Les normes internationales de protection des données personnelles et l'autoroute de l'information*

Karim BENYEKHLEF**

* La recherche pour cet article a été rendue possible grâce à une subvention du C.R.S.H.C. et du F.C.A.R. L'auteur remercie M^e^ François Themens pour sa contribution au repérage de la doctrine. Texte à jour au 31 mars 1995.

** Professeur, Centre de recherche en droit public, Faculté de droit, Université de Montréal.

L'avènement de l'autoroute de l'information relance, en quelque sorte, la question de la protection de la vie privée. Non pas que cette question ait perdu de son intérêt au cours des dernières années. Toutefois, l'observateur constate que les possibilités offertes ou promises par les nouvelles voies électroniques de communication cristallisent, d'une certaine manière, les craintes longtemps associées à l'informatisation des activités humaines. En effet, les possibilités techniques des nouvelles voies électroniques de communication augmentent considérablement la masse d'informations et, par conséquent, de données à caractère personnel circulant dans les réseaux. À cet égard, l'interconnexion des réseaux et l'interaction informatisée ne sont pas étrangères à l'augmentation quantitative des données personnelles circulant dans les réseaux électroniques[1]. Cette *dépossession* informationnelle touchant les citoyens suscite dès lors une série d'interrogations légitimes quant aux moyens susceptibles de protéger la vie privée.

Comment concilier le développement technologique avec les impératifs socio-juridiques représentés notamment par la protection de la vie privée? Cette volonté d'équilibration des intérêts concurrents n'est pas une tâche nouvelle pour le juriste. C'est là, en fait, une tâche récurrente. En l'espèce, celle-ci apparaît toutefois plus complexe à accomplir en raison de plusieurs facteurs afférents à la nature même de l'activité à régir. La délocalisation de l'information, sa grande fluidité, voire son insaisissabilité, son caractère multimédiatique (données, voix, son, image), son intangibilité, sa nature souvent interactive, la multiplicité des acteurs impliqués dans l'opération télématique et, surtout, nous semble-t-il, le caractère irrémédiablement international des réseaux de communication participent à la difficulté de procéder à un arbitrage efficace, opérationnel et harmonieux des intérêts en jeu. Nous aurons l'occasion de revenir sur ces enjeux normatifs dans la seconde partie de cet exposé.

Nous avons souligné le caractère résolument international des nouvelles voies de communication[2]. Il est de coutume maintenant de dire que la

---

1 Comité consultatif sur l'autoroute de l'information, *La protection de la vie privée et l'autoroute canadienne de l'information (Une nouvelle infrastructure de l'information et des communications au Canada)*, Ottawa, Industrie Canada, 1994, p. 3 (ci-après cité : «Comité consultatif-Vie privée»).

2 «Telematics being by its nature international, the multinational companies in particular have taken advantage of these new technological developments. The extended possibilities to transmit information almost without reference to distance, time or volume has given rise to a spectacular growth in transborder data flow through the use of the international telecommunication networks. Already in 1985 the volume in Europe alone stood at

ndialisation des échanges n'est pas étrangère à ce phénomène. Toutefois, delà du cliché, l'interprète note que l'information n'a plus de port d'attache qu'elle circule librement et qu'aucune autorité nationale ne peut à elle seule trôler ou, à tout le moins, policer les échanges d'informations. Cela explique efforts déployés par plusieurs organisations internationales dans le domaine données à caractère personnel. En effet, le droit international n'est pas ncieux en la matière. Il convient donc, dans une première partie, de décrire et nalyser les efforts normatifs entrepris par ces organisations. Dans une xième partie, on se demandera si ces normes internationales sont adaptées nouvelles voies électroniques de communication. En d'autres termes, le eloppement de la technique a-t-il rendu obsolètes, inadaptés ou incomplets principes fondamentaux en matière de gestion de l'information personnelle l'interprète peut retrouver dans les instruments internationaux? Cette stion nous amènera également à traiter des voies normatives susceptibles ncadrer l'autoroute de l'information pour ce qui est de la protection de la vie ée. En effet, au-delà de l'applicabilité des normes internationales, se pose la cile question de leur application pratique. Comment assurer le respect de ces nes dans un environnement électronique tentaculaire qui échappe, par la iplicité de ses réseaux et de ses acteurs, à toute autorité unique ou centrale?

LE DROIT INTERNATIONAL DE LA PROTECTION DES DONNÉES PERSONNELLES

Les documents internationaux

La circulation internationale de l'information soulève donc de difficiles stions liées à la protection transnationale des données à caractère personnel. protection apportée par une législation nationale en la matière ne peut en qu'être limitée géographiquement. Cette délocalisation de l'information a s incité plusieurs législateurs européens à assortir leurs lois de protection des eignements nominatifs de dispositions soumettant l'exportation de données onnelles vers l'étranger à des contrôles ou autorisations préalables. Nous ons que les nouvelles voies électroniques de communication permettent de ourner la législation mise en place sur un territoire national par la simple ortation des données personnelles, soumises à un corpus de règles précises ertu de la loi, vers des pays dépourvus de toute législation sur la protection renseignements nominatifs[3].

---

around 12 million transborder data transactions per day. Gradually the world economy is transforming itself rom an industrial-based economy to an information-based economy, in which the free exchange of nformation has become the life-blood of modern business life.» Adriana C.M. NUGTER, *Transborder Flow of Personal Data within the EC*, Deventer, Kluwer, 1990, p. 1.

«But it is not only the storage of personal data that constitutes a threat to the personal life sphere of the ndividual. Modern processing facilities as much as the interconnexion of computer systems, due to telematics,

Il existe donc des dispositions législatives qui prohibent toute transmission de données personnelles, à partir du territoire national, vers les pays dont le droit interne n'assure pas une protection satisfaisante aux données nominatives. D'aucuns ont soutenu que de tels dispositifs posaient un risque au regard de la libre circulation de l'information. En effet, ne se trouve-t-on pas à contrôler, et parfois à restreindre, la circulation de l'information au plan international? Deux principes fondamentaux afférents au droit des libertés publiques se trouvent dès lors en conflit : le droit au respect de la vie privée et la libre circulation de l'information, composante du droit à l'information[4].

Deux institutions internationales ont rapidement saisi la nécessité d'assurer une certaine harmonie dans le domaine des législations de protection des renseignements personnels. Il faut éviter que ces législations ne créent des barrières, parfois artificielles et injustifiées, à la libre circulation de l'information tout en tenant compte des préoccupations nationales légitimes relatives à la protection de la vie privée informationnelle. C'est ainsi que l'OCDE[5] adopte en 1980 les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*[6] et que le Conseil de l'Europe adopte en 1981 la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*[7]. Les Lignes directrices se présentent sous la forme d'une recommandation aux États membres. Il ne s'agit donc pas d'un instrument juridique contraignant contrairement à la Convention européenne. Nous y reviendrons.

C'est dans ce contexte que la Commission de l'Union européenne a décidé de proposer diverses mesures propres à assurer, d'une part, la protection des données à caractère personnel et, d'autre part, une circulation libre et sans

---

have increased the concern about the protection of privacy, especially in an international context. The question has arisen to what extent national privacy laws afford adequate protection to individuals when data concerning them flow across borders. In principle, it should make no difference to either multinational companies or data subjects whether data processing operations take place in one country or in one or more other countries. The same fundamental rules should apply and data subjects should be given the same safeguards for the protection of their rights and interests. In practice, however, the protection of individuals grows weaker when the geographic area is widened. Concern has been expressed that data users might seek to avoid data protection controls by moving their operations, in whole or in part, to so-called data h(e)avens, *i.e.*, countries which have less strict privacy legislation, or none at all. In order to counter that risk some countries have built into their domestic law special measures to control the export and import of personal data», A.C.M. NUGTER, *op. cit.*, note 2, pp. 3 et 4.

4 Lire Roger PINTO, *La liberté d'information et d'opinion en droit international*, Paris, Economica, 1984.

5 Organisation de Coopération et de Développement Économiques.

6 Organisation de Coopération et de Développement Économiques, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* (Paris, 1980) (ci-après citées : «Lignes directrices»).

7 Conseil de l'Europe, *Convention pour la protection de personnes à l'égard du traitement automatisé des données à caractère personnel* (Strasbourg, 1981) (ci-après citée : «Convention européenne»).

entraves de l'information personnelle. La création du grand marché intérieur militait également pour une initiative de la Commission[8]. En 1990, la Commission présentait un projet de directive sur le sujet qui s'est rapidement heurté à une forte opposition[9]. En 1992, la Commission présentait un projet amendé de directive : *Proposition 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*[10]. Cette proposition devrait, en principe, être adoptée en 1995 avec quelques modifications présentées dans la Position commune arrêtée par le Conseil des ministres[11].

Les Nations-Unies ont également développé un corpus réglementaire en la matière : les *Principes directeurs sur l'utilisation des fichiers personnels informatisés*[12]. Examinons maintenant succinctement ces divers instruments.

1. Les Lignes directrices de l'OCDE et la Convention européenne

Nous traiterons en même temps de ces deux instruments. Ceux-ci constituent en effet les premiers efforts normatifs internationaux visant à régir les flux transfrontières de données à caractère personnel. Les deux organismes ont d'ailleurs étroitement collaboré dans l'élaboration de leurs instruments

---

8 «La diversité des approches nationales et l'absence d'un système de protection à l'échelle de la Communauté constituent un obstacle à l'achèvement du marché intérieur. En effet, si les droits fondamentaux des personnes concernées, notamment le droit à la vie privée, ne sont pas assurés au niveau communautaire, le flux transfrontalier de données pourrait être entravé alors qu'il est devenu indispensable aux activités des entreprises et des organismes de recherche ainsi qu'à la collaboration entre les administrations des États membres dans le cadre de l'espace sans frontières prévu à l'article 8A du traité», *Communication de la Commission relative à la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté et à la sécurité des systèmes d'information*, COM(90) 314 final-SYN 287 et 288, Bruxelles, Septembre 1990, p. 4.

9 Sur ce premier projet de directive de la Commission, lire Karim BENYEKHLEF, «Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes», (1992) 2 *M.C.L.R.* 149.

10 *Proposition 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*, COM(92) 422 final-SYN 287, Bruxelles, 15 octobre 1992.

11 Position commune arrêtée par le Conseil le 20 février 1995 en vue de l'adoption de la Directive 94// CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation de ces données, 12003/3/94 REV 3, Bruxelles, 20 février 1995, (ci-après citée : «Position commune de 1995»). Ce texte reprend en le modifiant le projet de directive de 1992. Le projet de directive a finalement été adopté le 24 octobre 1995. La nouvelle directive reprend en substance le libellé de la Position commune. Les modifications sont mineures.

12 Nous ne traiterons pas de ces principes compte tenu de leur importance somme toute mineure dans le droit international de la protection des données personnelles. Le lecteur pourra toujours se référer à : Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Éditions Thémis, 1992, pp. 336-342.

respectifs[13]. Ces deux documents proposent un dispositif susceptible d'équilibrer le principe de la libre circulation de l'information et la protection des données personnelles. Cette préoccupation apparaît clairement dans les préambules des Lignes directrices et de la Convention européenne.

