur Internet de nombreux logiciels de cryptage (dont Pretty Good Privacy (...) qui permettent d'assurer dans une large mesure la confidentialité des données transmises et d'attribuer de manière assez sûre un message à un destinataire déterminé*".

Un des avantages des codes de conduite est de permettre l'élaboration de solutions dépassant les frontières nationales et européennes et, dans la mesure où ils sont facilement modifiables, une évolution parallèle aux progrès technologiques.

En outre, ils sont, en principe, élaborés au niveau le plus adéquat, c'est-à-dire celui d'où surgissent les problèmes (serveurs Internet, fournisseurs d'accès agissant de manière individuelle ou collective, etc.), ce qui contribue tant à la "*conscientisation*" des responsables du traitement qu'à l'effectivité de leur mise en oeuvre. Ils permettent ainsi de mettre au point des procédures spécifiques apportant des réponses appropriées aux questions soulevées.

Les codes de conduite présentent néanmoins des inconvénients majeurs. Il n'est en effet pas certain que le niveau de protection qu'ils sont à même de proposer puisse être qualifié d'"*adéquat*"[473] au sens de la Directive européenne pour autoriser les transferts à destination de pays tiers à l'Union européenne. En outre, le caractère effectif de la protection qu'ils apportent peut être sérieusement mis en cause dans la mesure où ils sont fondés essentiellement sur le "*volontariat*" de ceux qui sont amenés à les adopter et à les mettre en oeuvre, contrairement à la loi dotée d'une force juridique contraignante, garante de l'efficacité des principes énoncés.

Enfin, ils ne sont soumis à aucune publicité organisée et n'opèrent pas, de par leur caractère souvent unilatéral et par les choix techniques *a priori* qu'ils posent, une balance des intérêts en présence, contrairement au processus législatif auquel concourent toutes les personnes intéressées. Ils ne prennent souvent en considération les intérêts des utilisateurs des autoroutes de l'information que dans une certaine mesure,

---

[473] Dès lors que ce niveau de protection ne répondrait pas aux conditions examinées de représentativité, de publicité et de modes de contrôle et sanction.

sans leur reconnaître des droits ayant une portée effective[474].

Les autorités de contrôle, en invitant tous les intéressés à s'exprimer, sont parfois présentées comme pouvant à cet égard jouer un rôle important dans l'élaboration des codes[475]. La Directive européenne va dans ce sens, lorsqu'elle prévoit, en ses articles 27 et 30, l'intervention optionnelle du Groupe européen de protection des personnes à l'égard du traitement des données à caractère personnel, composé de représentants des commissions nationales, dans le processus d'élaboration des codes communautaires.

L'on peut toutefois s'interroger sur les limites de leur fonction régulatrice[476], voire légitimatrice[477], dans le cadre du contrôle de leur application.

Plutôt que la création d'une agence de contrôle, la maîtrise par l'individu de son "*image informationnelle*" devrait davantage s'appuyer sur le droit d'*habeas data* qui repose sur le consentement individuel comme justification de la libre circulation des données personnelles et dont le non-respect peut être judiciairement sanctionné[478].

---

[474] M.H. Boulanger et C. de Terwangne, *supra*, note 186, pp. 5 et 6; P. Thomas et M.H. Boulanger, *supra* note 2, pp. 230-231.

[475] P. Thomas et M.H. Boulanger, *supra* note 2, p. 231.

[476] "*Par le caractère général de la protection accordée, les droits de la personnalité deviendraient en quelque sorte les droits du citoyen, ou plutôt d'un citoyen présumé qui exercerait, lui, peu ou pas de contrôle sur ses propres données nominatives* " (H.P. Glenn, "Les droits de la personnalité, le respect de la vie privée et le droit à l'image", *supra* note 354, p. 564).

[477] "*(...) si la protection qu'elles peuvent accorder à la vie privée des citoyens est donc très relative, elles sont tout de même censées agir pour la protection de la vie privée, de sorte que leur approbation à la transmission des données nominatives constitue une caution qui autrefois manquait et pose la question fondamentale de savoir si le rôle des commissions est plutôt celui d'une agence de légitimation plutôt que celui d'une agence de protection*" (H.P. Glenn, "Le droit en l'an 2000: L'envahissement des contrôles gouvernementaux et des technologies nouvelles dans la vie privée des citoyens", *supra* note 104, p. 709).

[478] Sur les limites des remèdes du droit civil, voir H.P. Glenn, "Le droit au respect de la vie privée", *supra*, note 39, p. 903.

De même, la Directive européenne consacre une part importante de ses dispositions au consentement de l'individu. Les Etats membres peuvent prévoir qu'il constitue un facteur de légitimité du traitement et permettre sur cette base le transfert de données personnelles vers un pays tiers n'offrant pas un niveau de "*protection adéquat*"[479]. Si le consentement doit être, au terme de l'article 26.1, "*indubitable*" - risquant par là-même de restreindre le pouvoir des autorités de contrôle à un contrôle marginal car portant essentiellement sur les conditions de forme liées au consentement[480] -, une information préalable des personnes fichées (principe de transparence) et une définition claire des finalités du traitement (principe de finalité) est essentielle. Le cas échéant, elles donneront à l'intéressé la possibilité de se soustraire au traitement en ne communiquant pas ses données.

C'est en effet à la seule condition de connaissance que peut s'exercer la maîtrise de l'individu du sort réservé aux informations qui le concernent, laquelle s'exercera par le refus donné, refusé ou négocié à la divulgation, à l'utilisation ou à la communication des informations. Elle s'exprime encore par le contrôle de la qualité des données et le pouvoir corrélatif d'imposer des corrections via le droit d'accès et de rectification, ou par les recours que le sujet se voit reconnaître en cas d'utilisation illégitime des données le concernant, notamment dans les situations qui échappent au départ à son consentement (ainsi, lorsque le traitement se justifie par une loi ou par l'intérêt prédominant d'un tiers qui utilise abusivement les données).

