Sous la direction de
Damien Delhase et Dominique Verpoorten

# Quels paysages juridiques et socio-éducatifs pour les autoroutes de l'information?

Préface de Michel Lebrun
Introduction par Benoît Lips

"Technologies et éducation":
la parole aux universités francophones

CONTRIBUTIONS QUÉBÉCOISES

EDIFIE L.L.N.

# Technologies de l'information et société: un couple entre doutes et espoirs

Réseaux de pédophilie utilisant le Net pour démarcher des clients, livres interdits et mis à la disposition du monde entier sur l'Internet, escroqueries sur le télé-achat, atteintes à la vie privée rendues permises par les technologies télématiques, problématique complexe des droits d'auteurs : incontestablement, les technologies de l'information posent questions.

Nouvelles formes de convivialité et de participation, le bout du monde accessible par écran interposé, cédéroms éducatifs qui ouvrent de nouvelles pistes d'acquisition de savoirs, réconciliation de la pensée digitale et de la pensée analogique, cognition distribuée, arbres de connaissances, télé-enseignement, outils d'aide aux personnes handicapées : incontestablement, les technologies de l'information suscitent des espoirs.

Cette oscillation, entre défis et dangers, indique bien que les citoyens prennent conscience des potentialités ouvertes par les technologies en matière d'organisation communicationnelle, sociale et cognitive, potentialités qui diffèrent de celles qu'ont véhiculées les médiums typiques des sociétés orales ou scribales.

C'est à la description de ce projet et du changement social qu'il implique que souhaite contribuer cet ouvrage. Bien loin d'une description technique et éventuellement rébarbative, il invite le lecteur à découvrir les paysages à la fois sociaux et juridiques qui, demain, défileront le long des "autoroutes de l'information".

Le D.N.S. planet.be est géré par l'association sans but lucratif Louvain-la-Neuve Network. Ses objectifs sont principalement de développer les moyens télématiques de nature à favoriser les échanges entre étudiants, mais aussi entre étudiants et leurs futurs employeurs.

**http://www.planet.be**
I.S.B.N. 2-87379-012-1
Dépôt légal D/Jan. 1997/5883/13

Prix: 975 BEF

**Sous la direction de**

Damien Delhase et Dominique Verpoorten

# Quels paysages juridiques et socio-éducatifs pour les autoroutes de l'information ?

*planet.be*

**Contributions québécoises**

**“Technologies et éducation”:**

la parole aux universités francophones

EDIFIE L.l.N

**Siège Social:**

Av. du Castillon, 35

B - 1450 Chastre

**Secrétariat:**

rue Defacqz, 112

B - 1060 Bruxelles

**E-Mail: edifie@planet.be**

**http://www.planet.be/edifie/**

ISBN 2-87379-012-1

DEPOT LEGAL: D/JAN. 1997/5883/13

*planet.be*

## *Etudiants, mémorants, doctorants, ...*

allez à la rencontre de votre employeur.

## *Publiez*

vos travaux, thèses, mémoires, doctorats, ...
accompagnés de votre

## *curriculum vitae*

sur

*planet.be*

Tous nos remerciements à

Isabelle Garcez,

Sylvie Laurent,

Isabelle Giaux,

Audrey Billy,

Benoît Lips,

Jean-Marc Fricks,

François Gahylle,

Raymond Lepée,

Thierry Cambier,

Alain Saintpo,

ainsi qu'à tous les auteurs, ...

sans qui cet ouvrage n'aurait pas vu le jour, .

# PREFACES

**Michel LEBRUN**

**Ministre des Télécommunications de la Région wallonne**

L'informatique et les Télécoms seront incontestablement les moteurs de l'économie de cette fin de siècle et un tremplin pour aborder l'an 2000.

Comprendre et relever ce défi n'est certes pas la garantie de succès, mais l'ignorer serait à coup sûr la garantie de l'échec.

C'est pourquoi, sur mon initiative, le Gouvernement wallon vient d'adopter un programme de développement des Télécoms.

Ce programme, qui privillégie le rôle fondateur du Gouvernement wallon sur le plan des infrastructures et d'initiateur sur le plan des projets, a été baptisé WIN - Wallonie Intranet.

Son but : la diffusion culturelle des TELECOMS pour tous les wallons avec un accès démocratique afin de contribuer à l'essor économique, social et culturel de la Wallonie.

Tous les Wallons, où qu'ils soient, auront accès, grâce au WIN, à un outil de Télécommunications performant, démocratique, et économiquement porteur.

Nous le sentons tous, la Wallonie a besoin d'un nouveau projet de société, un projet dans lequel chaque citoyen sera à la fois bénéficiaire et responsable. Les Télécommunications, j'en ai la conviction, seront l'un des maillons essentiels de ce projet d'une Wallonie nouvelle.

L'histoire l'a montré, les grandes mutations de nos sociétés se sont toujours accompagnées d'une révolutions culturelle fondamentale.

Les opportunités offertes par les Télécoms sont à cet égard gigantesques.

Mais accéder à cette nouvelle ère que d'aucuns appellent "la société de la connaissance", ne peut se faire sans balises. C'est pourquoi dresser l'état des lieux du cadre juridique et socio-éducatif actuel est une démarche primordiale pour que ce paysage évolue rapidement, pour que les opportunités offertes par les Télécoms soient réellement au service du bien être de notre région et de ses citoyens.

**Benoît LIPS**

**Auteur du best-seller “Internet en Belgique”**

## A l'heure du net ...

A l'heure où beaucoup se posent des questions sur l'opportunité d'Internet, sur les enjeux que peut représenter cet environnement télématique, sur les dangers d'une société désincarnée, il est un fait trop souvent occulté : Internet existe ! Internet existe même depuis longtemps et - curieusement diront certains - vit sa propre vie. Il n'est donc plus question de polémiquer sur les bienfaits ou les méfaits de l'environnement mais simplement de prendre conscience de la réalité de cet environnement virtuel et d'examiner les modalités qui pourront faire que chacun puisse en tirer le meilleur.

Et là une fois encore, c'est la raison qui doit prendre le pas sur toutes autres considérations. Car Internet, prodigieux outil de communication et d'échange d'information, n'est que le résultat d'un fantastique travail collectif et individuel.

C'est dans cette constante alternance entre l'intérêt individuel et l'intérêt collectif que se trouve l'une des plus grandes richesses de cet environnement. Equilibre toujours précaire mais encore réalisé aujourd'hui, Internet reste l'espace où ce constant dialogue amène des résultats qui dépassent les finalités initiales. Et malgré toutes les bonnes ou mauvaises intentions qu'on lui prête, Internet n'est qu'un outil au service d'une communauté de plus en plus large et qui ne représente rien d'autre qu'une opportunité pour chacun.

Opportunité de l'information “immédiate” - qui n'élude pas la nécessité d'apprentissage et d'appropriation des connaissances, opportunité de la communication “totale” - ouvrant sur un monde sans barrières, mise à plat des différences ... ne sont que des concepts que chacun a le loisir de transposer en une réalité personnelle.

*planet.be*

Internet amènera inévitablement des répercussions dans tous les secteurs de l'activité humaine, entrainant des changements profonds des modes de fonctionnement, mais ne doit pourtant pas être confondu avec une réelle révolution. Contrairement a ce qui à souvent été dit, ce n'est pas d'Internet que nous devons attendre un monde meilleur mais bien plus de chacun d'entre nous.