Ce souci d'harmonie passe d'abord par l'affirmation du droit à la protection de la vie privée. Ainsi, l'article 6 des Lignes directrices est indicatif de cette affirmation :

> *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.*

Les principes consacrés dans les Lignes directrices constituent ainsi le plus petit commun dénominateur en matière de protection des données à caractère personnel. Il s'agit d'insuffler au droit général de la protection des données personnelles une harmonie législative minimale. Ces normes minimales sont néanmoins susceptibles d'une certaine extension. L'article 3a) énonce que les Lignes directrices ne devraient pas être interprétées comme interdisant d'appliquer, à diverses catégories de données personnelles, des mesures de protection différentes selon leur nature et le contexte dans lequel elles sont collectées, enregistrées, traitées ou diffusées. Cette disposition, qu'il faut lire en conjonction avec l'article 6, laisse entendre clairement que des mesures de protections plus strictes que celles mises de l'avant dans les Lignes directrices peuvent être adoptées par les pays membres. Le libellé de l'article 3a) est néanmoins prudent, puisqu'on évoque simplement certaines catégories de données personnelles. On réfère implicitement sans doute aux données à caractère sensible pour lesquelles plusieurs législateurs européens ont aménagé un régime de protection plus exigeant[14]. Cette prudence s'explique par le but poursuivi par les Lignes directrices, à savoir l'harmonisation des règles nationales relatives à la protection des données à caractère personnel. On ne saurait en effet permettre une protection pluriforme sans crainte de mettre ultimement en échec cet objectif fondamental[15].

Tout comme pour les Lignes directrices, une disposition de la Convention européenne permet aux pays signataires de prévoir une protection plus étendue

---

13 Michael D. KIRBY, «Transborder Data Flows and the "Basic Rules" of Data Privacy», (1980) 16 *Stan. J. Int'l L.* 42, 43.

14 Dans la législation européenne, certains types de données relatives à l'origine raciale et ethnique, aux opinions politiques, aux convictions religieuses, philosophiques ou morales, aux activités sexuelles ou à l'appartenance syndicale sont dites sensibles et soumises à un régime juridique plus strict.

15 L'article 18 des Lignes directrices confirme, en quelque sorte, cette analyse : «Les pays Membres devraient éviter d'élaborer des lois, des politiques et des procédures, qui, sous couvert de la protection de la vie privée et des libertés individuelles, créeraient des obstacles à la circulation transfrontière des données de caractère personnel et iraient au-delà des exigences propres à cette protection.»

celle que l'on retrouve dans cet instrument. L'article 11 autorise alors l'État à order à certaines catégories de données une protection spécifique plus ortante que celle, par ailleurs, reconnue aux autres types d'informations sonnelles. On pense ici encore une fois évidemment aux données sensibles. encore, ce régime particulier peut nuire à la circulation de l'information sonnelle. Ce régime, dérogeant à la notion de normes minimales, peut aîner une restriction à la libre circulation de l'information. Mais, à l'instar des es directrices, cette restriction apparaît légitime au regard de l'article 12(3)a) a Convention.

Pour ce qui est du champ d'application de ces instruments, on remarque s s'appliquent aussi bien au secteur public qu'au secteur privé. Alors que les es directrices couvrent tant les fichiers automatisés que les fichiers uels [16], la Convention européenne ne vise que les fichiers automatisés [17]. s ce dernier cas, en vertu de l'article 3(2)c), un État peut néanmoins préciser, du dépôt de son instrument de ratification ou à tout autre moment ultérieur, appliquera également la Convention aux fichiers manuels. Les deux ruments ne s'appliquent qu'aux personnes physiques à l'exclusion des sonnes morales. La Convention européenne prévoit toutefois explicitement la sibilité d'étendre la protection de son dispositif aux personnes morales [18].

Les deux instruments consacrent l'essentiel des principes fondamentaux en ière de gestion de l'information personnelle. Ces principes sont les suivants : cipe de la justification sociale [19], principe de la limitation en matière de ecte [20], principe de la qualité des données [21], principe de la spécification des ités [22], principe de la limitation de l'utilisation [23], principe de sécurité [24], cipe de la transparence [25], principe de la détention limitée dans le temps [26],

---

Lignes directrices, précitées, note 6, art. 2.

Convention européenne, précitée, note 7, art. 3(1).

Id., art. 3(2)b).

Id., art. 6.

Id., art. 5a) et Lignes directrices, précitées, note 6, art. 7.

Convention européenne, précitée, note 7, art. 5c) et 5d) et Lignes directrices, précitées, note 6, art. 8.

Convention européenne, précitée, note 7, art. 5b) et Lignes directrices, précitées, note 6, art. 9.

Convention européenne, précitée, note 7, art. 5b) et Lignes directrices, précitées, note 6, art. 10.

Convention européenne, précitée, note 7, art. 7 et Lignes directrices, précitées, note 6, art. 11.

Convention européenne, précitée, note 7, art. 8a) et Lignes directrices, précitées, note 6, art. 12.

Convention européenne, précitée, note 7, art. 5e) et Lignes directrices, précitées, note 6, art. 8 et 10 (interprétation conjuguée).

principe de la responsabilité[27] et principe de la participation[28]. Ces principes fondamentaux constituent, en quelque sorte, l'architectonique des diverses lois nationales de protection des renseignements personnels. En effet, bien que ces instruments puissent diverger au plan de leur structure et de leur portée, l'interprète peut remarquer qu'ils s'articulent, malgré tout, autour d'un corpus de règles communes. Ainsi, on retrouve ces principes fondamentaux, sous une forme ou une autre, dans les instruments nationaux ou internationaux de protection des données nominatives[29]. Cette invariance normative n'avait pas échappé aux rédacteurs des Lignes directrices et de la Convention européenne. À partir de cette invariance, l'OCDE et le Conseil de l'Europe ont été en mesure de développer un faisceau minimal de protection des données à caractère personnel. Il s'agit d'harmoniser les principes de base (*noyau dur*) et non pas de chercher à harmoniser les ensembles législatifs eux-mêmes[30]. Cette dernière tâche apparaît difficile, voire impossible, compte tenu de la diversité juridique des pays membres de l'OCDE ou du Conseil de l'Europe[31].

La mise en oeuvre des principes fondamentaux n'est pas abordée de la même manière dans les deux instruments. Ainsi, l'article 4 de la Convention européenne porte que chaque État doit prendre, dans son droit interne, les mesures nécessaires pour donner effet aux principes fondamentaux. Le

---

27 Convention européenne, précitée, note 7, art. 8d) et 10 et Lignes directrices, précitées, note 6, art. 14.

28 Convention européenne, précitée, note 7, art. 8 et Lignes directrices, précitées, note 6, art. 13. Pour une analyse des principes fondamentaux en matière de gestion de l'information personnelle, lire K. BENYEKHLEF, *op. cit.*, note 12, p. 100 et suiv.

29 «In spite of the great variety of methods and styles, the various European laws exhibit a basic harmony. They share a common philosophy in purpose and objective.» Frits W. HONDIUS, «Data Law in Europe», (1980) 16 *Stan. J. Int'l L.* 87, 94. Lire également du même auteur : «A Decade of International Data Protection», (1983) 30 *Neth. Int'l L. Rev.* 103, 109 et 110.

30 «Les principes du "noyau dur" reconnaissent aux personnes concernées dans tous les États 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 dès lors entre les Parties et, par conséquent, comportera une diminution des possibilités de conflits de lois ou de juridictions.» 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. 12 (ci-après cité : «Rapport explicatif»). Les rédacteurs du Rapport explicatif ont également remarqué l'existence d'un consensus parmi les lois nationales. Ils écrivent à la page 7 : «Toutes les lois nationales sur la protection des données ainsi que les propositions de législation qui ont été rendues publiques contiennent des *règles similaires* sur le droit matériel relatif au traitement des données, c'est-à-dire sur la qualité des données et sur leur utilisation.» (nos italiques).

31 Gassman souligne justement : «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 effort 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». Hans Peter GASSMANN, «Vers un cadre juridique international pour l'informatique et autres nouvelles techniques de l'information», (1985) *Annu. franc. de Droit Internat.* 747, 755.

paragraphe 2 du même article indique que ces mesures doivent être prises par l'État au plus tard au moment de l'entrée en vigueur de la Convention à son égard. L'État doit faire oeuvre de droit positif afin de consacrer les principes fondamentaux édictés à la Convention. Celle-ci n'est donc pas auto-exécutoire[32]. Quant aux Lignes directrices, son article 19 traite de cette question. Il ne faut pas perdre de vue le caractère non contraignant, au point de vue juridique, de cet instrument international. Il s'agit d'une recommandation. Cela explique sans doute le ton non-directif de l'article 19. On y dit, de manière liminaire, que les pays membres devraient établir des procédures juridiques, administratives et autres, ou des institutions pour protéger la vie privée et les libertés individuelles eu égard aux données de caractère personnel. Par ailleurs, les rédacteurs invitent les pays membres à s'efforcer d'adopter une législation nationale appropriée[33] ou de favoriser et de soutenir des systèmes d'autoréglementation (codes de déontologie ou autres formes)[34]. Il s'agit là des deux voies essentielles de mise en oeuvre des principes fondamentaux en matière de gestion de l'information personnelle.

La distinction entre les deux instruments est nette. Les Lignes directrices semblent autoriser les États à opter pour la voie exclusive de l'autoréglementation alors qu'une telle option est inacceptable au regard de la Convention européenne. Non pas que la Convention interdise le recours à l'autoréglementation. Elle refuse qu'on en fasse le véhicule exclusif de régulation interne du droit de la protection des données personnelles. L'autoréglementation apparaît alors comme un mode de régulation complémentaire à une action législative[35].

La Partie V des Lignes directrices, intitulée «Coopération internationale», et le chapitre IV de la Convention européenne, intitulé «Entraide», ont pour objet de pallier les difficultés pratiques suscitées par la circulation transnationale de l'information personnelle. Ces dispositifs prévoient que les Parties contractantes s'accordent mutuellement assistance dans la mise en oeuvre des principes fondamentaux. Il importe également de fournir une assistance aux personnes fichées désirant exercer leurs droits à l'endroit d'un fichier étranger. Il convient de souligner que le dispositif de la Convention européenne est beaucoup plus complet à cet égard que celui des Lignes directrices de l'OCDE. Ainsi l'assistance aux personnes fichées, notamment, fait l'objet de dispositions plus

---

32 «Comme cet article l'indique, la Convention oblige les Parties à incorporer des dispositions sur la protection des données dans leur législation. En effet, la Convention n'a pas été conçue comme self-executing [auto-exécutoire] et par conséquent les droits des individus ne peuvent découler directement d'elle.» Rapport explicatif, précité, note 30, p. 16.

33 Lignes directrices, précitées, note 6, art. 19a).

34 *Id.*, art. 19b).

35 Rapport explicatif, précité, note 30, p. 16.

détaillées[36]. Le caractère contraignant de la Convention européenne expliqu sans doute la complétude du système d'entraide et d'assistance.

Il faut rappeler que les Lignes directrices ne constituent qu'une simp recommandation. Le Canada a adhéré aux Lignes directrices en 1984. Quant la Convention européenne, il s'agit d'un document juridiquement contraignar Cette dernière est entrée en vigueur en 1985 suite à sa ratification par cinq pa membres du Conseil de l'Europe[37].