---

[479] Le transfert peut également être réalisé en cas de nécessité contractuelle, pour la sauvegarde d'un intérêt public important ou lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes; ces garanties peuvent notamment résulter de clauses contractuelles appropriées.

[480] "*Ne risque-t-on pas, dès lors, d'assister au développement de services dans lesquels la première démarche du prestataire consistera à demander à l'individu de consentir à l'utilisation de ses données pour les finalités décrites sans véritable recherche d'un équilibre des intérêts en présence?*" (P. Thomas et M.H. Boulanger, *supra* note 186, p. 229).

Si une approche du type "*normes de conduite sectorielles*", couplée à celle de la technologie présente un attrait certain, il reste que la protection des données dans un contexte international nécessite une démarche spécifique - tenant à la combinaison de la voie auto-réglementaire et législative - tendant à dégager des solutions praticables et efficaces garantissant la protection des personnes concernées, sans pour autant constituer des barrières tarifaires à la libre circulation de l'information[481].

Une approche concertée[482] semble en effet requise tant au niveau des propositions législatives appropriées qui pourraient s'avérer nécessaires pour corriger les effets éventuellement jugés néfastes de l'application des règles existantes au multimédia et aux autoroutes de l'information, qu'en ce qui concerne l'effectivité des codes de conduite qui pourra être assurée grâce aux connexions, parfois imprévisibles, qu'ils peuvent avoir avec des mécanismes de contrôle et de sanction plus classiques[483].

Cette démarche spécifique sera d'autant plus délicate à définir et l'équilibre entre les droits et libertés des individus et la circulation de l'information sera d'autant plus difficile à trouver et à adopter au niveau international, qu'ils se situent au confluent de cultures et traditions juridiques diverses qui peuvent toutefois prendre utilement le relais l'un de l'autre.

---

[481] Voir à ce sujet, K. Benyekhelf, *La protection de la vie privée dans les échanges internationaux d'informations*, *supra* note 39, p. 207 et s.: "Protection des données: Protection des droits de la personne ou protectionnisme économique?".

[482] D. Johnston, D. Johnston et S. Handa, *supra* note 19, pp. 206 - 207: "*IHAC proposed four [possible concrete solutions to the problem of privacy] : legislation, education, voluntary codes of conduct and Technological solutions. Adoption of any of these solutions must be tempered or guided by considerations of openness, disclosure (access), secondary usage, correction, reliability and security*".

[483] P. Martens, *supra* note 53, p. 207: "*ce que, semble-t-il, on n'avait pas prévu, c'est que, par le biais des usages honnêtes en matière commerciale, les concurrents plus encore que les victimes seront attentifs à faire la police des fichiers*".

Tel est le sens des Lignes directrices de l'O.C.D.E. ou de la Convention du Conseil de l'Europe même si l'on a critiqué la méthode qui consiste à vouloir harmoniser les législations existantes par le biais de normes internationales, alors qu'il faudrait repenser la protection des données personnelles au regard des nouvelles contraintes technologiques, en tenant compte de ce qu'un système de flux mondial ne peut se contrôler comme un fichier statique ou localisé[484].

Si le droit veut exercer un certain contrôle sur la circulation des données[485], il doit le faire, non en opposant négativement ses valeurs à une matière qui est physiquement rétive mais en adaptant sa discipline à leur nouveauté. Non seulement c'est une matière dans laquelle l'obsolescence galopante interdit la rigidité des définitions, mais on peut se demander si le monde virtuel est accessible au monde juridique. Le juriste est donc condamné à composer avec le technologue.

Souhaitons que cette réflexion, sous-tendue par la volonté des nouveaux intervenants de se départir du carcan normatif pour imposer leurs propres standards, s'initie au rythme du développement qu'impriment les techniciens des autoroutes de l'information, la protection des données à caractère personnel devant faire partie intégrante des services proposés dont le public, dans un milieu concurrentiel, risque de se détourner s'ils ne garantissent pas respect et protection.

---

[484] M. Briat et C.M. Petrat, "Protection des données. Autoroutes électroniques et flux d'informations", (1994) 3 D.I.T., pp. 6-9.

[485] Voir sur le *"droit retenu"* ou le *"droit engagé"* face aux nouveaux moyens de reproduction, H.P. Glenn, "Les nouveaux moyens de reproduction audio-visuelle et numérique et les droits de la personnalité: Rapport général", *supra* note 5, p. 698 et s; Comp. : H. Oberdoff, "Le droit, la démocratie et la maîtrise sociale des technologies", (1992) 4 Rev. du Droit Public, p. 983 et s.

Ainsi, la "*vigilance mercantile*" pourrait "*donner consistance à la norme éthique*"[486].

[486] P. Martens, *supra* note 53, p. 207.

BIBLIOGRAPHIE

LEGISLATION

OCDE

OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, Paris: OCDE, 1981.

CONSEIL DE L'EUROPE

Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, (Jan. 2, 1981), Eur. Treaty Series No.108.

Council of Europe, Parliamentary Assembly Recommandation (1968), Eur. Treaty Series No.509.

COMMUNAUTES EUROPEENNES

CE, *Resolution (EEC) of the European Parliament on the Protection of the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing*, J.O. Communications (1975) n°C60, p. 48.

CE, *Resolution (EEC) of the European Parliament on the Protection of the Rights of the Individual on the Face of Technical Developments in Data Processing*, J.O. Communications (1982) n° C87, p. 39.

CE, *Resolution (EEC) of te European Parliament on the Protection of the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing*, J.O. Communications (1976) n°C100, p. 27.

CE, *Resolution (ECC) of the European Parliament on the Protection of the Rights of the Individual in Connection in the Face of Technical Developments in Data Processing*, J.O. Communications (1979) n° C140, p. 34.