# AVANT-PROPOS

Depuis sa création, le LLN-Net se donne pour mission de contribuer à la promotion des technologies de l'information dans le secteur étudiant (primaire, secondaire et universitaire) ainsi que dans les secteurs associatifs.

Par-delà le discours “gadget” qui réduit les technologies de l'information à une nouvelle manne commerciale et publicitaire ou à un produit branché, le LLN-Net s'efforce d'attirer l'attention sur les mutations profondes qu'elles impriment à la société par leurs capacités de modifier les besoins et les habitudes de communication, de travail et de loisirs, et par leur aptitude à se profiler en de véritables services différenciés aux personnes, aux mouvements, et aux associations.

En ce qui concerne à son travail sur le terrain, c'est d'abord vers ces associations que s'est tourné le LLN-Net. Le volet pratique de son action consiste en effet à mettre à la disposition de toute association qui le demande, un site personnalisé sur le serveur LLN-Net, lui permettant ainsi de faire elle-même l'expérience de nouvelles formes de convivialité et d'information sur leur objet social. Le LLN-Net s'est ainsi constitué progressivement en un partenaire télématique privilégié des associations et organisations de jeunesse.

L'intérêt porté au travail du LLN-Net par les autorités de la Communauté Française de Belgique a en outre permis à deux de ses membres de prendre une part active à deux voyages d'étude thématique sur les autoroutes de l'information organisés par l'AQWBJ. Cette invitation a débouché sur une étude approfondie de la manière dont la perception des technologies de l'information peut être comprise sur le vieux continent et au Québec.

Enfin, le LLN-Net a développé un travail d'information qui a pris la forme d'une série de conférences dont ce livre est à la fois l'aboutissement et le prolongement. Le LLN-NET vous en souhaite riche et profitable lecture !

# PREMIERE PARTIE

# QUELLES TECHNOLOGIES POUR L'EDUCATION ?

L'école ne peut manquer de se sentir interrogée par les technologies de l'information. Une de leurs caractéristiques est en effet de permettre le déploiement de nouvelles formes d'interactivité, de nouveaux modes de participation et de nouvelles architectures du savoir. On parle beaucoup d'apprentissage autonome de l'élève et du changement du rôle du professeur qu'implique ce type d'apprentissage. Le maître se verrait appelé à passer de son rôle traditionnel de livreur de connaissances à celui de tuteur. A cela, il convient d'ajouter que l'Union Européenne s'est fixée, entre autres projets, d'aider à l'avènement d'une “lifelong learning society”, une société où l'on apprendrait tout au long de la vie et que rendrait possible le développement des technologies appliquées au champ de l'éducation et de la formation. Ce sont ces questions qui sont abordées dans cette première partie. En guise d'introduction à cette importante réflexion sur les relations entre éducation et technologies, nous avons demandé aux recteurs des universités belges francophones de nous présenter succintement la manière dont ils envisagent l'intégration des technologies de l'information au sein de leur institution.

# UNIVERSITE LIBRE DE BRUXELLES : LES BIBLIOTHEQUES

**Jean-Pierre DEVROEY, Professeur à l'ULB, Hervé GILSON, Bibliothèques de l'ULB, Catherine SCHOETTER, Bibliothèques de l'ULB**

**(à la demande de monsieur Jean-Louis Vanherweghem, Recteur de l'ULB)**

## 1. Technologies nouvelles et bibliothèques virtuelles

### 1.1 Contexte général

Le caractère à la fois globalisant et multiforme que tend à revêtir aujourd'hui la problématique de l'accès à l'information soulève de nombreuses questions, tant sur le plan technique ou économique de la gestion de nouveaux outils, que sur le plan conceptuel et humain de leur exploitation.

L'explosion et la diversification extrêmement rapides des nouvelles technologies de l'information s'accompagnent d'un ensemble de phénomènes déterminants :

- le rythme accéléré de l'évolution technologique, appelant un développement adapté des savoir-faire ;
- l'augmentation exponentielle des flux de l'information, entraînant la nécessité de les gérer et d'en organiser les modalités d'accès ;
- l'émergence de la diffusion électronique de documents, s'accompagnant de nouvelles exigences d'authentification ;

- la pléthore d'informations disponibles et le besoin qui en résulte de disposer de grilles de lecture adaptées à ce nouvel environnement.

Les services d'information documentaire, en particulier, connaissent une profonde mutation liée au développement de plus en plus marqué de ces tendances.

L'évolution des filières traditionnelles, basées sur le support papier, vers des filières électroniques de gestion amènent les professionnels de l'information à reconsidérer de nombreux aspects liés au stockage, à l'accessibilité et à la diffusion de l'information ainsi qu'à la commande et à la livraison des documents.

Dans ce contexte, la fonction de pourvoyeur d'information implique la mise en place d'une gamme de services nouveaux permettant une définition précise des besoins des utilisateurs, d'une part, et un accès efficace à l'information recherchée, d'autre part.

Fruits d'une évolution technologique rapide, les produits et services nouveaux sont actuellement conçus et organisés de façon empirique en fonction des moyens de production et de diffusion de l'information (normes, protocoles, logiciels, infrastructures, ...) ; afin d'assurer aux acteurs en la matière la maîtrise de ces développements, l'ingénierie documentaire doit donc se donner pour objectif l'élaboration de fondements théoriques pour la production et la diffusion de l'information par les réseaux.

En ce domaine, les grandes directions de recherche s'articulent selon trois domaines d'action :

- la production de l'information électronique ;
- l'optimisation de l'utilisation des réseaux ;
- la distribution de l'information.

Ces axes de développement conditionnent en particulier l'évolution des fonctions fondamentales des bibliothèques.

## 1.2 Evolution du rôle des bibliothèques

### 1.2.1 Les rôles traditionnels des bibliothèques

En quelques années, le développement des *technologies de l'information et des télécommunications* a imprimé une évolution très importante aux rôles traditionnels des bibliothèques :

- conservation ;
- consultation ;
- diffusion des documents ;
- information aux usagers.

A la conservation des livres et périodiques en édition papier s'est jointe celle des ouvrages et bases de données sur *support "numérique"*, disquettes informatiques, cédéroms et ordinateurs interrogeables à distance, chacun étant accessible selon des modalités propres.

D'autre part, les services spécialisés dans la *diffusion de l'information* s'automatisent eux aussi : des modules de prêt inter-bibliothèques en ligne permettent aux lecteurs d'effectuer leurs demandes à distance et à toute heure ; les projets de livraison de documents numérisés par l'intermédiaire des réseaux informatiques livreront bientôt leurs retombées concrètes.

Enfin, les informations relatives aux collections accessibles et aux services disponibles auprès de différentes sources sont à présent diffusées directement par la voie des réseaux informatiques.

### 1.2.2 Les rôles nouveaux des bibliothèques

Certaines fonctions traditionnelles de la bibliothèque peuvent aujourd'hui être assurées à distance au travers des réseaux télématiques. La bibliothèque se voit dès lors dotée de fonctions nouvelles et essentielles : celles de médiateur et de gestionnaire dans l'univers sans cesse plus riche et plus complexe des ressources documentaires accessibles par voie électronique.

Plus que jamais, en vertu des moyens techniques disponibles, la présentation de l'information aux utilisateurs constitue un *service à haute valeur ajoutée*. Plus encore, les techniques existantes de présentation et de diffusion électroniques de l'information permettent de la structurer et y garantissent l'accès le plus aisé.