Ces instruments internationaux ont eu un succès pour le moins mitigé. effet, la Commission de l'Union européenne note que la Convention européen n'a pas permis d'atténuer les disparités normatives entre les diverses législatio nationales :

> *La Convention du 28 janvier 1981 du Conseil de l'Europe pour protection des personnes à l'égard du traitement automatisé d données à caractère personnel n'a pas permis de limiter cette dispar dans la mesure où, d'une part, elle laisse ouvert un grand nomb d'options pour la mise en oeuvre des principes de base qu'elle définie d'autre part, elle n'a été ratifié que par sept Etats membres (Allemagr Danemark, Espagne, France, Irlande, Luxembourg, Royaume-Uni dont un (Espagne[39]) qui n'a toujours pas de législation interne. recommandation de la Commission du 29 juillet 1981 invitant les Eta membres de la Communauté à ratifier la convention du Conseil l'Europe n'a pas modifié cette situation.*[40]

La Commission a donc estimé nécessaire d'intervenir afin de corriger cet situation[41]. Nous y reviendrons. Quant aux Lignes directrices, l'interprè remarque que l'autoréglementation, voie de mise en oeuvre du dispositif de recommandation, n'a pas permis d'amoindrir l'écart normatif existant entre l

---

36 Pour en savoir plus, lire K. BENYEKHLEF, *op. cit.*, note 12, pp. 352 à 357.

37 Douze pays membres du Conseil de l'Europe ont, jusqu'à ce jour, signé, ratifié et adopté une législat relative à la protection des données personnelles : Allemagne, Autriche, Danemark, Espagne, Finlan France, Islande, Luxembourg, Norvège, Royaume-Uni et Suède. Sept pays ont signé ladite Convention s l'avoir ratifiée ou sans avoir adopté une législation relative à la protection des données personnelle Belgique, Chypre, Grèce, Italie, Pays-Bas, Portugal et Turquie.

38 Ce chiffre n'est plus exact aujourd'hui. Voir note 37.

39 L'Espagne est aujourd'hui dotée d'une législation en la matière : *Loi organique 5/1992, du 29 octobre, réglementation du traitement automatisé des données à caractère personnel*.

40 *Proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement des donn à caractère personnel* (Exposé des motifs), COM(90) 314 final-SYN 287, Bruxelles, Septembre 1990, p. Le lecteur notera qu'il s'agit là de l'exposé des motifs de la première version du projet de directive.

41 Pour un exposé plus complet des motifs d'intervention de la Commission, lire K. BENYEKHLEF, *loc. cit.*, r 9, 186-189.

rs européens et l'Amérique du Nord. Le Canada et les États-Unis ont ouragé le secteur privé à développer des codes de conduite propres à régir le tement de l'information personnelle. Le secteur privé nord-américain a galement répondu à l'appel[42]. En fait, l'OCDE elle-même semble reconnaître uffisance de la seule voie autoréglementaire[43].

En terminant, il importe de signaler que le Conseil de l'Europe a également pté toute une série de recommandations visant à assurer la protection des nées personnelles dans divers secteurs, comme la santé, le marketing direct la police[44]. Il faut bien comprendre que la Convention européenne est un rument de nature globale ou générale. C'est-à-dire qu'elle a vocation de pliquer tant au secteur public que privé sans que des distinctions, de nature damentale, n'affectent l'un ou l'autre de ces secteurs. Le Conseil de l'Europe néanmoins estimé nécessaire d'adapter ces principes généraux ou damentaux à certains secteurs de l'activité humaine. Ces recommandations vèrent alors complémentaires :

Sur le secteur des institutions financières américaines, lire Karim BENYEKHLEF, *La protection des données personnelles dans le secteur des institutions financières américaines*, Rapport rédigé pour le ministère fédéral de la Justice, Mai 1993. Après une analyse du droit américain en la matière, on procède à une comparaison avec le secteur des institutions financières canadiennes. Lire également H. Jeff SMITH, «Privacy Policies and Practices : Inside the Organizational Maze», (1993) 36 *Communications of the ACM* 105.

«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.*» OCDE, *Present Situation and Trends in Privacy Protection in the OECD Area*, Paris, DSTI/ICCP/88.5, 1er juin 1988, p.19 (nos italiques, ci-après cité : «Rapport de l'OCDE de 1988»).

Recommandation n° R(81) 1 relative à la réglementation applicable aux banques de données médicales automatisées (23 janvier 1981); Recommandation n° R(83) 10 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques (23 septembre 1983); Recommandation n° R(85) 20 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques (23 septembre 1985); Recommandation n° R(86) 1 relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale (23 janvier 1986); Recommandation n° R(87) 15 relative à l'utilisation de données à caractère personnel dans le secteur de la police (17 septembre 1987); Recommandation n° R(89) 2 relative à la protection des données à caractère personnel utilisées à des fins d'emploi (18 janvier 1989); Recommandation n° R(90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes (13 septembre 1990) et Recommandation n° R(91) 10 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics (9 septembre 1991).

> *The Council of Europe through its Legal Committee has developed a number of sectoral recommendations which arise from the more general provisions of the Convention on data protection. The view has been taken that specific sectors have particular difficulties with the Articles contained in the Convention, and so recommendations need to be made in order to make proper allowance for these problems.*[45]

Le texte des recommandations doit donc être lu à la lumière de la Convention européenne. Le dispositif de celles-ci est en effet fondé sur les principes fondamentaux énoncés à la Convention. Les recommandations explicitent donc simplement les principes fondamentaux (ou certains de ceux-ci) au regard des spécificités inhérentes au secteur d'activités visé. Par ailleurs, ces textes, ainsi que leur titre l'indique, n'ont aucune force exécutoire. On incite simplement les États membres à tenir compte, dans leur droit interne, du dispositif que l'on y retrouve.

2. La proposition de directive de la Commission européenne

La proposition de directive de la Commission européenne est un instrument ambitieux qui a pour objectif de concilier là encore le principe de la libre circulation de l'information, ingrédient primordial dans l'élaboration du grand marché intérieur, et la protection des données à caractère personnel. Il s'agit notamment de créer une zone européenne de libre circulation de l'information; les pays membres ayant traduit la directive dans leur droit interne, il ne devrait plus y avoir, en principe, de restrictions législatives à la circulation de données personnelles. Cet objectif apparaît clairement à l'article 1 du projet de directive tel qu'amendé par la Position commune de 1995 :

> *1- Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.*
>
> *2- Les États membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre États membres pour des raisons relatives à la protection assurée en vertu du paragraphe 1.*

Nous nous proposons dans les lignes qui suivent de décrire le contenu du projet de directive tel qu'amendé par la Position commune arrêtée par le Conseil des ministres en 1995[46]. Cet exercice n'est pas inutile puisque si ce document

---

45 Rapport de l'OCDE de 1988, précité, note 43, p. 4.

46 Voir note 11.

adopté, il constituera sans doute la norme internationale de référence en ière de protection des données personnelles.

a) *Champ d'application*

Le projet de directive s'applique, en principe, indistinctement au secteur lic et au secteur privé[47]. De même, il vise aussi bien le traitement automatisé 'information personnel que les fichiers manuels[48]. À ce propos, l'article 3(2) cise que sont exclus du champ de la directive, les traitements de données à actère personnel effectués par une personne physique pour l'exercice ctivités exclusivement personnelles ou domestiques. Le projet de directive ne pplique qu'aux personnes physiques, à l'exclusion, par conséquent, des sonnes morales[49].

b) *Collecte et traitement*

L'article 6 consacre les principe de la limitation en matière de collecte, de la cification des finalités et de la qualité des données. Autrement dit, les nées personnelles doivent être collectées loyalement et licitement. Elles ent être collectées pour des finalités déterminées, explicites et légitimes, et sées de manière compatible avec ces finalités[50]. De plus, les données ent être adéquates, pertinentes et non excessives au regard des finalités r lesquelles elles sont traitées[51]. Les données doivent également être ctes et, si nécessaire, mises à jour. L'article 6(1)d) précise à ce propos que es les mesures raisonnables doivent être prises pour que les données actes ou incomplètes, au regard des finalités de collecte, soient effacées ou ifiées. L'article 6(1)e) consacre, pour sa part, le principe de la détention ée dans le temps.

Les données personnelles ne peuvent être collectées, nous dit l'article 7, que personne concernée y consent indubitablement; si elles sont nécessaires r l'exécution d'un contrat ou de mesures précontractuelles; si elles sont essaires pour respecter une obligation légale à laquelle le responsable du ement est soumis; si elles sont nécessaires à la sauvegarde de l'intérêt vital

---

Le premier projet de directive de 1990 traitait différemment les deux secteurs. Lire notamment Robert G. BOEHMER et Todd S. PALMER, «The 1992 EC Data Protection Proposal : An Examination of Its Implications for U.S. Business and U.S. Privacy Law», (1993) 31 *Am. Bus. L.J.* 265, 294.

Position commune de 1995, précitée, note 11, art. 3.

Peter MEI, «The EC Proposed Data Protection Law», (1993-94) *Law & Pol. Int'l Bus.* 305, 311.

Position commune de 1995, précitée, note 11, art. 6(1)b).

Id., art. 6(1)c).

de la personne concernée; si elles sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ou finalement si elles sont nécessaires à la réalisation de l'intérêt légitime du responsable du traitement ou du ou des tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits ou libertés fondamentaux de la personne concernée. L'exposé des motifs de la Commission est silencieux quant au mode d'appréciation des intérêts légitimes du responsable du traitement et de ceux de la personne concernée. Il y a là un exercice d'équilibration. Toutefois, la Commission ne nous donne aucun indice susceptible de mieux saisir la nature de cet exercice.

L'article 8 porte sur des catégories particulières de données : les données dites sensibles. Ainsi, les données relatives à l'origine raciale et ethnique, l'opinion politique, les convictions religieuses ou philosophiques, l'appartenance syndicale, la santé et la vie sexuelle sont l'objet de conditions particulières de cueillette et de traitement. Ces conditions sont évidemment plus strictes.

c) *Droits des personnes fichées*

L'article 12 reconnaît le principe de la participation. Ainsi, la personne fichée a droit d'obtenir, sur demande, à des intervalles raisonnables et sans délai ou frais excessifs, la confirmation que des données la concernant sont ou ne sont pas traitées, la communication de ces données sous une forme intelligible et des informations sur leur origine ainsi que sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées[52]. Le projet de directive va beaucoup plus loin que la Convention européenne sur ce point. Le droit d'accès reconnu à la personne fichée lui permet d'exercer un véritable droit de regard sur les données la concernant. Le paragraphe 2 de l'article 12 complète le dispositif en octroyant à la personne fichée le droit d'obtenir la rectification des données inexactes ou incomplètes, leur effacement ou leur verrouillage lorsque le traitement n'est pas conforme aux dispositions de la directive. De plus, la personne fichée peut obtenir, en cas de rectification, d'effacement ou de verrouillage, la notification aux tiers, à qui ont été communiquées les données, de cette rectification, effacement ou verrouillage. L'article 13 prévoit des cas d'exception au droit d'accès. Il s'agit des exceptions désormais classiques relatives à la sûreté de l'État, de la sécurité publique, etc. Le paragraphe 4 de l'article 28 précise toutefois que chaque autorité de contrôle, c'est-à-dire l'agence nationale de protection des données personnelles, peut être saisie par toute personne d'une demande de vérification de la licéité d'un traitement lorsque les dispositions nationales prises en vertu de l'article 13 sont d'application. On ajoute que la personne concernée est à tout le moins informée

52 *Id.*, art. 12(1).

qu'une vérification a eu lieu. L'autorité de contrôle s'assure donc que le droit d'accès n'est pas restreint pour des motifs étrangers à ceux énumérés à l'article 13 (sûreté publique, poursuites pénales, etc.).