CE, *Proposition (CEE) de la Commission pour une Directive du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*, J.O. Communications (1990) n°C277, p. 3.

CE, *Proposition (CEE) de Directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Exposé des motifs)*, COM (90) 314 final - SYN 287 (Bruxelles, septembre 1990).

CE, *Proposition (CEE) modifiée de Directive du Conseil 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 (Exposé des motifs)*, COM (92) 422 final - SYN 287 (Bruxelles, 30 juillet 1992), p. 35.

CE, *Proposition (CEE) modifiée de Directive du Conseil relative à la protection des personnes à l'égard des traitements des données à caractère personnel et à la libre circulation de ces données du 15 octobre 1992*, COM (92) 422 final - SYN 287, p. 13.

CE, *Proposition (CEE) de Directive du Parlement européen et du Conseil du 24 octobre 1996 concernant "la protection des données à caractère personnel et de la vie privée dans le secteur des télécommunications, en particulier des réseaux numériques à intégration de services R.N.I.S. et des réseaux mobiles numériques*, J.O. Communication (1996) n° C315, p. 1.

CE, *Directive (CEE) No 95/46 du Parlement européen et du Conseil du 24 octobre 1995*, J.O. Législation (1995) n° L281, p. 31.

CE, *Recommendation (EEC) No 81/679 of the Commission Relating to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, J.O. Législation (1981) n° L246, p. 31

CE, *Recommandation (CEE) No. R (97) 5 relative à la protection des données médicales*, adoptée par le Comité des ministres le 13 février 1997.

CE, *Position commune (CEE) No 1/95 arrêtée par le Conseil le 20 février 1995*, J.O.Communications (1995) n° C93, p. 19 ("Exposé des motifs").

CANADA

Charte canadienne des droits et libertés, Partie I de la *Loi constitutionnelle de 1982 sur le Canada* (R.-U.), 1982.

Charte québécoise des droits et libertés de la personne, L.R.Q., c. C-12.

Loi sur l'accès à l'information, L.R.C. 1985, c. A-1.

Loi sur la protection des renseignements personnels, L.R.C. 1985, c. P-21.

Loi sur la protection des renseignements personnels dans le secteur privé (Loi 68), L.Q. 1993, c. 17.

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (loi sur l'accès), L.R.Q., c. A-2.1 (Québec).

Freedom of Information Act, S.N., 1981, c. 5 (Terre-Neuve).

Freedom of Information Act, S.N.S., 1990, c. 11 (Nouvelle-Ecosse).

Loi sur le droit à l'information, S.R.N.B., 1973, c. R-10.3, telle qu'amendée (Nouveau-Brunswick).

Freedom of Information and Protection of Privacy Act, 1987, S.O., 1987, c. 25, telle qu'amendée et *Loi de 1989 sur l'accès à l'information municipale et la protection de la vie privée*, S.O., 1989, c. 63 (Ontario).

Loi sur la liberté d'accès à l'information, L.M., 1985-1986, c. 6 Chap. F175, telle qu'amendée (Manitoba).

Access to Information Act, R.S.Y., 1986, c. 1 (Yukon).

Privacy Act, R.S.B.C., 1979, c. 336 (Colombie Britannique).

Privacy Act, S.M, 1970, c. 74 (Manitoba).

Privacy Act, R.S.S., 1979, c. P -24, (Saskatchewan).

An Act Respecting the Protection of Personal Privacy, S.N., 1981, c. 6 (Terre-Neuve).

RAPPORTS GOUVERNEMENTAUX/DOCUMENTS

CANADA

Ministère de la Justice, *Les lignes directrices régissant la protection de la vie privée et les flux transfrontières de caractère personnel de l'O.C.D.E.: incidences pour le Canada*, Ottawa, Ministère des Approvisionnements et Services, 1985.

Ministère de la Justice, *La vie privée: zone à accès restreint*, Synthèse du rapport du Comité interministériel sur la protection de la vie privée eu égard aux banques de données à caractère personnel, Québec, avril 1989.

Ministère des Communications, *La société canadienne à l'ère de l'information: Pour entrer de plain-pied dans le XXIe siècle*, Ottawa, Ministère des Approvisionnements et Services, 1996.

Groupe de recherche informatique et droit (BUREAU, R.D., LAPERRIERE, R., LEMASSON, J.P., MARTIN, J. et PELADEAU, J.P.), *L'identité piratée*, Montréal, SOQUIJ (société québécoise d'information juridique), 1986.

Information Highway Advisory Council, *Privacy and the Canadian Information Highway*, (Ottawa: Industry Canada), 1994.

Information Highway Adivsory Council, Final Report *Connection, Community, Content, Challenge* (Ottawa: Supply and Services Canada, september 1995) (Chair D. Johnston), 1995.

Rapport du Groupe d'étude, *L'ordinateur et la vie privée*, Ottawa, Ministères des Communications et de la Justice, Ottawa, 1972.

Rapport du Groupe de travail sur la commercialisation des banques de données des organismes publics, Ministère des Communication du Québec, Québec, 1991.

Rapport "*La protection de la vie privée dans le secteur privé sous juridiction fédérale*", cité dans (1996) 9 Justice, p. 17.

Commission de la culture, *La vie privée, un droit sacré*, Québec, Assemblée nationale, juin 1988.

Commission d'accès à l'information, *Une vie privée mieux respectée, un citoyen mieux informé*, Rapport sur la mise en oeuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, Les Publications du Québec, 1987.

Le Commissaire à la protection de la vie privée, *Rapport annuel 1995-1996*, Groupe Communication du Canada, 1996.

Le Commissaire à la protection de la vie privée, *Rapport annuel 1990-1991*, Groupe Communication du Canada, 1991.

Le Commissaire à la protection de la vie privée, *Rapport annuel 1987-1988*, Groupe Communication du Canada, 1988.