Dans le foisonnement actuel, il est de plus en plus évident que la *structuration de l'information*, c'est-à-dire le choix, l'organisation et la présentation de l'information constitue un défi majeur pour les producteurs et diffuseurs. Parmi ceux-ci, les bibliothèques sont particulièrement concernées par la prestation de ces services à l'intention de leurs usagers.

Il appartient donc aux spécialistes des bibliothèques et centres de documentation d'acquérir, de développer et de mettre en valeur un *savoir-faire* dans ces domaines ; ceci est d'autant plus crucial qu'ils figurent parmi les rares personnes suffisamment au fait des problèmes liés au traitement et à la diffusion de la documentation.

Ces compétences spécifiques permettront la mise sur pied de *systèmes d'information de campus* ou de *bibliothèques virtuelles* assurant les fonctions de base de l'accès à l'information et de sa diffusion par voie électronique.

La bibliothèque virtuelle PISTE, développée par l'ULB, constitue un projet pilote en ce sens.

## 1.3 Le projet “PISTE”

### 1.3.1 Cadre général

Il y a près d'un an, l'ULB annonçait son intention d'établir, sur son site carolorégien de Parentville, une antenne des Bibliothèques. Celle-ci a

ouvert ses portes le 6 octobre 1995 sous la forme d'une *bibliothèque virtuelle*.

PISTE, “Point d'accès et de diffusion de l'Information Scientifique et Technique par voie Electronique”, s'appuie sur les compétences et le savoir-faire acquis par les Bibliothèques de l'ULB, particulièrement depuis l'ouverture, en septembre 1994, de la “Nouvelle Bibliothèque des Sciences Humaines” sur le campus du Solbosch, à Bruxelles.

### 1.3.2 Description du projet

La mise sur pied de PISTE vise le développement de l'*utilisation des réseaux télématiques* dans une perspective de service documentaire à haute valeur ajoutée pour la communauté universitaire, les entreprises et les particuliers.

Les Bibliothèques de l'ULB proposent à Charleroi un éventail de produits et services extrêmement large touchant à tous les domaines du savoir. Les modalités d'accès à l'information sont diverses et dépendent du type d'information recherchée ainsi que du degré de précision exigé.

Le visiteur de PISTE peut effectuer une recherche autonome basée sur des écrans de navigation spécialement conçus à cet effet tout en bénéficiant de l'aide du spécialiste présent sur place. Ce dernier peut également effectuer des recherches plus pointues ou nécessitant un plus haut degré d'exhaustivité.

Outre ce volet de recherche de l’information, PISTE offre aussi la possibilité de se procurer les documents, qu’il s’agisse de livres ou d’articles, obtenus auprès d’organismes spécialisés ou acheminés par le biais du traditionnel “prêt inter-bibliothèques”, redynamisé lui aussi grâce à la mise en place d’un système de commande informatique.

Aux utilisateurs habituels des bibliothèques universitaires - chercheurs et étudiants - s'adjoint un public nouveau constitué de particuliers, de membres d'organismes publics, d'entreprises ou d'écoles. Cette politique nouvelle d'ouverture à un public extérieur à l'université donne à ces nouveaux usagers la possibilité d'accéder à des sources d'information extrêmement riches, jusque-là généralement réservées à un cercle restreint d'utilisateurs.

Enfin, PISTE constitue un site pilote dans le cadre des projets de développement des technologies de l'information auxquels participent les Bibliothèques de l'ULB.

# LES RESEAUX INFORMATIQUES A L'UCL SITUATION ET PERSPECTIVES

**Auguste LALOUX**

**Professeur au Laboratoire de Télécommunications et Télédétection, Président de l'Institut de Pédagogie universitaire et des multimédias**

**(à la demande du Professeur Marcel Crochet, Recteur de l'UCL)**

## 2. L'interréseau UCL

Dès la mise en place du plan informatique 1985-1990, l'UCL s'est résolument engagée dans une politique de décentralisation informatique entraînant la mise en place de réseaux informatiques locaux connectés entre eux par un inter-réseau.

L'interréseau UCL s'est agrandi petit à petit pour atteindre 220 réseaux en décembre 1995. L'ensemble compte un nombre de l'ordre de 4. 000 machines connectées, auxquelles une adresse IP est attribuée. Cet interréseau est géré par le Service des réseaux informatiques.

L'architecture de l'interréseau est hiérarchisée. Elle comporte trois classes de réseaux :

- **classe 1** : un réseau “dorsal” qui fait partie de l'infrastructure commune de l'université et auquel ne sont connectés que des réseaux de classe 2, appelés réseaux “côtes” et certaines machines d'intérêt général, telles que les serveurs centraux de l'interréseau (courrier électronique, nouvelles, systèmes de noms de domaines, interconnexion avec les réseaux publics, ...) ;

- **classe 2** : des réseaux “côtes” connectés à la dorsale et desservant des quartiers, c'est-à-dire des groupes de bâtiments de l'UCL ;

- **classe 3** : des réseaux départementaux, d'unités, ..., connectés aux soit directement, soit via un autre réseau qui devrait, en général, dépendre de la même entité ou d'une entité englobante. Il y a actuellement plus de 200 réseaux de classe 3, gérés par une septantaine de responsables.

L'interconnexion des réseaux locaux constituant l'interréseau est réalisée au moyen d'équipements baptisés “routeurs DDN-IP”. Ceci implique que les services globaux exploitant l'interréseau soient basés sur les protocoles DDN (appelés aussi TCP/IP).

Cette famille de protocoles offre plusieurs avantages : indépendance vis-à-vis des constructeurs, implantations existant pour la plupart des ordinateurs et des systèmes d'exploitation, migration annoncée vers les protocoles ISO.

Tous les réseaux sont accessibles selon n'importe quel mode (Ethernet, FDDI, LocalTalk, Token Ring, ...) pourvu qu'ils supportent les protocoles DDN, c'est-à-dire qu'ils permettent le passage de paquets DDN-IP, qui est le protocole utilisé par les routeurs DDN-IP pour déterminer à quel réseau local est connecté le destinataire.

L'utilisation de protocoles unifiés n'est pas une contrainte faisant obstacle à la liberté de chacun. En effet, l'usage d'autres protocoles sur les réseaux constituant l'interréseau n'est pas interdit, pour autant qu'ils puissent coexister avec DDN-IP sur ce réseau. L'usage d'autres protocoles resterait néanmoins limité soit à un groupe de machines connectées au même réseau local, soit à un ensemble de machines de divers réseaux de l'interréseau, à condition qu'un service transporteur soit installé.

L'UCL est directement connectée aux autres institutions d'enseignement supérieur du pays par l'intermédiaire de Belnet, le réseau national belge pour la recherche. Comme suite à l'évolution de ce réseau, la liaison point à point entre Louvain-la-Neuve et Heverlee a vu son débit passer de 256 kbit/s à 1 Mbit/s.

## 3. Connexion aux réseaux publics

Le service d'interconnexion de l'interréseau UCL avec les réseaux publics (Datel et DCS), ouvert aux membres du personnel de l'UCL, a connu un développement important. A partir des réseaux publics, les accès possibles sont la connexion directe sur la passerelle d'interconnexion (via Datel et DCS) et PPP (Point to point protocol), via Datel uniquement. A partir de l'interreséau UCL, le seul accès possible est une connexion Telnet à la passerelle à Louvain-la-Neuve pour se connecter alors au réseau DCS.