L'article 14 constitue une innovation intéressante par rapport aux autres nstruments internationaux en la matière. Il prévoit que la personne fichée peut s'opposer, à tout moment et dans certains cas, pour des raisons prépondérantes enant à sa situation particulière, à ce que des données la concernant fassent 'objet d'un traitement. Si son opposition est justifiée, le traitement mis en oeuvre par le responsable ne peut plus porter sur ces données. L'article 15, visiblement nspiré par la législation française, reconnaît à toute personne le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou 'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé destiné à évaluer certains aspects de sa personnalité (rendement professionnel, crédit, fiabilité, comportement, etc.)[53].

La Section IV, intitulée «Information de la personne concernée», oblige le responsable du traitement à donner certaines informations à la personne fichée. Ainsi, l'article 10 prévoit que toute personne a le droit de connaître l'identité du responsable du traitement et, le cas échéant, de son représentant, les finalités du traitement auquel les données sont destinées, les destinataires des données, 'existence d'un droit d'accès et de rectification concernant ces données et le caractère obligatoire ou non de la réponse aux questions qui font l'objet de la collecte. Il s'agit là bien sûr de l'application du principe de la transparence. L'article 11 astreint le responsable du traitement lorsque les données n'ont pas été collectées auprès de la personne concernée à fournir à cette dernière, dès 'enregistrement des données ou, si une communication à un tiers est envisagée, au plus tard lors de la première communication des informations relatives à 'identité du responsable du traitement et aux finalités du traitement. Le responsable du traitement peut être astreint également à informer la personne fichée des catégories de données concernées, des destinataires ou des catégories de destinataires des données et de l'existence d'un droit d'accès et de rectification des données la concernant dans la mesure où, poursuit la directive, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations sont nécessaires pour assurer à l'égard de la

---

53 Mei note que la disposition du Projet de directive de 1992 compliquera sans doute la tâche d'un grand nombre d'entreprises américaines ayant recours à la décision assistée : «The United States may have difficulty complying with Article 16 of the Amended Proposal. This is the provision that forbids adverse decisions against individuals from being based solely on automated processing. According to the Amended Proposal, any such adverse decision must be reviewed by a human being before it may be issued. Many categories of decision making are based strictly on factual criteria and can be processed more quickly and efficiently if performed by a computer. Examples include systems that check for a minimum annual income before issuing a credit card, or a minimum income-to-debt ratio before approving a personal loan. Such decision making would be permitted by the Proposed Amendment to justify positive responses, but every negative response requires that the decision result from personal, as well as computer, analysis.» P. MEI, *loc. cit.*, note 49, 330.

personne concernée un traitement loyal des données. Le paragraphe
l'article 11 prévoit une exception à ces obligations d'information dans le cas
traitement à finalité statistique, historique ou scientifique ou alors dar
situation où l'information de la personne concernée se révèle impossibl
implique des efforts disproportionnés ou encore si la législation pr
expressément l'enregistrement ou la communication des données. Dans ces
la directive oblige les États membres à prévoir des garanties appropriées.

d) *Devoirs du responsable du traitement*

Nous avons déjà présenté ci-haut quelques obligations du responsabl
traitement. Ce dernier doit, de plus, notifier à l'autorité de contrôle la mis
oeuvre d'un traitement automatisé[54]. L'article 19 prévoit le contenu c
notification. Cette notification comprend les nom et adresse du responsabl
traitement, la ou les finalités du traitement, la ou les catégories de perso
concernées, la description des données ou des catégories de données
lesquelles porte le traitement, les destinataires ou les catégories de destinat
auxquels les données sont susceptibles d'être communiquées, les transfer
données envisagés avec des pays tiers et la description des mesure
sécurité. L'article 18 prévoit une procédure de notification simplifiée et,
certains cas, l'exonération de l'obligation de notification[55].

Par ailleurs, l'article 17 oblige le responsable du traitement à prendre
mesures techniques et d'organisation appropriées nécessaires à la prote
contre la destruction, accidentelle ou illicite, la perte accidentelle, ainsi
contre l'altération, la diffusion ou l'accès non autorisés et contre toute a
forme de traitement illicite de données à caractère personnel. La dispos
précise d'autres modalités de sécurité auxquelles doit s'astreindre le respons
du traitement.

e) *Autoréglementation*

Le projet de directive, à l'instar de la Convention européenne, reconn
complémentarité que peut apporter la voie autoréglementaire au plan norr
Mais il ne s'agit bien que de complémentarité. En d'autres mots, cette voi
saurait à elle seule satisfaire aux exigences de la directive. L'article 27(1
explicite à cet égard :

---

54 Position commune de 1995, précitée, note 11, art. 18(1).

55 «Some commentators estimate that simplified requirements could excuse eighty percent of a con
processing operations from the notification provision.» P. MEI, *loc. cit.*, note 49, 331.

1- Les États membres et la Commission encouragent 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 états membres en application de la présente directive.

Cet article reconnaît donc la possibilité de développer des codes nationaux bonne conduite. Le paragraphe 3 de l'article 27 reconnaît également cette sibilité au plan communautaire. On y encourage les milieux professionnels à ticiper à l'élaboration de codes de conduite communautaires, destinés à tribuer à la bonne application de la directive en fonction de la spécificité des teurs.

Au plan national, le paragraphe 2 de l'article 27 énonce que les projets de le peuvent être examinés par l'autorité nationale de contrôle, qui s'assure de conformité des projets soumis avec les dispositions nationales prises en lication de la directive. Si elle l'estime opportun, l'autorité nationale de trôle peut recueillir les observations des personnes concernées ou de leurs résentants.

f) *Institutions*

Au plan institutionnel, le projet de directive prévoit, à son article 28, la mise place d'une autorité de contrôle chargée de surveiller l'application des positions nationales prises en application de la directive. Cette autorité stitue bien évidemment l'agence de protection des données personnelles[56]. paragraphe 3 énonce les pouvoirs dont doit disposer cette autorité de trôle : pouvoirs d'investigation, droit d'ester en justice, pouvoir d'ordonner le rouillage ou l'effacement, etc.

L'article 29 établit un groupe de protection des personnes à l'égard du tement des données à caractère personnel à l'échelle communautaire. Ce upe à caractère consultatif et indépendant est composé des représentants autorités de contrôle mises en place en vertu de l'article 28, d'un résentant de la Commission et d'un représentant de l'autorité ou des autorités ées pour les institutions et organismes communautaires. Il s'agit, en quelque e, d'une agence européenne de protection des données personnelles. Ce upe n'a cependant qu'un caractère consultatif en ce que sa mission se limite, on l'article 30, à donner des avis sur le niveau de protection dans la nmunauté et dans les pays tiers, à conseiller la Commission sur tout projet de lification à la directive, à donner son avis sur les codes de conduite élaborés niveau communautaire, à contribuer à l'application homogène des

---

Sur ce sujet, lire David H. FLAHERTY, *Protecting Privacy in Surveillance Societies*, Chapel Hill, The University of North Carolina Press, 1989.

dispositions nationales prises pour la mise en oeuvre de la directive. Par ailleurs, le groupe peut émettre *proprio motu* des recommandations sur toute question pertinente au droit de la protection des données personnelles.

La Commission européenne présentait en 1990 un autre projet de directive relatif à la protection des données personnelles utilisées en matière de télécommunications[57]. Ce projet fut également l'objet d'importantes modifications. La Commission devait présenter en 1994 une version remaniée de ce projet de directive[58]. Cette proposition constitue, en quelque sorte, une application des principes fondamentaux, énoncés dans le projet de directive générale (que nous venons d'examiner), au domaine particulier des télécommunications. Il s'agit donc de mesures complémentaires. On peut parler d'une directive sectorielle, à l'instar des recommandations adoptées par le Conseil de l'Europe[59]. La Commission estime que le secteur des télécommunications exige l'élaboration d'un instrument spécifique qui tiendra compte de ses particularités; d'autant plus qu'il semble que les législations nationales pertinentes en l'espèce instituent des normes de plus en plus divergentes entre elles[60].

Le projet de directive sectorielle établit donc un corpus de règles propres à assurer la protection des données personnelles relativement à des opérations de télécommunications, telles que les données de facturation, l'identification des appels (ligne appelante), les renvois d'appel, l'écoute des communications, les appels non sollicités et les annuaires.

---

57 Proposition de directive du Conseil concernant la protection des données à caractère personnel et de la vie privée dans le contexte des réseaux de télécommunications numériques publics, et en particulier du réseau numérique à intégration de services (RNIS) et des réseaux numériques mobiles publics, COM(90) 314 final SYN-288, Bruxelles, Septembre 1990.

58 Proposition modifiée de directive du Parlement européen et du Conseil concernant la protection des données à caractère personnel et de la vie privée dans le cadre des réseaux numériques de télécommunications, en particulier des réseaux numériques à intégration de services (RNIS) et des réseaux mobiles numériques, COM(94) 128 final-COD 288, Bruxelles, 13 juin 1994.

59 *Id.*, p. 3 : «Les dispositions générales en matière de protection des données à caractère personnel, telles que celles établies par la Convention du Conseil de l'Europe et celles qui le seront par la directive du Conseil .../.../CEE [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] offrent un cadre général, mais ne prévoient rien quant aux détails spécifiques nécessaires pour traiter tous les aspects concernés.» Voir note 44.

60 *Id.*, p. 3. «Les dispositions générales sur la protection des données à caractère personnel ne sont pas aptes à empêcher l'élaboration, à laquelle on assiste actuellement, de mesures législatives, réglementaires et administratives nationales sur le fonctionnement des futurs réseaux numériques. Les législations nationales en vigueur divergent considérablement aussi bien en ce qui concerne le contenu que la nature des instruments juridiques utilisés. Il en résulte une insécurité croissante dans la Communauté en matière de réseaux, de services et d'équipements de télécommunications. L'introduction de mesures législatives nationales divergentes dans ce secteur menace gravement la mise en place d'un marché intérieur des services et des équipements de télécommunications. Sans une directive, il serait impossible d'empêcher un émiettement du marché, des services et des équipements dans la Communauté.»

En terminant, il importe de signaler que le projet de directive générale ient bien évidemment des règles relatives au transfert à partir d'un État nbre de données personnelles vers les pays tiers. Nous nous proposons ntenant d'examiner cette importante question.

Le principe de l'équivalence

Nous savons déjà que la plupart des lois européennes de protection des nées personnelles contiennent des dispositions soumettant l'exportation ormations nominatives à des contrôles ou autorisations préalables. Ces ositifs s'avèrent nécessaires afin d'éviter le contournement des prescriptions onales par un transfert informationnel vers un pays dépourvu de toute slation ou doté d'une législation beaucoup plus laxiste que celle du pays portation. En général, le transfert sera permis si le pays importateur assure données personnelles transferées une protection de même nature que celle nt cours dans le pays exportateur. C'est là le principe de l'équivalence qu'on reformuler ainsi : un pays ne s'opposera pas à la transmission de données onnelles vers un pays tiers pourvu que ce dernier assure, dans son droit rne, une protection aux données personnelles qui équivaut en substance à existant dans le pays exportateur.