Commission d'accès à l'information du Québec, *Rapport annuel 1994-1995*, Les publications du Québec, 1995.

Commission d'accès à l'information du Québec, *Rapport annuel 1991-1992*, Les publications du Québec, 1992.

Commission d'accès à l'information du Québec, "Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la santé et des services sociaux", (1992) 8 L'accès 22.

Commission d'accès à l'information du Québec, "La protection des renseignements personnels dans le secteur privé: un mouvement international", (1992) 8 L'accès 1.

Commission d'accès à l'information du Québec, "Rapport annuel 1991-1992", (1992) L'accès 1, p. 3.

Commission d'accès à l'information du Québec, "Informatisation des dossiers contenant des renseignements confidentiels: la CAI adopte des mesures de sécurité" (1992) 7 L'accès 1.

Commission d'accès à l'information du Québec, "Pour quand la protection des renseignements personnels dans le secteur privé ?", (1991) 7 L'accès 1.

The Canadian Bankers Association, "Model Privacy Code for Individual Customers", December 1990.

COMMUNAUTES EUROPEENNES

CE, Commission, *DG XV News*, mars 1995, n° 1, p. 19.

OCDE

OECD, *Policy Issues in Data Protection and Privacy*, dans 10 OECD Informatics Studies (1974).

OECD, *Guidelines Governing the Protection of Privacy and Transborder Data Flow of Personal Data*, dans 80 OECD Document C58 final (1980).

OECD, *Present Situation and Trends in Privacy Protection in the Area*, DSTI/ICCP/88.5 (1er juin 1988).

OCDE, Série PIIC, Paris, OCDE, 1994 cité par POULLET, Y.,"O.C.D.E.: Protection des données et de la vie privée", (1995) 2 D.I.T., 83.

CONSEIL DE L'EUROPE

Conseil de l'Europe, *Rapport explicatif concernant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (Strasbourg, 1981).

Conseil de l'Europe, "*Contrat type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de données et rapport explicatif*", (Strasbourg, 1992) T-PD (92) 7, révisé le 2 novembre 1992.

COMMUNAUTES EUROPEENNES

CE, *Explanatory Memorandum of the Commission of the European Communities*, COM (92) 422 final - SYN, p. 15.

FRANCE

CNIL, Délibération n° 89-79 du 11 juillet 1989 relative à la transmission d'informations relatives aux cadres supérieurs de la société Fiat-France à la société Fiat à Turin (Déclaration ordinaire n° 893-947)

ALLEMAGNE

Palandt BGB, Beck'sche Kurz Kommentar, Bd 7, 44 neubearbeitite Aufl., C.H. Beck'sche Verlagsbuchhande., München, 1985, § 823, Anm. 15.

JURISPRUDENCE

ETATS-UNIS

De May v. Roberts, *46* Mich. 160, 9. N.W. 146 (1881).

Brents v. Morgan, 221 ky. 765, 299 S.W. 967 (1927).

Rhodes v. Graham 238 Ky. 225, 37 S.W. 46 (1931).

Melvin v. Reid, 112 Cal App. 285, 297 P. 91 (1931).

Fitzsimmons v. Olinger Mortuary Ass'n, 91 Colo. 544, 17 P. 2d 535 (1932).

Sidis v. F.R. Publishing Corporation, 113 F. 2d 806 (2d circ.) (1940).

Barber v. Lime, Inc., 348 Mo. 1199, 159 S.W. 2d 291 (1942).

Hinish v. Meir and Frank Co., 166 Ore. 482, 113 P. 2d 438 (1942).

Gill v. Curtis Pub. Co., 38 Cal. 2d 273, 239 P. 2d 630 (1952).

Griswold v. Connecticut, 381 U.S. 484 (1965).

Berger v. New York, 338 U.S. 41 (1967).

Katz v. United States, 389 U.S. 347 (1967).

Eisenstadt v. Baird, 405 U.S. 438 (1972).

Roe v. Wade, 410 U.S. 113 (1973).

Whalen v. Roe, 429 U.S. 589 (1977).

Bowers v. Hardwik, 478 U.S. 186 (1980).

Boyd. v. United States, 116 U.S. 616 (1986).

ANGLETERRE

Gee v. Pritchard, (1818) 2 Swartson 403, 36 E.R. 670 (Chanc.).

Abernethy v. Hutchinson, (1825) 1 H and Tw. 28, 47 E.R. 1313 (Chanc.).

Prince Albert v. Strange, (1849) 2 De G. and Sm. 712, 64 ER 304 (Chanc.).

CANADA

Victoria Park Racing and Recreation Co. Ltd v. Taylor, [1937] 58 C.L.R. 479, 496.

R.c. Kirby, [1970] 1 C.C.C. (2e) 286 (C.A. Qué.).

Insurance Corporation of British columbia C. Heerspink, [1982] 2 R.C.S. 145.

Hunter c. Southam, [1982] 2 R.C.S. 145.

Commission ontarienne des droits de la personne c. Simpson - Sears Inc., [1985] 2 R.C.S. 536.

Winnipeg School Division n° 1 c. Craton, [1985] 2 R.C.S. 150.

Boucher c. Office du crédit agricole du Québec, [1986] C.A.I. 372.

Action travail des femmes c. Compagnie du Chemin de fer nationaux du Canada, [1987] 1 R.C.S. 1114.

R.c. Zundel, [1987] 31 C.C.C. (3e) 97 (C.A. Ont.).

La Reine c. Dyment, [1988] 2 R.C.S. 417.

Stewart c. La Reine, [1988] 1 R.C.S. 963.

Morgentaler c. La Reine, [1988] 1 R.C.S. 30.

ALLEMAGNE

BverfG, 18 décembre 1953, BverfGE 3, 225, 241-242.

BverfG, 16 juin 1959, BverfGE 9, 338, 343.