Un équipement comparable a été installé à Woluwe (UCL-Bruxelles). Grâce à cet équipement, mis en service dans le courant de l'été 1995, la moitié des membres du personnel de l'UCL peuvent désormais bénéficier de connexions vers l'UCL dans leur zone téléphonique. Les accès étant gérés de manière identique à Louvain-la-Neuve et Bruxelles, les utilisateurs peuvent se connecter indifféremment sur l'un ou l'autre équipement, à leur meilleur choix du moment.

Le nombre d'utilisateurs PPP est passé à 248 en fin 1995. En décembre 1995, il y a eu 201 connexions directes pour une durée totale de presque 55 heures. Les connexions via PPP ont été au nombre de 5.414 pour une durée totale qui dépasse les 1.442 heures.

## 4. Services disponibles

La mise en place d'un important réseau interne connecté au monde extérieur permet à tous les membres de la communauté universitaire de bénéficier des services classiques des réseaux informatiques tels que la messagerie électronique, l'accès à des bases d'information communes, le transfert de fichiers, la possibilité de se connecter à d'autres ordinateurs (pour autant qu'on y soit admis comme utilisateur), ...

L'UCL ayant décidé de mettre son information à disposition au moyen du système WWW, un serveur HTTP a été mis en place afin d'accueillir les pages de base du système WWW de l'UCL. Toute l'information servie précédemment par Gopher a été transformée pour être présentée désormais

par WWW. Le serveur de base de l'UCL reçoit quelque 60.000 connexions par mois, dont un tiers environ de l'extérieur de l'UCL.

Le serveur FTP mis en place dans le cadre de la banque d'informations mise à la disposition des membres de l'UCL (1991) connaît un succès sans cesse croissant. Si les connexions à partir de l'interréseau UCL restent aux environs de 400 à 500 par mois, celles à partir du reste de l'Internet en revanche ont triplé de janvier à décembre 1995, pour atteindre 7.000 connexions par mois.

Le volume de nouvelles gérées par le serveur de l'UCL s'est encore accru pour atteindre fin 1995 1.500.000 articles pour une période de 30 jours, sauf pour les groupes des hiérarchies “alt” (6 jours) et “rec” (15 jours). Les nombres d'articles reçus et supprimés varient entre 80.000 et 120.000 par jour. L'espace disque occupé est de l'ordre de 7 GB.

## 5. Accès des étudiants

L'accès des étudiants à l'Internet est une question difficile. Si l'on admet qu'ils doivent pouvoir bénéficier de l'accès à cet incomparable outil d'information, il faut aussi reconnaître qu'une ouverture sans restriction risque d'engendrer des inconvénients énormes : engorgement des salles de terminaux, encombrement des mémoires d'ordinateurs, coût des communications à charge de la communauté, ... L'UCL a donc décidé d'ouvrir prudemment l'usage de l'Internet à ses étudiants. De même qu'il n'est pas possible de permettre à tous les étudiants l'utilisation gratuite illimitée du téléphone (pourtant formidable outil d'information), il a été jugé raisonnable de gérer de façon prudente l'accès aux ressources de l'interréseau.

L'utilisation de l'interréseau UCL est généralement ouvert à tous les étudiants. L'accès au réseau externe n'est normalement admis que par les machines d'unités, notamment dans le cadre des mémoires de fin d'études, sous la responsabilité du promoteur.

En faculté des sciences appliquées, à titre d'essai, un dispositif a été mis en place permettant un libre accès des étudiants à l'interréseau. L'accès des

étudiants de candidatures aux réseaux externes est soumis à l'obtention d'une autorisation préalable du responsable d'un cours ou du Secrétaire académique. Les étudiants du deuxième cycle n'ont pas besoin d'une autorisation préalable pour naviguer sur le réseau externe : ils doivent pouvoir justifier leurs accès dans un objectif pédagogique et dans le cadre de leurs études.

Les étudiants qui veulent consulter des rubriques autres que celles normalement acceptées dans le cadre de leurs études sont invités à prendre un abonnement personnel auprès d'un distributeur de services Internet s'ils disposent d'un poste personnel à domicile.

Les étudiants peuvent avoir accès au logiciel Netscape leur permettant d'accéder à l'interréseau, mais dans le cadre strict de leurs activités didactiques, comme l'indique le “code de bonne conduite”

Ce code que doivent accepter les étudiants au moment de l'octroi d'un nom d'accès à l'interréseau reprend les principes de bonne conduite dans l'utilisation des réseaux informatiques. On y rappelle notamment que “En matière informatique, l'UCL vous confie du matériel et du logiciel, de la même façon que, dans les autres domaines, elle met à votre disposition des locaux et des outils de travail. On ne peut pas mettre des cadenas partout, ni prétendre tout régenter par des règlements. Il n'en va pas autrement dans le domaine informatique : le bon fonctionnement de l'université demande qu'elle fasse confiance à ses membres, chacun étant conscient de ses responsabilités. (...) Dans la vie courante, on ne peut admettre qu'un individu entreprenne de pousser les portes d'entrée des immeubles, dans l'espoir de franchir celle qui ne serait pas verrouillée. Par analogie, l'attitude qui consiste à rechercher et à exploiter les failles des mesures de protection ne peut donc être admise. Autrement dit, nul ne peut prétendre que tout ce qui est possible est autorisé. (...) Ce n'est pas parce que le coût de l'utilisation des réseaux informatiques ne vous est pas imputé que ce coût est nul. Il est pris en charge par la communauté nationale et s'élève à une centaine de millions de francs par an, pour les institutions d'enseignement et de recherche du pays.

## 6. Des services en croissance

Les services rendus aux chercheurs par les réseaux sont bien connus. Ceux qui osent encore évoquer le souvenir de pénibles travaux de rédaction de textes en commun avec des chercheurs d'outre-Atlantique, à l'aide de fastidieux envois postaux successifs, semblent déja décrire des temps préhistoriques. Un collègue en déplacement lointain reste maintenant aussi accessible que s'il n'avait pas quitté son bureau. Les catalogues des bibliothèques peuvent être consultés de façon entièrement décentralisée. Des revues scientifiques fournissent désormais leurs publications sur réseau. On peut également trouver sur réseau les Actes de colloques qui, auparavant, restaient d'un accès très confidentiel. La constitution d'un portefeuille de documentation sur un nouveau sujet est devenue d'une facilité dérisoire.

Ces ressources bénéficient directement à la formation des étudiants de l'université dans le cadre de leurs cours spécialisés et de leurs travaux de recherche.

En ce qui concerne l'organisation des études, la communauté étudiante peut aussi tirer un grand parti de ces nouveaux outils. C'est ainsi que la consultation du catalogue de cours de l'université est accessible sur réseau. On peut y trouver la liste des cours disponibles et y consulter une description des objectifs, des contenus et des dispositifs particuliers mis en oeuvre. Les programmes des différentes filières d'enseignement proposées par les facultés y sont aussi décrits.

L'accès au réseau permet aux étudiants de consulter les informations mises à leur disposition par les Facultés et d'envisager une série de démarches administratives comme l'inscription aux examens, le choix des sujets de mémoire, la confection des horaires des travaux pratiques, ...