Le principe de l'équivalence est au coeur du dispositif réglementant les flux sfrontières de données à caractère personnel à l'article 17 des Lignes ctrices et à l'article 12 de la Convention européenne. Qu'on en juge :

> *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 les 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.

Quant à l'article 12 de la Convention européenne, il se lit ainsi :

> *2- 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 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 réglementation spécifique pour certaines catégories de données à caractère personnel ou de 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 équivalente.

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.

La grande difficulté tourne autour de ce qu'il faut entendre par protection équivalente. Cela signifie-t-il que le pays importateur doit être pourvu d'une législation en bonne et due forme en la matière? L'existence de règles protectrices éparses, non assemblées dans un instrument unique et cohérent, satisfait-elle au principe de l'équivalence? La question de l'autoréglementation se greffe à ces interrogations. En l'absence d'indications précises, il faut sans doute s'en remettre aux moyens de mise en oeuvre prévus par l'un et l'autre des instruments internationaux. Ainsi, pour ce qui est des Lignes directrices, nous savons que l'article 19 autorise les États, dans la mise en oeuvre du dispositif de la recommandation, à opter pour l'action législative ou la voie autoréglementaire. Il est donc permis de croire que l'équivalence, dans le cadre des Lignes directrices, peut se satisfaire de la voie autoréglementaire. En d'autres termes, le principe de l'équivalence semble satisfait bien que le pays importateur ne soit pas forcément doté d'une législation en bonne et due forme en matière de protection des données personnelles si, par ailleurs, son secteur public ou son secteur privé (dépendant de la destination des données) s'est pourvu d'un code de conduite reprenant les principes fondamentaux en matière de gestion de l'information personnelle que l'on retrouve dans les Lignes directrices[61].

L'article 4 de la Convention européenne apparaît plus strict. Il prévoit que chaque État prend, dans son *droit interne*, les mesures nécessaires pour donner effet aux principes de base de protection des données nominatives. L'expression «mesures nécessaires en droit interne» est ainsi présentée dans le Rapport explicatif :

En fonction du système juridique et constitutionnel du pays concerné, les «mesures nécessaires dans son droit interne» peuvent revêtir, outre la loi, différentes formes telles que règlements, directives administratives, etc. De telles mesures contraignantes 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

61 Voir pourtant note 43.

conduite professionnelle. Toutefois ces mesures volontaires ne suffisent pas par elles-mêmes pour donner suite à la Convention.[62]

Ainsi, un pays importateur ayant opté pour la seule voie autoréglementaire ne satisferait apparemment pas au principe de l'équivalence dans le cadre de la Convention européenne. Cela ne règle pas tout. Qu'en est-il du pays, comme les États-Unis, par exemple, dont l'approche est sectorielle[63], c'est-à-dire qui ne protège les données personnelles que dans certains secteurs d'activité (banques, crédit, etc.)? La question est ouverte.

Le projet de directive de la Commission européenne a le mérite de clarifier, dans une certaine mesure, la question de la protection équivalente. L'article 25(1) pose tout d'abord le principe selon lequel le transfert vers un pays tiers de données personnelles ne peut avoir lieu que si le pays tiers en cause assure un *niveau de protection adéquat*. On ne parle plus de protection équivalente mais bien de protection adéquate. Cette distinction sémantique aurait fait couler beaucoup d'encre si la Commission n'avait pas précisé, au paragraphe 2 du même article, ce qu'il fallait entendre par là :

2- Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données; en particulier sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, le pays d'origine et de destination finale, 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.

Voilà qui facilite la tâche de l'interprète[64]. L'article 26(2) permet également le transfert lorsqu'une entente contractuelle entre les parties impliquées assure la protection des données exportées :

Sans préjudice du paragraphe 1, un État membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère

---

62 Rapport explicatif, précité, note 30, p. 16.

63 Sur l'approche américaine, lire entre autres K. BENYEKHLEF, *op. cit.*, note 42.

64 Certains auteurs américains estiment que cette disposition du projet de directive de 1992 ne clarifie pas vraiment la situation pour ce qui est des exportations de données personnelles vers les États-Unis : «Although the introduction of this "all the circumstances" test does add clarity and flexibility, significant problems remain. First, it refers only to "legislative" provisions in the third party country. This would appear to exclude significant privacy guarantees in the United States, for example, based on common law, state and federal administrative regulations, and state and federal constitutions. Second, it will certainly be cumbersome to apply on a day-to-day basis. For example, a transfer from an EC member state to several branch offices of the same corporation in the United States might be proposed. Given the variations in individual state laws in the United States, a significant source of privacy protection, the outcome of the test might well be different for each state.» R.G. BOEHMER et T.S. PALMER, *loc. cit.*, note 47, 294.

personnel vers un pays tiers n'assurant pas un niveau de protection adéquat, 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'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées.

Dans ce cas, l'État membre doit informer la Commission et les autres États membres du projet d'autorisation. Un État membre ou la Commission peut s'opposer à un tel projet. Dans une telle occurence, le transfert est, en principe, annulé[65]. L'article 26 institue donc un régime d'exception qui n'est toutefois pas automatique. Il semble bien que chaque cas soit un cas d'espèce. Les termes liminaires de l'article 26(2) nous semblent confirmer cette interprétation. Par conséquent, la voie contractuelle ne saurait pallier *dans tous les cas de figure* l'absence d'un niveau de protection adéquat.

Une manière d'apprécier le caractère adéquat du niveau de protection est de tenir compte des engagements internationaux du pays tiers[66]. Ainsi, un pays ayant signé et ratifié la Convention européenne, sans être membre bien entendu de l'Union européenne, satisfait sans doute aux exigences communautaires. À cet égard, on peut noter que l'article 23 de la Convention européenne permet l'adhésion de pays non-membres du Conseil de l'Europe, comme le Canada, par exemple. Par ailleurs, les paragraphes 3 et 4 de l'article 25 instituent, en quelque sorte, un réseau d'information entre les pays membres et la Commission. Ainsi, les États membres s'informent mutuellement des cas dans lesquels ils estiment qu'un pays tiers n'assure pas un niveau de protection adéquat. De même, lorsque la Commission constate qu'un pays tiers n'assure pas un niveau de protection adéquat, les États membres doivent prendre les mesures nécessaires afin d'empêcher tout transfert vers le pays tiers en cause. Au surplus, la Commission peut engager des négociations avec un pays tiers en vue de remédier à cette absence de protection adéquate.

Le chapitre IV du projet de directive, intitulé «Transfert de données à caractère personnel vers des pays tiers», semble donc instituer un contrôle relativement sévère des transmissions de données nominatives. Chalton semble penser que les États membres et la Commission s'avéreront beaucoup plus souples en pratique :

Since in practice international business requires the regular and unrestricted flow of personal data between members of the Community and other countries, a rigid regime which requires consideration of all

---

65 Sur la voie contractuelle comme moyen de pallier l'absence de législation nationale dans le pays importateur, lire K. BENYEKHLEF, *op. cit.*, note 12, pp. 269-272 et pp. 347 et 348.

66 Position commune de 1995, précitée, note 11, art. 25(6).

prospective flows of personal data would be unworkable. Chapter IV may prove to be more in the nature of a political instrument for encouraging the adoption of European-style data protection laws in other countries, rather than a definitive set of rules for regulating the international flow of personal data to and from the Community.[67]

Chalton a peut-être raison. Toutefois, on voit mal les entreprises non péennes se contenter de cette opinion dans leurs opérations internationales. e fi du dispositif communautaire, sous prétexte qu'il s'agit, par hypothèse, exercice rhétorique, constitue sans doute une décision périlleuse pour une eprise. Par ailleurs, si la volonté de la Commission est en fait d'encourager ays non européens à adopter l'approche législative européenne en matière rotection des données personnelles, on voit mal comment l'Union péenne pourra y arriver sans user des pouvoirs que le chapitre IV du projet irective lui confère. Autrement, qu'est-ce qui pourra bien pousser les pays européens à aligner leur politique législative sur celle des États membres de on européenne?

L'APPLICABILITÉ DES NORMES INTERNATIONALES AUX NOUVELLES VOIES ÉLECTRONIQUES DE COMMUNICATION

Les nouvelles voies électroniques de communication

l n'est pas inutile de décrire sommairement les caractéristiques et ibilités des nouveaux environnements électroniques. Cet exercice devrait permettre de mieux déterminer et apprécier l'adéquation des normes nationales aux potentialités techniques de l'autoroute de l'information.

À ce propos, le réseau Internet illustre sans doute ces potentialités[68]. Celui-ci gure ce que devraient être les futures autoroutes électroniques. Les munications électroniques apparaissent novatrices en ce qu'elles lgament des techniques jusqu'ici isolées, comme le téléphone, la odistribution, la radiodiffusion, l'ordinateur, etc. En d'autres termes, les elles voies de communication permettent la transmission de la voix, du son, mage et de données (textes, graphiques, etc.). La communication n'est plus rectionnelle, comme pour la câblodistribution, ou bidirectionnelle, comme le téléphone, mais plutôt multidirectionnelle et interactive. L'usager n'est

---

imon CHALTON, «A Privacy Law for Europe : Back to the Data Protection Drawing Board», (1993) 9 *omputer L. & Prac.* 4, 6 et 7.

n estime qu'il existe entre 8,9 à 17,8 millions d'utilisateurs du réseau Internet, ce qui en fait évidemment le us grand réseau électronique du monde. Sur le réseau Internet, lire entre autres : J.J. QUATERMAN et S. arl MITCHELL, *The Internet Connection. System Connectivity and Configuration*, Reading, 1994, p. 5.

plus un spectateur passif; il peut devenir un acteur en participant à des échanges ou discussions électroniques, en créant des fichiers accessibles (FTP, WWW[69]), en établissant son propre babillard électronique, en ayant accès à des sources documentaires, visuelles ou sonores inédites ou autrement difficilement accessibles, etc.

Au surplus, l'usager peut nouer des rapports commerciaux avec diverses entreprises présentes sur l'autoroute de l'information. L'achat de biens et services peut emprunter les canaux électroniques. L'usager pourra réaliser des opérations bancaires ou boursières, acheter certains produits, commander des films ou des disques, jouer à des jeux électroniques, réserver des billets de théâtre ou d'avion, des chambres d'hôtel, lire des magazines ou des journaux, etc. Soulignons, au passage, que les transactions dématérialisées soulèvent, outre la question de la protection de la vie privée, de nombreuses interrogations au plan juridique[70]. Le secteur public offre également à l'usager une multiplicité de services. L'accès aux banques de données gouvernementales, la déclaration d'impôt sous forme électronique, l'information aux prestataires de programmes sociaux, la formation, etc. constituent des exemples de l'activité de la puissance publique sur l'autoroute de l'information.