BverfG, 29 juillet 1959, BverfGE 10, 59, 67-69.

BverfG, 22 juin 1960, BverfGE 11, 234, 238.

BverfG; 24 février 1971, *Mephisto*, BterfGE 3O, 173, 192.

BVerfG, 3 juin 1980, *Heimrich Böll*, BVerfGE 54, 148, 154.

Bverf, 15 décembre 1983, Volkszählengsgesetz, BverfGE, 65, 1, 41.

BverfG, 9 mars 1988, BverfGE 78, 77.

ITALIE

C. cost., 12 avril 1973, n. 38, Giurispr. cost., 1973, I, 354, 362.

Cass. Scz. I civ., 27 mai 1975, n. 2629, Principessa Soraya Esfarandi, Giust. Civile, 1975, I, 1686, 1696.

EUROPE

Affaire *Klass et autres* (1978), Cour Eur.D.H., Sér. A, No 28, p. 17.

Affaire *Malone* (1984), Cour Eur.D.H., Sér. A, No 82, p. 6.

Affaire *Lingens* (1986), Cour Eur. D.H., 8 juillet 1986, , Sér. A, No. 103, p. 11.

Affaire *Barford* (1989), Cour Eur.D.H., Sér. A, No 149, p. 12.

Affaire *Kruslin et Huvig* (1990), Cour Eur. D.H.,Sér. A., No 1.

DOCTRINE

MONOGRAPHIES

BENYEKHLEF, K., *La protection de la vie privée dans les échanges internationaux d'informations*, Thémis, Université de Montréal, 1992.

BUCHER, A., *Personnes physiques et protection de la personnalité*, éd. Helbing et Lichtenhahm, Bâle et Frankfurt a/M, 1985.

CARBONNIER, J., *Droit civil, I. Introduction. Les personnes*, 16e éd., P.U.F., Coll. Thémis, 1987.

DABIN, J., *Le droit subjectif*, Paris, Dalloz, 1952, p. 103.

DE CUPIS, A., *I diritti della personnalità*, 1a ed., t. I, 1959, Milano, Giùffre, dans Trattato di diritto civile e commerciale diritto dei prof A. Cicu et F. Messineo, vol IV, 2a ed. riv. e aggiornata, 1982.

DE HOUWER, J., *Privacy and Transborder Data Flows (A comparative study of International and National Regulations)*, Document inédit, Vrije Universiteit Brussel, octobre 1989.

DE VITA, A., Persone fisische. Commentario del codice civile, Scialoja - Branca, Libro primo, Persone e familia, art. 1-10, Zanchelli éd. Bologna, Il foro italiano, Roma, 1988.

FLAHERTY, D.H., *Protecting Privacy in Surveillance Societies: the Federal Republic of Germany, Sweden, France, Canada and the United States*, Chapel Hill, The University of North Carolina Press, 1989.

FLAHERTY, D.H., *Protecting Privacy in Two-way Electronic Services*, White Plains New York, Knowledge Industry Publications, 1984.

FREEDMAN, W., *The right of Privacy in the Computer Age*, New York, Quorum Books, 1977.

GHESTIN, J., GOUBEAUX, G., *Traité de droit civil, Introduction générale, I*, 2e éd., Paris, L.G.D.J., 1983.

HUBMANN, H., *Das Persönlihkeitsrecht*, 2te veränd. und erweiterte Auflage, Böthan Verlag, Köln, Graz, 1967.

JOHNSTON, D., JOHNSTON, D. et HANDA, S., *Getting Canada Online-Understanding the information Highway*, Toronto, Stoddart, 1995.

KAYSER, P., *La protection de la vie privée. Protection du secret de la vie privée*, 1ère éd., Paris, Economica, Presses Universitaires d'Aix-en-Provence, 1984 et 2e éd, Paris, Economica, Presses Universitaires d'Aix-en-Provence, 1990

LAPERRIERE, R., COTE, R., LE BEL, G.A., ROY, P. et BENYEKHLEF, K., "*Vie privée sans frontières: les flux transfrontières de renseignements personnels en provenance du Canada*", Ottawa, Ministère fédéral de la Justice, 1991.

LAPERRIERE, R., *La protection des renseignements personnels dans le secteur privé*. Résumé du mémoire soumis à la Commission de la culture de l'Assemblée nationale du Québec, GRID, 10 février 1988 et version révisée (4 mars 1993).

LEMASSON, J.P., MARTIN, J., PELADEAU, P. et LAPERRIERE, R., *Les renseignements personnels et l'ordinateur enquête sur la situation des bases de données à caractère personnel dans le secteur privé québécois*, Montréal, SOQUIJ, 1986.

LUCAS, A., *Le droit de l'informatique*, Paris, P.U.F, 1987.

MACKAY, P., PELADEAU, P. et LAPERRIERE, R., *Droit, informatique et vie privée: bibliographie sélective, canadienne et internationale*, Montréal, SOQUIJ, 1986.

MAISL, H., et VITALIS, A., *Les libertés, enjeu d'une société informatisée* (Etudes, avril 1985), 472.

MILLER, A., *The Assault on Privacy*, Michigan, The University of Michigan Press, 1971.

NERSON, R., *Les droits extrapatrimoniaux*, Lyon, Bosc Frère M. et L. Riou, 1939.

NEUNER, C., *Wesen und Arten der Privatrechsverhältnisse*, Kiel, Schwers'sche Buchhandlung, 1866.

NUTGER A.C.M., *Transborder Flow of Personal Data Within the E.C.*, Kluwer, Computer Law Series.

PELADEAU, P. et LAPERRIERE, R., *Le droit sur la protection des renseignements personnels - étude sur les bases privées de données à caractère personnel en droit canadien, comparé et international*, Montréal, SOQUIJ, 1986.

PEMBER, D.R., *Privacy and the Press, The Mass Media and the First Amendment*, 1972.