Il est déjà possible de consulter certaines notes de cours, rendues disponibles sur Internet. La généralisation de ce système pourrait se révéler particulièrement intéressante. En effet, le système actuel de distribution de notes de cours par les services d'impression se heurte à de nombreuses difficultés de gestion des stocks. Il faut que les cours soient disponibles à temps pour tous les étudiants qui souhaitent les acquérir, même si leur

nombre est difficile à estimer. Par ailleurs, la remise à jour régulière des notes de cours impose parfois la destruction du stock des invendus. La disponibilité de notes de cours sur réseau rend possible une consultation à distance avec envoi des pages souhaitées vers une imprimante locale ou un service d'impression central à grand débit. Elle faciliterait également la recherche d'information dans des notes de cours d'autres programmes d'études.

Depuis longtemps, certains professeurs rêvent de voir leurs étudiants disposer d'un ordinateur personnel permettant d'effectuer à domicile des travaux pratiques en disposant de logiciels ou de fichiers distribués par les enseignants. C'est ainsi qu'en première candidature ingénieur civil, une licence “classroom” prise pour le logiciel d'analyse numérique Matlab permet aux étudiants de disposer à domicile d'une version de ce logiciel et d'y travailler aux projets demandés pour certains cours.

Il est certain que la perspective de voir les étudiants se connecter sur un réseau local permettant la diffusion du matériel didactique permet d'envisager de nouvelles formes d'enseignement et des travaux pratiques plus personnalisés.

Enfin, les nouveaux réseaux de communication rendent possible l'organisation de cours spécialisés en collaboration avec plusieurs universités distantes, en permettant de faire appel aux spécialistes locaux.

Un Centre audio-visuel performant, doté d'un équipement de pointe dans le domaine de la vidéo, de l'image de synthèse et du multimédia, permet la réalisation de documents appelés à être utilisés dans le cadre de tels enseignements.

Pour la formation continuée en particulier, les réseaux devraient permettre de faciliter la participation des professionnels à des sessions de recyclage. Une partie de la formation peut être diffusée par réseau et suivie à domicile, rendant aux heures de contact avec les enseignants toute la richesse des discussions sur des sujets déjà assimilés à domicile.

## 7. Le CEDITI

Dans le cadre d'Objectif 1, l'UCL, en collaboration avec d'autres universités, a mis en place à Charleroi le CEDITI, Centre de diffusion des technologies de l'information. Ce Centre a pour objectif de diffuser dans la région de Charleroi et dans le Hainaut en général les technologies modernes de l'information.

On mentionnera en particulier trois projets de l'équipe UCL du CEDITI, liés directement aux réseaux d'information.

Le premier, BizNet, a pour objectif l'ouverture et l'exploitation de l'Internet dans le Hainaut. L'idée de base est de faire éclore de nouveaux services liés aux réseaux, tout comme le Minitel l'a fait en France il y a une quinzaine d'années. BizNet propose de faire beaucoup mieux sur base de la technologie Internet.

Le deuxième vise à l'établissement de Centres Locaux de Téléservice Multimédias (CLTM) dans la région de Charleroi. Il a pour objectif de mettre à la disposition du public, au sein de centres conviviaux, des ensembles de terminaux multimédias permettant l'accès à toutes informations jugées intéressantes. Ces terminaux sont utilisables individuellement, mais surtout en groupes de travail, de formation ou de loisir, à l'aide d'un accompagnement approprié. Ces Centres abritent des solutions technologiques nouvelles qui favorisent l'interaction avec et autour des machines et des programmes. Ce projet est en synergie avec une recherche interdisciplinaire menée à l'UCL, consacrée à l'appropriation sociale des nouvelles technologies de l'information et de la commuication, et en particulier du multimédia en réseau.

Mentionnons aussi le projet GEOTEL qui a pour objectif l'étude des méthodes, techniques et outils relatifs au télé-enseignement, ainsi que la réalisation d'un prototype d'un système de formation à distance.

## 8. Perspectives de développement

Les prochains développements attendus pour les réseaux, avec notamment la mise en place des réseaux ATM à large bande, devraient multiplier les possibilités actuelles en accroissant les débits possibles et en réduisant les délais de transmission.

Le réseau de télédistribution de Louvain-la-Neuve, mis en place au début des années 70 avait déjà prévu une possibilité d'utilisation bidirectionnelle. En effet, différents points d'accès ont été ménagés sur le réseau à partir desquels il est possible de renvoyer des images vers la tête de réseau pour les réinjecter sur le câble à destination de tous les abonnés. Depuis 20 ans, cette possibilité n'a pas été exploitée, faute de demande. L'accroissement constant de la demande en matière de formation continuée, joint à l'explosion des communications sur réseaux, laisse entrevoir une prochaine utilisation de ces possibilités jusqu'à présent inexploitées.

La toute prochaine libéralisation des communications prévues par l'Union Européenne va permettre aux exploitants des réseaux de télédistribution de fournir divers services de communications sur leurs câbles, depuis la téléphonie jusqu'à l'interconnexion d'équipements informatiques. Un projet élaboré par l'exploitant du réseau de Louvain-la-Neuve avec le Laboratoire de Télécommunications et Télédétection de l'Université doit voir la mise en place d'un Campus-net permettant d'utiliser le réseau de télédistribution pour l'interconnexion d'ordinateurs répartis sur le site.

Parallèlement au développement des techniques, l'UCL veille également à la disponibilité des outils d'exploitation : installation de salles de terminaux multimédias en libre accès et connexion des auditoires à l'interréseau. Des équipements de projection vidéo et vidéo-data sur grand écran peuvent être installés à la demande dans n'importe quelle salle de cours.

Enfin, il convient de mentionner la mise en place d'une équipe interdisciplinaire réunissant des ingénieurs, des pédagogues, des juristes et des spécialistes en communication, chargés d'étudier les différents aspects des développements du multimédia et des réseaux d'information, avec un

accent particulier sur les problèmes d'appropriation sociale et d'impact humain de ces nouvelles technologies.

Il importe aussi de multiplier les efforts en matière de formation du personnel de l'université afin d'accroître la maîtrise de ces nouvelles technologies, mais surtout pour développer l'esprit critique au moment de poser les choix en matière d'utilisation pertinente de ces nouvelles technologies.

Les perspectives qu'offrent les progrès des réseaux de communication pour les universités sont prodigieuses et enthousiasmantes. Puissions-nous y voir, non seulement de nouvelles prouesses technologiques, mais surtout un nouvel outil à utiliser avec discernement et réflexion.

Les données chiffrées fournies en début de ce texte ont été puisées dans le rapport d'activités du Service des réseaux informatiques de l'UCL, disponible sur Internet.

# L'INTERRESEAU ULg : UNE PORTE D'ACCES A L'INTERNET MONDIAL

**Arthur BODSON, Recteur de l'Ulg**

## 9. Accès à l'Internet et intérêt de l'Internet

Le terme "Internet" désigne l'infrastructure qui, au départ, interconnectait les réseaux des institutions académiques et de recherche dans le monde entier. Elle s'est élargie aux organismes privés.

Le développement de l'Internet a été favorisé par les services qu'une telle infrastructure offre : en premier lieu le courrier électronique qui a permis aux chercheurs de dialoguer entre eux par des techniques très performantes, ensuite la multiplication des "serveurs" de toutes sortes : distribution de programmes et documents, bases de données de tous types, etc.

La participation de I'ULg à I'Internet mondial se réalise grâce à l'Interréseau Ulg.

On désigne sous ce terme l'infrastructure qui interconnecte l'ensemble des réseaux locaux de I'ULG, offrant ainsi aux équipements connectés la possibilité de communiquer entre eux. L'Interréseau ULg étant lui-même connecté à I'Internet mondial au travers de l'infrastructure fédérale Belnet[1], la communication est ainsi assurée également avec les autres institutions belges et étrangères.