L'observateur peut alors remarquer qu'une constellation de rapports, juridiques ou non, se nouent dans le cyberespace. Cette variété de rapports dans un univers dématérialisé dont la configuration technique permet et, dans certains cas, oblige l'identification de l'usager, de même que le caractère quasi public des opérations commerciales, ludiques ou publiques — riches d'informations personnelles — auxquelles se livre l'usager ne peuvent manquer de démultiplier les occasions d'atteintes au droit à la vie privée.

Les fonctionnalités de l'autoroute de l'information sont diverses. On peut tenter de les grouper par catégorie. Cette classification n'est pas toujours étanche et est, sans doute, appelée à se modifier et à évoluer par l'intégration notamment de nouvelles fonctionnalités, résultat du développement technologique. Cinq fonctionnalités peuvent être identifiées :

- Commerciales;
- Culturelles et ludiques;
- Publiques ou gouvernementales;
- Académiques et informatives;

---

69 FTP : File Transfer Protocol; WWW : World Wide Web.

70 Lire Karim BENYEKHLEF, «Les transactions dématérialisées sur les voies électroniques : panorama des questions juridiques», dans Daniel POULIN, Pierre TRUDEL et Ejan MACKAAY, (dir.), *Les autoroutes électroniques : usages, droit et promesses*, Cowansville, Éditions Yvon Blais, 1995, p.115.

- Communicationnelles.

Les trois premières fonctionnalités se passent d'explication. La quatrième se ıporte aux échanges d'informations entre universitaires, à la publication de ues électroniques, à la tenue de séminaires électroniques ou de listes de cussions (babillards électroniques) sur des sujets d'intérêt divers. De même, :onsultation de banques de données, l'accès à des sites de documentation ou ıformations de type journalistique s'intègrent dans cette catégorie. Quant aux ctionnalités communicationnelles, nous faisons simplement référence au ırrier électronique (E-Mail[71]), c'est-à-dire à la possibilité de correspondre, par :ruchement d'un réseau électronique de communication, avec des usagers ɜl que soit leur lieu de résidence.

Il faut bien comprendre qu'un réseau comme l'Internet, offre, en général, tes ces fonctionnalités. Celles-ci coexistent dans le cyberespace. L'usager ıse de l'une à l'autre sans difficulté. Évidemment, ces services ne sont pas s gratuits. Certaines fonctionnalités, comme la commande de films ou de ques, par exemple, supposent un déboursé qui s'additionne aux frais ɔonnement au réseau[72]. Cette classification a un objet juridique. Elle permet mieux cerner les enjeux afférents, notamment, à la protection du droit à la vie ée. En effet, l'interprète aura deviné que les potentialités d'atteintes au droit à ie privée sont plus grandes dans le cas des opérations commerciales que ıs celui des échanges académiques. De même, la consultation de sites ıformations de type journalistique soulève, en général, moins de risque teinte à la vie privée que la commande de biens et services. Ce n'est pas tant hat, dans ce dernier cas de figure, qui constitue un danger pour la vie privée ı la possibilité pour le serveur commercial de dresser un profil des habitudes consommation de l'usager (données transactionnelles[73]). Ce profil devient ı précieuse source de données personnelles qui peut être vendue à d'autres reprises entraînant par là, bien souvent, un détournement des finalités mières de collecte[74].

Electronic Mail.

Sur les environnements réseaux, lire entre autres : Ruel Torres HERNANDEZ, «ECPA and Online Computer Privacy», [1988] 41 *Fed. Comm. L.J.* 17, 19-23 et Pierre TRUDEL (avec la collaboration de R. GÉRIN-LAJOIE), «La protection des droits et des valeurs dans la gestion des réseaux ouverts», dans *Les autoroutes électroniques : usages, droit et promesses*, *op. cit.*, note 70, p. 299 et suiv.

Lire K. BENYEKHLEF, *op. cit.*, note 12, pp. 358-364.

«La collecte de données transactionnelles deviendra beaucoup plus facile dans un monde informatisé et maillé. Les grands progrès réalisés quant à la capacité des ordinateurs, la liaison d'un grand nombre d'entreprises par des systèmes de paiement électronique, et le maillage complet des bases de données sur les ventes et les commandes ont révolutionné la relation entre les consommateurs et les producteurs de biens et services. [...] L'autoroute de l'information pourrait grandement faciliter l'établissement du profil des personnes en fonction de leurs besoins, de leur style de vie ou de leurs choix d'achats. Cela pourrait avoir des répercussions malencontreuses si ces profils servaient à empêcher les personnes, et ce, à leur insu, de saisir

Ces fonctionnalités nous permettent de mieux saisir concrètement les potentialités opérationnelles de l'autoroute de l'information. Elles illustrent la nature de l'information circulant sur les réseaux électroniques. Il s'agit maintenant de déterminer l'adéquation des normes internationales de protection des données personnelles[75] aux nouveaux environnements électroniques de communication.

B. La vie privée et la protection des données personnelles

La variété des fonctionnalités de l'autoroute de l'information nous permet d'apprécier la diversité et l'inégale importance des possibles atteintes au droit à la vie privée. À ce propos, il convient de distinguer entre le droit à la vie privée et la protection des données personnelles. La première notion englobe la seconde. Autrement dit, la protection des données personnelles n'est qu'un sous-ensemble du droit à la vie privée. La protection des données nominatives représente l'aspect informationnel du droit à la vie privée[76]. Les principes fondamentaux en matière de gestion de l'information personnelle traduisent en termes pratiques les préoccupations afférentes aux dimensions informationnelles du droit à la vie privée.

Nous savons que ces principes établissent des procédures et des pratiques quant à la gestion de l'information nominative (*fair information practices*). Ces procédures et pratiques ont, entre autres, pour objet d'assurer à la personne fichée un certain contrôle sur les données la concernant. Ce *corpus* normatif s'applique au premier chef aux organismes publics et aux entreprises commerciales, c'est-à-dire aux organes qui détiennent une masse importante d'informations personnelles. En effet, il est bien clair que les dangers posés à la vie privée sont le fait de ceux qui font une grande utilisation des données nominatives dans l'accomplissement de leurs missions publiques et de leurs tâches commerciales. Par conséquent, les normes internationales en matière de protection des données personnelles s'appliquent, de prime abord, aux organismes publics et aux entreprises commerciales oeuvrant sur l'autoroute de l'information. Les données collectées par ces organes sur l'autoroute de l'information sont, en principe, soumises à ce *corpus* normatif.

---

les occasions qui s'offrent à elles. Le stockage dans des bases de données et les rapprochements des renseignements permettraient de prendre des décisions sur des particuliers, ce qui modifierait les conditions d'accès à divers produits, services et perspectives d'emploi.» Comité consultatif-Vie privée, *op. cit.*, note 1, p. 6.

75 Cet exercice de détermination s'applique également aux normes nationales, c'est-à-dire aux diverses lois nationales de protection des renseignements personnels, puisque les principes fondamentaux en matière de gestion de l'information personnelle se retrouvent dans les deux types d'instruments.

76 Sur ce sujet, lire K. BENYEKHLEF, *loc. cit.*, note 9, 38-61. Lire également l'arrêt *R.* c. *Dyment*, [1988] 2 R.C.S. 417, 429 et 430.

Toutefois, ces organes ne sont pas les seuls acteurs du théâtre télématique. a également les usagers. Or les principes fondamentaux en matière de tion de l'information personnelle ne s'appliquent pas aux individus dans ercice de leurs activités privées[77]. Il est donc clair que ces principes ne sont applicables à l'interception par un tiers du courrier électronique d'un sateur. Ces principes ne couvrent pas davantage les situations d'accès non orisé à des sites pouvant contenir des données personnelles et la émination de ces données sur le réseau. Certaines lois pourvoient parfois à type de situation. Quoi qu'il en soit, ces situations mettent également en se le droit à la vie privée ou, à tout le moins, un élément de celui-ci que stitue le principe de confidentialité.

Par conséquent, la protection de la vie privée sur les nouvelles voies ctroniques de communication ne se limite pas aux simples questions rentes aux principes fondamentaux en matière de gestion de l'information sonnelle. Ainsi, la possibilité d'échanger des messages électroniques sans e l'objet d'une interception par un tiers ou même par l'État ou sans faire l'objet ne surveillance par son employeur[78], par exemple, s'inscrit dans une blématique certes associée au droit à la vie privée, mais tout de même incte de celle relative à la gestion de l'information personnelle telle envisagée par les normes internationales examinées en première partie. Il ne git pas de déplorer l'inapplicabilité de ces normes à ces situations. Celles-ci nt pas été, en effet, élaborées pour répondre à ces interrogations. D'autres mes doivent alors être développées ou adaptées pour corriger ces atteintes droit à la vie privée. Il faut donc bien comprendre que les principes damentaux en matière de gestion de l'information personnelle n'ont pas ation à régir toutes les situations soulevant le problème du droit à la vie ée dans le cyberespace. Par ailleurs, il nous semble que les atteintes entielles les plus graves et les plus nombreuses au droit à la vie privée sont vertes, de prime abord, par ces principes fondamentaux. En effet, les anismes publics et les entreprises commerciales sont, sans aucun doute, les cipaux détenteurs de renseignements personnels. Cette formidable umulation de données constitue, en soi, une menace beaucoup plus ortante au droit à la vie privée que les exactions de quelques individus.

Il s'agit maintenant de se demander si ces principes fondamentaux sont en quation avec le nouvel environnement électronique mis en place sur oroute de l'information. En effet, comme le souligne le professeur Poullet, réglementations «ont combattu le risque relatif aux traitements d'informations

---

Lire, par exemple, l'article 3(2) du projet de directive de 1992 tel qu'amendé par la Position commune de 1995 qui énonce : «La présente directive ne s'applique pas au traitement de données à caractère personnel [...] effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.»

Lire, par exemple, Steven WINTERS, «The New Privacy Interest : Electronic Mail in the Workplace», (1993) 8 *High Tech. L.J.* 197.

recueillies *a priori* pour les centres de traitement»[79]. Or, poursuit-il, «les risques dénoncés ici concernent des données nées *a posteriori* par l'utilisation du service lui-même»[80]. Deux concepts fondamentaux sont ici mis en cause : les définitions des expressions «données à caractère personnel» et «fichier automatisé». Ainsi, les données personnelles sont définies de même manière dans la Convention européenne et les Lignes directrices de l'OCDE : «toute information concernant une personne physique identifiée ou identifiable (personne concernée).» Cette définition couvre-t-elle les nouvelles techniques de collecte, d'enregistrement et de transmission des images, des sons et des voix? Elle nous semble suffisamment large pour englober ces nouvelles applications techniques[81]. La définition du projet de directive de la Commission européenne est encore plus englobante :

> *Données à caractère personnel : toute information concernant une personne physique identifiée ou identifiable («personne concernée»); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.*[82]

Quant à la notion de «fichier automatisé», elle s'entend, selon l'article 2b) de la Convention européenne, de tout ensemble d'informations faisant l'objet d'un traitement automatisé[83]. On ne retrouve pas de disposition similaire dans les Lignes directrices. Celles-ci ne sont pas en effet limitées au traitement automatisé. Toutefois, le professeur Bing estime que, bien que les Lignes directrices ne fassent pas référence explicitement à la technique dans la définition de leur champ d'application, il n'en demeure pas moins qu'implicitement elles reposent sur une gestion ordonnée et centralisée de l'information personnelle au même titre que la Convention européenne[84]. Or, la notion de fichier, et avec elle l'idée d'une gestion ordonnée et centralisée, est battue en brèche par les nouvelles technologies. L'idée selon laquelle des

---

79 Yves POULLET, «Le marché de l'information. Aspects contractuels : les clauses de confidentialité», Texte inédit, Namur, p. 42.