RAVANAS, J., *La protection des personnes contre la réalisation et la publication de leur image*, Paris, L.G.D.J., 1978.

RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant, 1990.

ROBERTSON, A.H., *European Institution Cooperation, Integration, Unification*, 3e éd., London, Stevens/Matthew/Bender, 1973.

ROUBIER, P., *Droits subjectifs et situations juridiques*, Paris, Dalloz, 1963.

ROUX, A., *La protection de la vie privée dans les rapports entre l'Etat et les particuliers*, Paris, Economica, 1983.

TERCIER, P., *Le nouveau droit de la personnalité*, Schlulthess, Zurich, 1984, p. 131.

TRIBE, L.H., *American Constitutional Law*, 2e éd., Mimeola, New York, Foundation Press, 1988.

VITALIS, A., *Informatique, pouvoirs et libertés*, Paris, Economica, 1988.

WESTIN, A.F., *Privacy and Freedom*, New York, Atheneum, 1967.

PERIODIQUES

ACQUARONE, D., "L'ambiguité du droit à l'image", D., 1985, Chr., 129-136.

BARREAU DU QUEBEC, "La protection de la vie privée eu égard aux renseignements personnels détenus dans le secteur privé", Août 1991.

BENNETT, C., "Privacy Codes, Privacy Standards and Privacy Laws: The Instruments for Data Protection and What They Can Achieve", (1995) Int'l L.R 5.

BENYEKHLEF, K., "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", (1991-1992) 2 Média and Communications L.R. 157.

BIGELOW, R., "Privacy", (1993) 2 Comp. Law Ser. Rep 50.

BLUME, P., "An EEC Policy for Data Protection", (1992) 11 Computer L. J. 399.

BOEHMER, R. C., PALMER, T. S., "The 1992 EC Data Protection Proposal: An Examination of its Implications for V.S. Business and U.S. Privacy Law" (1993) 31 Am. Bus. L. J. 265.

BOUCHARD, M.P., "Loi sur l'accès québécoise: principes, structures et recours, à la lumière des législations d'autres juridictions provinciales", dans *Développements récents en droit de l'accès à l'information (1991), Coswanville*, éd. Yvon Blais, 1991, p. 8.

BOULANGER, M.H. et DE TERWANGNE, C., "Commentaires de la proposition de Directive", dans Lamy, *Droit de l'Informatique*, 1992.

BOULANGER, M.H., DE TERWANGNE, C., LEONARD, Th., LOUVEAUX, S., MOREAU, D. et POULLET, Y., "La protection des données à caractère personnel en droit communautaire", (1997) J. des Trib. de Droit Eur. 121.

BRIAT M. et PETRAT, C.M., "Protection des données. Autoroutes électroniques et flux d'informations", (1994) 3 D.I.T. 6.

BRIAT M., "Personal Data and the Free Flow of Information", dans G.P.V. Vanderberghe éd., *Freedom of Data Flows and EEC Law*, (Proceeding of 2nd CELIM Conference), Deventer, Kluwer Law & Taxation Publishers, 1988.

BURNS, P., "The Law and Privacy: the Canadian Experience", (1976) 54 R. du B. can. 1.

COLE, P.E.,"New Challenges to the U.S. Multinational Corporation in the European Economic Community: Data Protection Laws", (1985) 17 N.Y.V.J. Int'l L. & Pol. 893.

COMEAU, P.A., et OUIMET, A., "Freedom of Information and Privacy: Québec's Innovative Role in North America", (1995) 80 Iowa L.R. 3.

COOMBE, G.W. et KIRK, S.L., "Privacy, Data Protection and Transborder Data Flow: A Corporate Response to International Expectations", (1983-84) 39 Business Lawyer 33.

DANDURAND, L., "L'accès à l'information dans un débat démocratique" (1996) 16 Paroles de droit (Bulletin de la Fondation canadienne des droits de la personne) 5.

DE TERWANGNE, C. et DE LA CROIX-DAVIO, Th., "L'accès à l'information administrative et la commercialisation des données publiques", Namur, C.R.I.D., 1994, 105-118.

DOCKRILL, C., "Computer Data Banks and Personal Information: Protection Against Negligent Disclosure", (1988) 11 Dalhousie L. J. 546.

DONALDSON, R.A., "Annotation, False Light Invasion of Privacy-Cognizability and Elements", (1991) 57 A.L.R. 422.

DORE, L., "Panorama de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels" dans *Développements récents en droit de l'accès à l'information (1991)*, Coswanville, éd. Yvon Blais, 1991, pp. 29-68.

DUSSAULT, Y.D., "Le point sur deux sujets complexes inhérents à la Loi sur l'accès: les renseignements fournis par un tiers et la notion de renseignements nominatifs" dans *Développements récents en droit de l'accès à l'information (1991)*, Coswanville, éd. Yvon Blais, 1991, pp. 107-122.

DWORKIN, G., "The Common Law Protection of Privacy", (1967) Univ. of Tasmania L.R. 422.

EBONE, J. W., "Personhood and the Contraceptive Right" (1982) 57 Indiana L.J. 579.

ELGER, R., "Dater export" dans (1993) Drissraten, 1 CR 2.

EPPERSON, G.M., "Contacts for Transnational Information Services: Securing Equivalency of Data Protection" (1981) 22 Har. Int'l. L. J. 157.

EVANS, A.C., "European Data Protection Law" (1981) 29 Am. J. Comp. L. 571.

FOCSANEANU, L., "La protection des données à caractère personnel contre l'utilisation abusive de l'informatique", (1982) 109 J. Droit Int'l 55.

GASMANN, H.P., "The Activities of the OECD in the Field of Transnational Data Regulation in Online, Data Regulation and Third World Realities", (1978) Int'l L.R. 177.