Les éléments qui interviennent dans l'exploitation de l'Interréseau ULg, et plus largement dans l'usage de I'Internet sont les suivants :

---

[1] Pour rappel, Belnet est géré par le ministère fédéral de la Politique scientiflque et prend en charge le coût des communications Internet des universités belges, soit un budget annuel d'environ 100 millions de BEF.

* l’nfr
astructure physique d'interconnexion ;

*

* les services mis à disposition par l'institution pour sa propre communauté d'utilisateurs, ou ouverts à l'accès d'utilisateurs externes, services qui comportent un volet informatique (moyens matériels et logiciels), mais aussi un volet relatif à la nature et au contenu des services ainsi offerts aux utilisateurs ;

* la formation et l'aide aux utilisateurs pour exploiter les services de I'Internet, aussi bien sur le plan technique (maîtrise des outils informatiques), que sur le plan “documentaire” (navigation dans l'Internet).

## 10. L’infrastructure physique

Le Service Général d'informatique de l'ULg (SEGI) a très tôt fait bénéficier l'ULg d'une liaison vers l'Internet. Faute d'une infrastructure généralisée couvrant toute l'institution, il a été nécessaire de répondre aux besoins au coup par coup. C'est ainsi que les utilisateurs des premières heures ont pu avoir accès à l'interréseau grâce à des câblages locaux et des liaisons entre bâtiments réalisés de manière ponctuelle. L'évolution de la demande est telle que cette approche n'était plus acceptable, et qu'il fallait équiper l'ULg dans son ensemble, en bénéficiant des techniques les plus récentes.

En matière d'infrastructure physique, l'objectif poursuivi est de couvrir l'ensemble de l'institution par un câblage à la hauteur des besoins présents et futurs des utilisateurs.

Cela consiste à assurer une couverture comparable à celle que l'on connaît en matière de téléphonie : aucun bureau de l'Université ne sera exclu d'un possible raccordement à l'Interréseau.

Compte tenu de l'évolution technologique (imagerie, vidéo, données informatiques, ...), cette infrastructure sera capable de véhiculer des volumes d'informations énormes à des débits très importants. L'ULg a retenu l'objectif d'une capacité de 155 Mbit/sec de poste à poste.

Les éléments qui interviennent dans cette infrastructure physique sont

* les câbles entre bâtiments, que ce soit dans le domaine du Sart Tilman (fibre optique), ou entre sites (câble Belgacom) ;

* le câblage “structuré” qui, partant de répartiteurs, atteint les bureaux d'un bâtiment ;

* les “éléments actifs” qui, exploitant l'infrastructure “passive” que sont les fils, réalisent concrètement l'Interréseau en implémentant des réseaux locaux, en les interconnectant entre eux, en distribuant et filtrant le trafic, etc.

La couverture en fibre optique du domaine du Sart Tilman est terminée. Le complexe du 20-Août, le Val Benoît, l'Astrophysique sont connectés par des liaisons Belgacom, dont il faudra augmenter les capacités au fil des besoins.

## 11. Les équipements des utilisateurs

L'insertion d'un équipement utilisateur dans l'Interréseau ULg doit être organisée administrativement (attribution d'adresse, de nom, enregistrement, ...) et techniquement (complément matériel sur l'équipement, implantation de logiciels de communication, et ce, sur des plates-formes très diverses). Le public utilisateur s'est également élargi, englobant de plus en plus de non-techniciens, qui requièrent une aide plus importante.

L'expérience montre que l'utilisateur a besoin d'un encadrement conséquent, non seulement lors du raccordement, mais tout au long de l'exploitation de celui-ci. En complément au support que le SEGI peut fournir, l'encadrement quotidien est assuré par une structure très proche de l'utilisateur : les Unités Décentralisées d'informatique.

## 12. Les services

La majorité des services actuellement offerts globalement à l'institution sont implantés sur des équipements du SEGI, qui en assure la gestion technique. Le développement des services de type “Internet” se traduit généralement par la nécessité de mettre en place de nouveaux “serveurs” et

de nouvelles capacités de stockage d'informations. Il n'est pas possible de prévoir le volume d'informations que l'ULg pourrait vouloir offrir à terme, mais il est certain qu'il connaîtra un développement important.

Les exemples d'universités - américaines notamment - qui ont poussé très loin l'information électronique, montrent, en effet, que tous les secteurs d'une institution académique peuvent être concernés par ce mode de communication. On peut offrir de l'information administrative, scientifique, bibliographique, sociale, culturelle. L'information peut s'adresser aux étudiants, aux chercheurs, au personnel, à un public extérieur à l'institution. Elle peut être de nature consultative (accès à des documents électroniques), ou participative (communication entre les utilisateurs et l'institution).

Les scientifiques associés à des partenaires extérieurs dans le cadre de projets de recherche peuvent trouver un intérêt à proposer un serveur à l'ULg comme pivot de l'information utilisée ou produite dans le cadre de leurs projets, ...

L'organisation de l'information électronique est du ressort d'entités dont la gestion de l'information est la vocation. Une cellule spécialisée attachée au Bibliothécaire en chef et les Unités de Documentation sont tout indiquées pour prendre une large part de cette activité.

Le SEGI entreprend également la diffusion de l'usage du courrier électronique parmi toute la communauté universitaire, y compris l'administration.

## 13. La formation et l'aide à l'utilisation de l'Internet

L'usage de l'Internet devenant accessible à tout utilisateur équipé d'un ordinateur personnel (P.C. ou Macintosh), il est nécessaire de le guider et de l'assister dans l'installation et l'usage des très nombreuses et diverses applications informatiques qui peuvent lui être utiles dans l'exploitation de l'Interréseau Ulg et plus largement de l'Internet. Tout comme il a été nécessaire de former les dactylos au traitement de texte sur micro-ordinateur, il convient aujourd'hui d'assurer un tel support pour les applications de consultation de l'Internet.

L'apprentissage de nombreux logiciels se fera sur le terrain (profitant de la convivialité générale de ces logiciels). Une assistance à l'installation des

logiciels, à leur paramétrisation et à leur usage quotidien sera exercée par une structure proche de l'utilisateur : les Unités Décentralisées d'informatique.

L'usage de l'Internet comporte différents aspects, dont les principaux sont la communication (le courrier électronique, l'échange de documents) et l'accès à l'information résidant sur des serveurs.

Ce dernier s'apparente, dans sa finalité, à la recherche documentaire, qui prend ici la forme de “navigation” dans l'Internet. Cette navigation nécessite une expertise et une connaissance de la structure de l'information et des outils de recherche qu'il est illusoire de trouver chez chaque utilisateur. Pour cette partie également, une structure d'assistance s'avère donc indispensable et sera assumée par les Unités de Documentation.

## 14. Moyens mis en œuvre - budget

Les moyens à mettre en oeuvre s'inscrivent dans le plan de restructuration de l'ULg pour les années 1995 à 1999 et s'élèvent à 300 millions de FB répartis sur 5 ans.

Ils se composent :

* de moyens humains pour la gestion de l'information ;
* de moyens humains pour la gestion informatique ;
* de serveurs pour l'hébergement des données ULg et pour les services destinés à la communauté de l'Ulg ;
* de câblage et d'éléments passifs ;
* d'éléments actifs.