80 *Id.*, p. 42.

81 CONSEIL DE L'EUROPE, *Les nouvelles technologies : un défi pour la protection de la vie privée?* (Étude préparée par le Comité d'experts sur la protection des données, CJ-PD), Strasbourg, Conseil de l'Europe, 1989, pp. 34 et 35 (ci-après cité : «Nouvelles technologies»).

82 Position commune de 1995, précitée, note 11, art. 2a).

83 L'expression «traitement automatisé» est définie à l'article 2c) de la Convention européenne : «Traitement automatisé s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion.»

84 Jon BING, «Impact of Developing Information Technology on Data Protection Legislation», Paris, OCDE, DSTI/ICCP(86)5, Février 1986, pp.13 et 14.

nnées personnelles sont stockées et ordonnancées dans un fichier, localisé en endroit bien précis, vole en éclat. La notion de fichier n'est pas adaptée. Les nnées sont aujourd'hui éparpillées et ne s'intègrent donc plus dans un semble ordonnancé et unique (fichier)[85]. Or, la notion traditionnelle de fichier ondait aux exigences de transparence et d'accessibilité aisée aux données la personne concernée. Le Conseil de l'Europe propose alors le concept de hier logique» afin de pallier ces difficultés de définition. La délocalisation et arpillement des données ne constitueraient pas des obstacles à la création n fichier virtuel. En d'autres mots, il est possible, par le couplage notamment, réunir des données dispersées en un ensemble unique et ordonnancé. Nous mmes alors en présence d'un fichier potentiel; celui-ci se matérialisant à la te de diverses opérations informatiques[86].

Le projet de directive de la Commission européenne, tel qu'amendé par la sition commune de 1995, répond à ces développements technologiques en andonnant la notion de «fichier automatisé». L'application de la directive n'est nc pas tributaire de l'existence d'un fichier structuré pour ce qui est du tement automatisé :

> *L'alinéa 1er de la proposition modifiée concilie les points de vue de ceux qui souhaitent se référer en matière informatique au seul concept «de traitement automatisé» (puisqu'un traitement automatisé n'implique pas nécessairement l'existence d'un fichier) et de ceux qui redoutent de voir la directive étendue à toutes les données même non structurées figurant sur support papier.*
>
> *Par conséquent, la proposition modifiée adopte des critères distincts pour définir le champ d'application de la directive, selon que les données font ou non l'objet d'un traitement automatisé : elle n'est applicable au traitement non automatisé de données que si ces données sont contenues dans un fichier; en revanche, en matière informatique, la définition dépasse la notion de fichier, et la directive s'applique à tout traitement automatisé de données même si ces données ne sont pas contenues dans un fichier.*

«Il se peut, toutefois, que la notion de fichier, telle qu'utilisée dans la Convention, suggère un enregistrement et un traitement centralisés, ce qui ne correspond plus tout à fait à la nouvelle réalité de l'informatique répartie et des réseaux qui permettent aux données de se disperser tout en pouvant être reliées à volonté à travers la possibilité d'un dialogue d'ordinateur à ordinateur ou de terminal à ordinateur.» Nouvelles technologies, *op. cit.*, note 81, p. 35.

«Il paraîtrait nécessaire d'examiner la nécessité de pouvoir établir l'existence de ce qu'on pourrait appeler "un fichier logique" permettant de situer en dernier ressort, à travers des méthodes d'extraction, toutes les données dispersées dans le réseau à la suite d'un traitement et d'un enregistrement légitimes au sein d'une organisation donnée. De même, la transparence n'est plus assurée par le simple fait de connaître l'existence d'un fichier. Il serait donc souhaitable de rendre plus claire l'influence du réseau sur les opérations de traitement des données.» *Id.*, p. 36.

> *Ainsi, sont concernées les données à caractère personnel structurées soit par leur organisation dans un fichier manuel, soit au moyen d'un traitement automatisé.*[87]

On remarque que le projet de directive apparaît plus en phase avec l'évolution connue par les nouvelles voies électroniques de communication. Il s'agit évidemment d'un document plus récent. Cela ne signifie pas que les Lignes directrices ou la Convention européenne constituent des instruments normatifs dépassés. La généralité de leurs termes et le développement du concept de «fichier logique» permettent sans doute à ceux-ci de demeurer dans la course. Par ailleurs, en ce qui concerne les principes fondamentaux proprement dits, ceux-ci nous semblent en mesure de répondre aux défis posés par le développement de l'autoroute de l'information. L'essence de ces principes demeure actuelle. Le Conseil de l'Europe note justement :

> *Il convient tout d'abord de préciser que les principes de la Convention ont un caractère général. Comme les garanties constitutionnelles ou internationales en matière de droits de l'homme, les principes pour la protection des données sont énoncés en des termes permettant une adaptation aux situations en évolution.*[88]

La comparaison avec des dispositions constitutionnelles nous semble tout à fait juste. Les principes fondamentaux constituent finalement des énoncés philosophiques qui circonscrivent les enjeux en imposant des limitations. Ils sont donc appelés, à l'instar des garanties constitutionnelles, à évoluer et à s'adapter aux circonstances nouvelles. On doit reconnaître néanmoins que le développement de règles spécifiques et/ou complémentaires peut s'avérer nécessaire afin de préciser, dans un cadre opérationnel et pratique, l'exercice des principes fondamentaux. On peut penser ici notamment aux multiples recommandations du Conseil de l'Europe[89] ou au projet de directive sectorielle concernant les télécommunications. En effet, la variété fonctionnelle de l'autoroute de l'information oblige sans doute l'interprète à préciser la teneur générale des principes fondamentaux afin de faciliter leur mise en oeuvre. De

---

87 Projet de directive de 1992, précité, note 10, p. 12. L'interprète note que la définition de l'expression «traitement de données à caractère personnel» est identique dans le projet de directive de 1992 et dans la Position commune de 1995. Mei ajoute sur ce point : «The Amended Proposal protects individual privacy by regulating the use of "personal data files", which include any set of data organized to allow structured access and searches for information on individuals. However, the scope of protection varies depending on whether or not the data is processed by automatic means. For the automated processing of data, the extent of protection does not depend on the actual presence of a "file". The file requirement only applies when the information is to be processed manually. Any set of structured records, including paper records, fits within this provision of the directive. In effect, the index card record system of a small business would be subject to the same regulations as the large computerized databases of a major corporation.» P. MEI, *loc. cit.*, note 49, 311.

88 Nouvelles technologies, *op. cit.*, note 81, pp. 44 et 45.

89 Voir note 44.

s, le caractère résolument international des nouvelles voies électroniques de nmunication réclame l'élaboration de normes propres à faciliter la circulation l'information et à assurer une protection uniforme des données personnelles. dépit des efforts de l'OCDE, du Conseil de l'Europe et de la Commission opéenne, le droit de la protection des données à caractère personnel est loin re uniforme. L'absence au Canada, par exemple, de tout instrument général ant à protéger les renseignements personnels dans le secteur privé illustre re propos[90]. La même remarque peut être formulée pour ce qui est des États-s[91]. Le problème de l'équivalence des protections se pose donc avec acuité.

Ce problème apparaît d'autant plus délicat que l'intangibilité du cyberespace d difficile l'application des règles de protection des données personnelles. rement dit, comment assurer une application effective de ces règles lorsque ager est domicilié à Montréal et que le serveur, une entreprise commerciale, a place d'affaires à la Nouvelle-Orléans ou à Hong Kong? Quelle autorité urera l'application et la sanction de ces règles? Comment déterminer la ation de ces règles dans un environnement aussi volatil et insaisissable? me si, par hypothèse, toutes les nations étaient dotées d'une loi de protection données personnelles, le problème de l'intangibilité et de la délocalisation tinuerait à se poser : quelle loi appliquer? quelle autorité est compétente? nment assurer l'exercice des droits d'accès et de correction de la personne ncernée? comment cette dernière peut-elle déterminer l'existence d'un tement automatisé la concernant? comment concilier les différences matives qui ne manqueront pas d'affliger les instruments pertinents[92]? Ces estions ne constituent que la pointe de l'iceberg.

L'interprète constate alors qu'au-delà de la question de l'applicabilité stricte normes internationales au champ de l'autoroute de l'information, c'est la estion de l'application pratique et opérationnelle de ces normes qui soulève le s de difficultés. Une coopération internationale apparaît dès lors nécessaire, re inéluctable, si l'on entend assurer vraiment la protection de la vie privée usagers de l'autoroute de l'information[93]. En attendant la concrétisation ne telle coopération, certains mécanismes peuvent, avec plus ou moins de nheur, atténuer les difficultés inhérentes à l'intangibilité du cyberespace. Ces canismes constituent, en plus, une voie complémentaire de protection des

---

Le Québec constitue une exception : voir la *Loi sur la protection des renseignements personnels dans le secteur privé*, L.Q. 1993, c. 17.

Lire Joel R. REIDENBERG, «Setting Standards for Fair Information Practice in the U.S. Private Sector», (1995) 80 *Iowa L.Rev.* 497.

Pensons, par exemple, au régime particulier que connaissent les données sensibles dans beaucoup de pays européens; régime inconnu dans les instruments législatifs nord-américains.

Sur les modalités de coopération internationale, lire les articles 13 à 17 de la Convention européenne, précitée, note 7 et les articles 28 à 30 de la Position commune de 1995, précitée, note 11.

données personnelles. En d'autres termes, même en présence d'une coopération internationale, il nous semble que ces mécanismes pourraient permettre une protection complémentaire de la vie privée. Ils s'ajouteraient au *corpus* général mis en place au plan international. Nous pensons ici, entre autres, à l'autoréglementation et au principe de proximité, au développement d'un standard de type ISO 9000 et à la voie contractuelle.

Le développement de normes autoréglementaires par des associations d'entreprises, des réseaux de communication ou même des usagers ne saurait être négligé. Bien que la voie autoréglementaire puisse apparaître déficiente au regard du contrôle et de la sanction des normes qu'elle institue[94], elle peut constituer une voie complémentaire — et non pas exclusive[95] — intéressante en ce qu'elle traduit les principes fondamentaux dans l'industrie ou le secteur concerné. En d'autres mots, elle particularise les principes fondamentaux en tenant compte des spécificités du secteur visé. Il doit donc y avoir *adéquation* entre les normes volontaires et les spécificités du secteur pour lequel un code de conduite est élaboré. À ce propos, la mise en place de codes de conduite communautaires, envisagée par l'article 27 du projet de directive de 1992, tel qu'amendé par la Position commune de 1995, ne peut que contribuer à faciliter la protection transnationale des données nominatives. Ces codes communautaires peuvent avoir un effet d'entraînement et obliger les entreprises non européennes à adhérer à leur contenu. De tels instruments, conçus sous la supervision et avec la collaboration d'autorités publiques[96], peuvent certes contribuer à une protection plus efficace de la vie privée informationnelle.