GASMANN, H.P., "Vers un cadre juridique international pour l'informatique et autres nouvelles techniques de l'information", (1985) Annuaire français de droit international 747.

GERETY, T., "Redefining Privacy", (1977) 12 Harvard Civil Rights-Civil Liberties L.R. 233.

GLENN, H.P., "Le droit au respect de la vie privée", (1979) 39 R. du B. 879.

GLENN H.P., "Les nouveaux moyens de reproduction audio-visuelle et numérique et les droits de la personnalité: Rapport général", (1986) 46 R. du B. 693.

GLENN H.P., "Le droit en l'an 2000: L'envahissement des contrôles gouvernementaux et des technologies nouvelles dans la vie privée des citoyens, (1987) R.G.D. 705.

GLENN H.P., "Les droits de la personnalité, le respect de la vie privée et le droit à l'image" dans G.A. Beaudoin, dir., *Vues canadiennes et européennes des droits et libertés*, Actes des journées strasbourgeoises de l'Institut canadien d'études juridiques supérieures, 1988.

GORMLEY, K., "One Hundred Years of Privacy", (1992) Wis. L. R. 1335.

GRAHAM, J. P., "Privacy, Computers and Commercial Dissemination of Personal Information", (1987) Texas L.R. 1395.

GROSS, H.,"Privacy and Autonomy", dans *Nomos XIII, Privacy*, éd. J. Chapman et J. R. Pennock, New York: Lieber-Atherton, 1971, pp. 169-182.

GROSSEN, J.M., "La protection de la personnalité en droit privé (quelques problèmes actuels)", (1960) 79 Revue de droit suisse, 2 p. 9a.

H.M., "Marketing direct et données personnelles, définition d'une déontologie", (1995) D.I.T. 72.

HONDIUS, F. W., "Data Law in Europe", (1980) 16 Stanford J. of Int'l. L. 87.

KIRBY, M.D., "Transborder Data Flows and the "Basic Rules" of Data Privacy" (1980) 16 Stanford J. Int'L L. 27.

KROTOSZINSKY, R.J., "Autonomy, Community, and Traditions of Liberty: The Contrast of British and American Privacy Law", (1990) Duke L.J. 1398.

LECLERCQ, P., "Essai sur le statut juridique des informations" dans A. Madec, *Les flux transfontières de données: vers une économie internationale de l'information?*, Paris, La Documentation française, 1982.

LOUVEAUX, S., "Article-by-article guide to Directive 95/46/EC", dans *A Business Guide to Changes in European Data Protection Legislation*, Cullen International, 1996.

LUME, P "An EEC Policy for Data Protection", (1992) 11 Computer L.J. 399.

MACKAAY, E., "Les biens informationnels ou le droit de suite dans les idées", dans *L'appropriation des informations*, Paris, Litec, 1985; (1986) 3 Informatica e diritto 45.

MAISL, H., "La directive communautaire du 24 octobre 1995 relative à la protection de la vie privée", (1995) 4 D.I.T. 43.

MARTENS, P., "La vie privée est-elle soluble dans l'éther?" dans C. Doutrelepont, P. Van Binst et L. Wilkin, dir., *Libertés, droits et réseaux dans la société de l'information*, Bruxelles, Bruylant, 1996, p. 183.

MATHEWS, C., R.C. Mathews, "Protection of Rights on Individuals in the EEC in Relation to Automatic Processing of Personal Data" (1987) Int'l Bus. L. 410.

MAXEIMER, J. R., "Freedom of Information and The EU Data Protection Directive"?, (1995) 48 Federal Communications L.J. 93.

MEI, P., "The EC proposed Data Protection Law" (1993) 25 Law & Pol'y Int'l Bus. 305.

MILLAR, S.A., "FTC Expores Consumer Protection in Cyberspace", (1996) The Multimedia L. Report 4.

MILLARD, C. et CAROLINA, R., "Commercial Transactions on the Global Information Infrastructure: A European perspective", (1996) 15 The John Marshall J. of Computer Information L. 269.

MILLER, A.R., "Teleinfomatics, Transborder Data Flaws and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age", (1986) 20 Colum. J.L. & Social Prob. 89.

MOLINARI, P. A., "Les nouveaux moyens de reproduction et les droits de la personnalité", (1986) 46 R. de B. 717.

MOLINARI, P.A. et TRUDEL, P., "Le droit au respect de l'honneur, de la réputation et de la vie privée: Aspects fédéraux et applications" dans *Application des Chartes des droits et libertés en matière civile* (Formation permanente du Barreau), Coswanville, éd. Yvon Blais, 1988, p. 218.

OBERDOFF, H.,"Le droit, la démocratie et la maîtrise sociale des technologies", (1992) 4 Rev. du Droit Public 983.

OSBORNE, P.H., "The Privacy Acts of British Columbia, Manitoba and Saskatchewan" dans D. Gibson, *Aspects of Privacy Law*, Toronto, Butterworths, 1980, p. 75

OUIMET, A., "Vers un régime universel de protection des renseignements personnels dans le secteur privé" dans *Développements récents en droit de l'accès à l'information (1991)*, Coswanville, éd. Yvon Blais, 1991, p. 190.

PARKER, R., "A Definition of Privacy", (1973-74) 27 Rutgers L.R. 275.

PEARSON, H.E, "Data Protection in Europe", (1991) 8 Computer L.J. 24.

PECK, R., "Extending the Constitutional Right to Privacy in the New Technological Age", (1984) 12 Hofstra L.R. 893.

PELADEAU, P., "Esquisse d'une théorie juridique des procès d'information relatifs aux personnes" (1989) 34 Revue de droit de Mc Gill 953.

POST, L., 77 California L.R. 963.

POULLET Y. "La commercialisation des données par le secteur public et vie privée", (1994) Droit de la Consommation 68.

POULLET Y., "OCDE: Protection des données et de la vie privée", (1995) 2 D.I.T. 83.