**Moyens humains pour la gestion des informations**

Dans la mesure où la plupart des secteurs d'une université sont ou seront concernés par l'Internet et par l'Interréseau, une cellule attachée au Bibliothécaire en chef sera mise en place qui aura pour mission :

a. de s'informer en permanence des possibilités des logiciels d'accès à l'Internet, de connaître les informations disponibles sur Internet et de tenter une étude critique du contenu des banques de données ;

b. de promouvoir l'usage de ces nouveaux moyens d'accès à l'information en informant et en formant les utilisateurs potentiels ;

c. de valoriser vers l'extérieur les banques de données qui existent dans notre Institution en contribuant à leur mise en réseau ;

d. de développer la distribution d'informations par le réseau à destination de la communauté locale ULg, en ce compris les étudiants ;

e. d'assurer la liaison, pour les aspects non techniques, entre l'ULg et les services de Belnet.

Les tâches touchent donc à la fois à la recherche et à l'analyse d'informations, à la promotion des données rassemblées dans l'Institution, à la formation des membres de l'Université et à la diffusion de documents propres à informer un public universitaire aussi large que possible.

Pour remplir ces missions, deux personnes seront nécessaires. D'une part, un membre du personnel scientifique qui sera plus particulièrement chargé des missions a, c, d et e énumérées ci-dessus, et, d'autre part, un documentaliste qui collaborera plus spécialement à la mission b et à l'aspect “information” de la mission a.

Le Réseau des Unités de Documentation et des Bibliothèques fournira à la cellule des relais où l'on trouvera des personnes compétentes en matière de recherche documentaire.

**Moyens humains pour la gestion informatique**

Ces moyens s'inscrivent dans un cadre plus large que celui de l'Interréseau.

En résumé, il est prévu de recruter 11 universitaires et 11 gradués spécialisés en informatique.

**Serveurs**

Un budget de 3 millions de BEF/an est prévu pour l'acquisition de serveurs ou l'extension de serveurs existants.

**Câblage, éléments passifs et éléments actifs**

***Le câblage et les éléments passifs***

Le câblage et les éléments passifs sont destinés à compléter l'infrastructure fibre optique déployée aujourd'hui dans le domaine du Sart Tilman afin de garantir une capacité de 155 Mbit/sec de poste à poste.

Ils permettront l'installation d'un câblage structuré dans les bâtiments existants situés sur l'ensemble des sites de l'ULg à l'exclusion du Val-Benoît, de l'Institut d'Astrophysique ou de la Résidence André Dumont pour lesquels les déménagements vers de nouvelles constructions (voir le volet “immobilier” de ce dossier de presse) sont prévus dans les prochaines années ; elle ne tient pas compte non plus des nouveaux

bâtiments, en cours de réalisation ou à réaliser, pour lesquels le câblage structuré est prévu dans la réalisation même de la construction, ce qui concerne par exemple le Trifacultaire ou le nouvel Institut de Mathématique (les coûts sont donc couverts par la dotation immobilière).

Signalons enfin que ce câblage “universel” approprié aux transmissions de données informatiques mais aussi aux liaisons téléphoniques permet de répondre aux besoins actuels, y compris ceux induits par les fréquents déménagements partiels au sein des bâtiments existants.

***Les éléments actifs***

Les éléments actifs permettent l'exploitation de l'infrastructure “passive” constituée par les câbles afin d'assurer la réalisation concrète de l'Interréseau.

Le projet permettra de répondre aux demandes actuelles et futures émanant de TOUS les sites de notre Université. En outre, l'installation progressive, dans le domaine du Sart Tilman, d'équipements constituant l'ossature capable de supporter les technologies de “switching”, autorisera les transferts “hauts débits” vers les stations individuelles.

Contrairement aux éléments passifs, ce poste couvre également les besoins des nouveaux bâtiments.

***Estimation budgétaire***

Un budget global de 167 millions de BEF (84 millions pour le câblage et éléments passifs, et 83 millions pour les éléments actifs) est prévu. Ce budget est réparti en tranches annuelles variables pour les deux postes. Ainsi, l'Administration des Ressources Immobilières pourra répondre rapidement aux demandes induites par l'absence quasi-totale de “câblage structuré” et le SEGI pourra répondre aux besoins immédiats en pouvant mieux s'adapter, pour le choix des éléments actifs, à l'évolution rapide des technologies qui permettront au terme des 5 ans de disposer d'une infrastructure “up-to-date”.

# OU EN SONT LES NOUVELLES TECHNOLOGIES AUX FACULTES DE NAMUR ?

**Jean-Pol VIGNERON**

**(à la demande du Père Maurice Gilbert, Recteur des Facultés Universitaires Notre-Dame de la Paix à Namur)**

On serait tenté de répondre à cette question de manière un peu trop évidente : elles sont là où quelques enthousiastes ont bien voulu faire l'effort et les mettre en oeuvre. C'est que les technologies nouvelles ne se répandent pas dans les laboratoires de recherche, les amphithéâtres ou les bureaux par l'intervention d'une décision numérotée. Que ce soit l'informatique, les moyens audiovisuels ou le transport de données, les nouveaux moyens d'expression demandent d'abord une sérieuse évolution des habitudes. Si des efforts considérables sont exigés pour la mise au point de ces techniques - et le travail, aux FUNDP, des laboratoires de recherche comme le LISE[1], l'Institut d'informatique ou le SCF[2] n'y est pas étranger - leur utilisation à bon escient demande un travail réfléchi et des efforts constants de réorganisation.

Dans l'enseignement, par exemple, le recours à des outils nouveaux de formation demande de plus grandes précautions que dans d'autres domaines. C'est qu'ici, la mission à remplir ne souffre aucun compromis : si la transmission du savoir peut être portée par des moyens de communication parfois plus efficaces et mieux adaptés à nos habitudes de vivre, l'encadrement des étudiant ; par de vrais professeurs, ouverts à la discussion, porteurs d'enthousiasmes et forts d'un engagement personnel dans la recherche scientifique reste irremplaçable. Les Facultés de Namur souhaitent ne pas devoir faire face à des économies d'enseignants, même si l'on nous dit un jour que de nouveaux moyens techniques permettront de

---

1 Laboratoire Interdépartemental de Spectroscopie Electronique.

2 Scientific Computing Facility.

surpeupler les auditoires. La qualité de la formation passe d'abord par des contacts humains et il est important de conserver cette occasion de les privilégier.

Néanmoins, en parallèle à l'action pédagogique classique, les Facultés de Namur disposent de plusieurs installations de haute technicité, qui constituent des aides importantes à l'enseignement : le laboratoire de langue et le centre audiovisuel à côté de plusieurs ateliers spécialisés, sont des outils voulus très performants mis à la disposition des enseignants et de leurs projets pédagogiques. Plus récemment, la mise en place d'un réseau informatique couvrant l'ensemble du campus urbain, y compris les amphithéâtres et salles de cours a ouvert de nouvelles perspectives à l'imagination. Ici encore, les moyens nouveaux offerts par ces grandes voies d'échanges électroniques ne seront pas utilisés sans une réflexion préalable et une guidance appropriée : ouvertes aux étudiants qui en ont besoin pour la réalisation de leur projet, ces facilités demandent un investissement important et formateur, si elles sont considérées avec une exigence impérative de rentabilité. Le réseau informatique ne sera qu'un outil, au même titre que le livre, visant à rendre plus direct le contact avec notre planète, comprendre d'autres étudiants du monde et s'ouvrir à d'autres enseignements. Il deviendra une occasion de capter de nouveaux savoirs, qu'il restera important d'évaluer, avec l'aide expérimentée du reste de la communauté universitaire. Le réseau n'est pas donné à l'étudiant pour l'occuper stérilement, mais pour lui donner plus d'envie encore de rencontrer réellement les autres et partager (donner et recevoir), sur place, des expériences nouvelles qui s'intégreront à sa formation.