On peut aller plus loin sur la voie autoréglementaire. Les auteurs des normes autoréglementaires sont proches de l'action. Il sont souvent les mieux placés pour répondre efficacement aux problèmes soulevés dans les univers dématérialisés. Ces auteurs constituent ce qu'on pourrait appeler des agents de proximité. Qui sont-ils? Ces agents peuvent être les gestionnaires de réseaux, les transporteurs, les fournisseurs ou producteurs d'informations, les utilisateurs, etc. On pourrait donc leur confier la tâche d'élaborer des normes particulières propres à assurer la mise en oeuvre des normes générales qu'on retrouverait dans la loi nationale ou dans un accord international. Les agents de proximité compléteraient ainsi l'action normative entreprise par les autorités publiques. Mais au-delà de l'élaboration et de la conception de normes sectorielles ou

---

94 Sur les conditions à respecter pour qu'un code de conduite constitue un véritable instrument de régulation des données personnelles, lire K. BENYEKHLEF, *op. cit.*, note 42, pp. 233-239. Pour une approche critique de la voie autoréglementaire, lire Pauline ROY, «La Loi sur la protection des renseignements personnels dans le secteur privé : un acte de foi dans les vertus de l'autoréglementation» , dans René CÔTÉ et René LAPERRIÈRE (dir.), *Vie privée sous surveillance : la protection des renseignements personnels en droit québécois et comparé*, Cowansville, Éditions Yvon Blais, 1994, p. 83.

95 Lire note 43.

96 Lire l'article 27(3) de la Position commune de 1995, précitée, note 11.

articulières, on pourrait également leur confier la tâche de mettre en oeuvre ces ormes. En d'autres termes, les agents de proximité devraient assurer ipplication des normes élaborées. C'est là, nous semble-t-il, une des seules anières de répondre adéquatement à la délocalisation et à l'intangibilité de nformation circulant dans le cyberespace. Puisque l'information est délocalisée, convient également de délocaliser les tâches d'élaboration *et* de mise en euvre ou d'application des normes. Autrement, les autorités publiques ne ourront jamais assurer le respect des règles qu'elles auront édictées.

Le principe de proximité nous semble une solution concrète susceptible de ciliter la normalisation des inforoutes. Le caractère international de celles-ci oppose, en effet, à toute solution normative uniquement globale ou générale. ne telle approche se heurte à d'immenses difficultés pratiques d'application. Le incipe de proximité a pour avantage de localiser ou de régionaliser, en quelque orte, la résolution des problèmes ou des conflits suscités par un environnement ectronique transnational. En fait, ce principe est le pendant, d'une certaine anière, du principe de subsidiarité que l'on retrouve en droit européen[97]. Selon principe de subsidiarité, il convient de laisser aux instances nationales ou cales le soin de régler les difficultés qui ne peuvent être raisonnablement aitées au plan communautaire. Il importe de rappeler que l'action des agents de oximité doit s'inscrire dans le cadre normatif général mis de l'avant par le gislateur national ou par un accord international. Autrement dit, les normes onçues et appliquées par les agents de proximité tirent leur légitimité et leur éité du fait qu'elles complètent ou explicitent le cadre normatif général. Bien videmment, il s'agit de prévoir des mécanismes garantissant l'indépendance es agents de proximité afin d'éviter leur inféodation à des intérêts clientélaires» ou financiers[98]. Par ailleurs, on remarque que le principe de oximité peut s'appliquer à d'autres domaines du droit que celui de la protection es données personnelles (droit d'auteur, transactions dématérialisées, exercice e la liberté d'expression, etc.).

Voir, entre autres, Commission européenne, «Le principe de subsidiarité», (1992) 28 *Rev. trim. dr. europ.* 731, 732 : «Le principe de subsidiarité appliqué au domaine institutionnel part d'une idée simple : un État ou une Fédération d'États dispose dans l'intérêt commun des seules compétences que les personnes, les familles, les entreprises et les collectivités locales ou régionales ne peuvent assumer isolément. Ce principe de bon sens doit garantir que les décisions sont prises le plus près possible des citoyens par la *limitation des actions menées par les échelons les plus élevés* du corps politique.» ; «Le principe de subsidiarité», (1992) *Bull.CE 10-1992*, 122.

À cet égard, la Loi allemande de protection des données personnelles du 20 décembre 1990 (Federal Law Gazette 1990 I 2954) prévoit, à son article 36, la nomination dans l'entreprise d'un employé responsable de la protection des données nominatives. Cet employé doit donc s'assurer que les prescriptions de la loi sont respectées (article 37). La loi énonce que l'employé ne saurait être sanctionné en raison de l'exécution de ces tâches. La loi garantit donc l'indépendance de l'employé chargé d'assurer sa mise en oeuvre. Voilà un modèle intéressant qui pourrait être pris en compte et adapté à la situation des agents de proximité ayant pour fonction d'assurer la mise en oeuvre et le respect des normes particulières et générales.

L'Association canadienne des standards (ACS) est en train d'élabore code de conduite standard qui serait applicable, en principe, à l'ensembl secteur privé. L'ACS travaille en collaboration avec des représentants du se privé, d'associations de consommateurs et des autorités publiques. L'origi de l'approche de l'ACS est qu'elle se propose d'intégrer les normes afféren la protection des données personnelles aux standards de gestion connaissent les entreprises (*Quality Management*). Autrement dit, les norme protection des données personnelles constitueraient un standard de gestio même titre que le respect des règles comptables reconnues dans l'élabor des états financiers. Un audit pourrait donc être effectué et compren l'analyse des modalités de gestion de l'information personnelle au regar standard pertinent. Cette initiative canadienne pourrait être appliquée au international (ISO 9000) et faire de la protection des données personnelle standard de gestion internationalement reconnu et uniforme. Ceci contribu sans aucun doute, à atténuer les problèmes inhérents à l'intangibilit cyberespace[99].

Finalement, la voie contractuelle peut constituer une voie complémentai de substitution. Toutefois, elle comporte certains inconvénients qui en dimin sérieusement l'attrait. En 1992, le Conseil de l'Europe, conjointement av Commission européenne et la Chambre de commerce internationale, a entr la rédaction d'un contrat-type applicable aux flux transfrontières de donné caractère personnel[100]. L'objet essentiel d'un tel contrat est de facilit circulation internationale de données nominatives en assurant un degr protection aux données, ainsi transmises, équivalent, en principe, à celui du exportateur. Cette équivalence est, bien entendu, la résultante des exigen cet effet que l'on retrouve dans la plupart des lois européennes et dan instruments internationaux[101]. Ainsi plutôt que de bloquer l'exportatio données personnelles vers un pays dépourvu de toute législation en la ma l'agence de protection des données personnelles va permettre cette export à condition que les parties à la transmission s'engagent à respecter, par contractuelle, les principes fondamentaux édictés dans la loi du d'exportation[102].

---

99 Il ne s'agit là cependant que d'un projet : discussions tenues lors d'un séminaire électronique inter organisé par l'auteur sur l'Internet (INFLOWS-L@cc.umontreal.ca) portant sur les *Rules go international flows of information*, Octobre 94-Mars 95.

100 Conseil de l'Europe, *Contrat-type visant à assurer une protection équivalente des données dans le ca flux transfrontières de données et Rapport explicatif*, Strasbourg, T-PD (92) 7 révisé, 2 novembre 1 peut aussi retrouver une copie du contrat-type en anglais à : NOTE, «Transborder Date Flow Model C Agreed», (1992) *Privacy Laws & Business* 13.

101 Voir point B. Le principe de l'équivalence, p. 84.

102 Lire l'article 26 de la Position commune de 1995, précitée, note 11.

Les rédacteurs du contrat-type reconaissent néanmoins le fait que la voie contractuelle ne saurait constituer une voie exclusive et définitive :

> *The conclusions to the 27-28 March 1990 EC/Council of Europe conference stated : «While emphasizing that the law of contract could never replace the need to legislate for data protection, contractual techniques could nevertheless be used as a sort of palliative or complement to the legal framework for data protection and transborder data flow».*[103]

Cette solution nous apparaît, en effet, complémentaire. Elle ne saurait remplacer la nécessité de normes plus contraignantes et surtout, plus concrètes en matière de protection des renseignements nominatifs[104]. Au surplus, la voie contractuelle n'apparaît possible que si le pays exportateur est doté d'une législation en la matière. En effet, la solution contractuelle a été élaborée dans le but d'assurer au pays exportateur le respect de ses dispositions législatives et ainsi, garantir l'équivalence. En outre, cette solution suppose, dans ses applications, l'existence d'une agence de protection des renseignements personnels dont la mission est d'analyser les clauses contractuelles pertinentes et de contrôler la conformité de celles-ci aux dispositions législatives. Par conséquent, la voie contractuelle ne présente que peu d'attrait pour policer les échanges d'informations personnelles entre le Canada et les États-Unis, puisque ces deux pays sont dépourvus de toute loi générale de protection de l'information personnelle dans le secteur privé. En outre, en raison de la doctrine de l'effet relatif des contrats, la personne fichée ne pourrait se prévaloir du contrat conclu entre les parties à la transmission de données personnelles[105].

Ces voies alternatives ou complémentaires ne sont pas dénuées d'intérêt. Il nous semble qu'elles peuvent constituer, avec d'autres[106], une technique souple et adaptable de régulation du cyberespace. Il est, en effet, trop tôt encore pour entrevoir une modalité unique et exclusive de réglementation des échanges informationnels sur les nouvelles voies électroniques de communication[107].

---

103 NOTE, *loc. cit.*, note 100, 13.

104 Pour une analyse critique du contrat-type, lire K. BENYEKHLEF, *op. cit.*, note 42, pp. 271-283.

105 Lire J.R. REIDENBERG, *loc. cit.*, note 91, 545-548. Dans son article, le professeur Reidenberg propose un modèle contractuel original susceptible d'éviter les difficultés que l'interprète retrouve dans le contrat-type élaboré par le Conseil de l'Europe. Cette proposition ne règle cependant pas le problème majeur lié à l'absence de législation dans le pays exportateur. Il est vrai que ce modèle contractuel a pour vocation de régir les échanges d'informations personnelles entre les pays européens, dotés d'une loi générale de protection des données personnelles, et les pays dépourvus d'une législation générale ou globale en la matière, comme les États-Unis.

106 Comité-consultatif-Vie privée, *op. cit.*, note 1, pp.15-18. Lire aussi Marc ROTENBERG, «Electronic Privacy Legislation in the United States», (1994) *The International Privacy Bulletin*, 15 et 16.

107 Sur cette question, lire P. TRUDEL, *loc. cit.*, note 72.

CONCLUSION

La protection des données à caractère personnel sur l'autorout
l'information soulève d'importantes difficultés. Les principes fondamentau
matière de gestion de l'information personnelle, consacrés dans les docun
internationaux sont, de prime abord, en mesure d'assurer la protection de
privée sur les nouvelles voies de communication. Mais, cette appréciatio
théorique. En effet, l'intangibilité du cyberespace et la délocalisation des ac
télématiques rendent ces principes difficilement applicables au plan pratiqu
coopération internationale semble donc primordiale. Suffira-t-elle? Il nous se
que le développement de voies complémentaires, propres à affiner les prin
fondamentaux et à assurer leur traduction pratique, est nécessaire. Cette v
des approches normatives semble, pour le moment, le seul moyen effica
répondre aux nouveaux défis posés par la révolution des communica
électroniques.