POULLET, Y. et GERARD, Ph., "Pour un cadre juridique de la diffusion des produits informationnels juridiques", (1994) D.A.O.R. 39.

POULLET, Y., "Le fondement du droit à la protection des données nominatives: Propriété ou Liberté" dans *Nouvelles technologies et propriété*, Montréal, Les Editions Thémis et Litec, 1991, p. 184.

POULLET, Y., "The European Directive relating to the protection of physical persons with regard to the processing of personal data and its free circulation - a state of relative harmony", dans *A Business Guide to Changes in European Data Protection Legislation*, Cullen International, 1996.

POUND, R.,"The Right of Privacy" (1932) Illinois L.R. 237.

PROSSER, L., "Privacy", (1960) 48 California L.R., 383.

RAMKIN, M., "Privacy & Technology: A Canadian Perspective", (1984) 22 Alberta L.R. 323.

REICH, C., "The New Property", (1964) 73 Yale L.J. 733.

REIDENBERG, J., "Data Protection Measures in the United States", (1995) 80 Iowa L. R. 497.

REIDENBERG, J., "Setting Standards for Fair Information Practice in the USA", (1995) 80 Iowa Law Review 13.

REIDENBERG, J.R., "The Privacy Obstacle Course Hurdling Barriers to Transnational Financial Services", (1992) 60 Fordham L.R. S137.

REITER, R. A., "The Legal Protection of Personal Information in the Context of Videotext: A Preliminary Inquiry", (1986) 2 Intel. Prop. J. 273.

RIGAUX, F., "La liberté de la vie privée", (1991) 3 R.I.D.C. 539.

RIGAUX, F., "la protection de la vie privée à l'égard des données à caractère personnel", Ann. dr. Louvain, 1993, 53.

ROCH, M.P.,"Filling the void of Data Protection in the United States: Following the European Example", (1996) 12 Santa Clara Computer and High Technology L. J. 71.

ROTELMANN, W., "Persönlichkeirechte, inbesondere der widerruf ehrenrühriger Behauptungen", (1971) N.J.W. 1637.

SAMUEL, G., "Le "droit subjectif" and English Law", (1987) 46 Cambridge L. J. 264.

SCHWARTZ, P., "European Data Protection Law and Restrictions on International Data Flows", (1995) 80 Iowa L.R. 487.

SCHWEIZER, R.J., "La Convention du Conseil de l'Europe sur la protection des données personnelles et la réglementation des flux transfrontières de données" (1986) 4 Droit de l'informatique 191.

SIMITIS, S., "From the Market to the Polis. The EU Directive on the Protection of Personal Data", (1995) 80 Iowa L.R. 3.

SKALA, S.M., "Is there a Legal Right to Privacy?", (1977-78) 10 Queensland L.J. 127.

STEEVES, V., "Humaniser l'espace cybernétique: la vie privée, la liberté d'expression et l'autoroute de l'information", (1995) 28 Droits de la personne 1.

STERLING, R. A., "Privacy, Computerized Information Systems, and the Common Law-A Comparative Study in The Private Sector", (1983) 18 Gonzaga L.R. 567.

THOMAS P.et BOULANGER M.H., "Y a-t-il un ange gardien dans la salle?", dans C. Doutrelepont, P. Van Binst et L. Wilkin, dir., *Libertés, droits et réseaux dans la société de l'information*, Bruxelles, Bruylant, 1996.

TRUDEL, P., "De l'autoréglementation", (1989) 19 R.D.U.S. 249.

TRUDEL, P., "Introduction au droit du commerce électronique sur l'Internet", (1995) 55 R. du B. 521.

TRUDEL, P., "Les effets juridiques de l'autoréglementation", (1989) 19 Revue de droit de l'Université de Sherbrocke, 251.

TRUDEL, P., "Réflexion pour une approche critique de la notion de droit à l'information en droit international", (1982) 23 Les Cahiers de Droit 847.

VELU, J. et ERGEC, R., "Convention européenne des droits de l'homme, R.P.D.B., compl. t. VII, n° 656.

WACKS, R., "The Proverty of "Privacy"", (1980) 96 The Law Quaterly R. 73.

WARREN S.D. et BRANDEIS, L.D., "The Right of Privacy", (1890) 4. Harv. L.R. 193.

WEINRIB, A. S., "Information and Property", (1988) 38 U.T.L.J. 117.

WESTIN, A. F., "Science, Privacy and Freedom: Issues and Proposals for the 1970's", (1996) 66 Col. L.R. 1003.

WINFIELD, P. H., "Privacy", (1931) The Law Quaterly R., 23-42.

WUERMELING, U.U., "Harmonisation of European Union Privacy Law", (1996) 14 the John Marshall J. of Computer & Information L. 418.

X., "Informatique et libertés: ce qui va changer dans la loi française", (1995) 11 Droit et affaires 1.

ZERDICK, Th., "European Aspects of Data Protection: what rights for the citizen?" (1995) 2 Legal Issues of European Integration 59.

CONFERENCE

THYRAUD, J., "Commentaire article par article du projet de proposition de directive du Conseil des Communautés européennes à l'égard du traitement des données à caractère personnel", Conférence annuelle des commissaires à la protection de la vie privée, Paris, septembre 1990.

SIMITIS, S., "Les propositions pour une directive relative à la protection des données nominatives - une première appréciation", Conférence annuelle des Commissaires à la protection de la vie privée, Paris, septembre 1990.

LAPERRIERE, R., "La protection des renseignements personnels dans le secteur privé au Québec et le projet de loi 68", Conférence de l'UQUAM sur la protection des renseignements personnels: bilans et enjeux, Montréal, 16 avril 1993.BOULANGER,

M.H. et DE TERWANGNE, C., "Internet et la vie privée", Conférence du CRID sur Internet face au droit, Namur, 21 et 22 novembre 1996, p. 7.