La recherche fondamentale et la recherche appliquée sont par nécessité l'endroit où les nouvelles technologies - ou les technologies encore hasardeuses - sont le plus nécessaires. Aujourd'hui, si la science fondamentale contribue de plus en plus directement au développement technologique, la technologie de pointe est devenue un facteur important de progrès dans la connaissance du monde. La photographie à l'échelle atomique[3], par exemple, ne s'est révélée que grâce à l'amélioration des matériaux piézoélectriques, du contrôle de la réalisation de pointes, des

[3]Introduite à Namur au LASMOS, Laboratoire de Spectroscopie Moléculaire de Surface.

progrès dans la mesure de courants électroniques ultra-faibles et de la capacité de traitement informatique des signaux acquis. En retour, la connaissance des surfaces de matériaux à l'échelle de l'atome contribue au développement accéléré de nouveaux dispositifs électroniques et des autres composants d'un microscope à sonde locale. Dans un autre registre, la simulation par le calcul[4] du comportement des portes logiques à semiconducteurs contribuera à améliorer les processeurs qui seront utilisés peut-être pour ces mêmes calculs, par les générations futures. La reconnaissance de cette rétroaction entre la science fondamentale et la technologie est l'un des mécanismes essentiels du succès des grandes installations de développement industriel ou universitaire.

Les Facultés de Namur entendent continuer à promouvoir cette synergie nécessaire entre recherche fondamentale, enseignement et développement technologique.

[4]Le S. C. F., installation namuroise de calcul numérique intensif dédicacé à la physique et la chimie théoriques , est actuellement capable de délivrer plus de sic cent millons d'opérations arithmétiques par seconde.

# LES NOUVELLES TECHNOLOGIES A LA F.U.C.A.M.

**Michel DELATTRE**

**(à la demande de monsieur Albert LANDERCY, Recteur des Facultés Universitaires Catholiques de Mons)**

**Professeur au département d'informatique et de gestion de la fucam**

Les Facultés Universitaires Catholiques de Mons forment des gestionnaires pour les organisations privées et publiques. L'enseignement est orienté principalement vers les sciences économiques appliquées, l'ingéniorat commercial et de gestion, et le management des organisations publiques et des affaires internationales. Depuis 1967, le programme de l'ingéniorat commercial met l'accent sur les méthodes quantitatives de gestion et de traitement automatisé de l'information. A cette époque, il s'agissait principalement d'analyse, de programmation en Fortran et Cobol, et de l'étude de systèmes d'exploitation de systèmes informatiques fonctionnant en traitement par lots. Les premiers terminaux apparurent au début des années septante, les premiers micro-ordinateurs en 1980 et le cours de micro-informatique de gestion en 1983. Depuis 1994, un réseau Ethernet en étoiles parcourt l'ensemble du campus, mettant à la disposition des étudiants et du personnel les services de serveurs de fichiers et d'impression en mode client serveur. Ce réseau local fut alors connecté sur le réseau Belnet et à travers lui sur le réseau mondial Internet. Le courrier électronique et les services de navigation sur les serveurs des grandes institutions sont ainsi devenus disponibles.

Les nouvelles technologies de l'information sont également utilisées par d'autres départements : le laboratoire audio-actif comparatif propose un apprentissage interactif des langues étrangères sur un petit réseau de PC munis de cartes vocales. Il apporte la souplesse au rythme de travail, permet le travail en duo ... Un autre réseau de micro-ordinateurs dédié à l'enseignement assisté par ordinateur permet l'auto-formation ou la remédiation en comptabilité, en diagnostic financier, en statistiques. Le serveur de cédéroms de la bibliothèque permet la consultation rapide de nombreuses sources d'informations primaires et secondaires : catalogues des

bibliothèques universitaires belges, quotidiens et autres périodiques, données statistiques ou financières. Les facultés préparent des programmes multimédia pour la formation de juristes à la mise au point de contrats.

Elles participent, dans le cadre de l'inter-universitaire montoise, à un programme européen de recherche visant à mettre en communication de grand débit sur fibres optiques les universités de Mons et de Valenciennes : des débits de 150 Mbps devraient pouvoir être atteints sur une distance de plus de cinquante kilomètres. De nombreuses applications exigeantes en quantité d'informations à transmettre pourront ainsi être partagées à travers la frontière et rapprocher des utilisateurs.

Ce rapide examen de l'utilisation des nouvelles technologies de l'information situe la place occupée par ces outils dans notre enseignement et notre recherche. Elles sont considérées essentiellement comme des outils d'assistance aux enseignants et aux étudiants, qui viennent appuyer l'enseignement magistral, ou comme des outils performants de recherche d'informations.

Cependant, l'utilisation de ces nouvelles technologies pose de nombreux problèmes qu'il est nécessaire de résoudre avant d'en généraliser l'emploi.

Le premier me paraît lié au coût de ces développements : investissement dans l'équipement des postes de travail, coût d'utilisation de ceux-ci en réseau, coût du développement des nouvelles applications.

Si le prix des micro-ordinateurs diminue à performances égales, le marché s'oriente vers des propositions de plus en plus puissantes. Les applications multimédia par exemple exigent une puissance importante, puisque le matériel doit permettre d'afficher des images suffisamment riches et précises, de diffuser un son de qualité ou encore des séquences d'images vidéo. Le micro-ordinateur adapté à ces applications doit ainsi posséder un processeur très puissant, utiliser une mémoire centrale et un disque de grande capacité, disposer de périphériques exigeants comme le lecteur de cédéroms. Le prix d'une telle configuration ne pourrait baisser en termes absolus à moins de l'équivalent de mille dollars. De plus, ces applications nécessitent généralement une durée importante d'utilisation. La mise à disposition de postes en nombre suffisant est donc à la fois indispensable et difficile à concilier avec les contraintes budgétaires qui nous sont imposées et le resteront de nombreuses années encore.

D'autre part, le coût de transmission des informations sur des réseaux étendus, s'il baisse également pour une quantité constante d'informations transmises, ne cesse d'augmenter avec les niveaux de débit impliqués par l'apparition de nouveaux utilisateurs sans cesse plus exigeants. La consultation d'informations en mode graphique par rapport au mode caractères (Netscape ou Mosaic plutôt que Gopher par exemple) décuple les débits nécessaires. De plus, l'illusion de gratuité est entretenue au niveau des utilisateurs. Ceux-ci acquièrent de nouveaux comportements de travail, avec un recours de plus en plus fréquent à des connexions à des serveurs qui les intéressent, même s'ils sont très distants. Dans le pays des acquis, comment financerons-nous nos communications si les sources fédérales, régionales ou communautaires se tarissent ?

Enfin, le développement d'applications intégrant en grande masse images et sons, données et textes, nécessite des ressources humaines, techniques et financières très importantes. Le risque est grand de voir la production de telles applications réservée à quelques grands éditeurs et de conduire plus sûrement et rapidement encore vers une “culture unique”. Au niveau mondial, quel équilibre se formera-t-il entre les droits des auteurs et ceux des éditeurs ?

Un deuxième problème est lié à la productivité de l'utilisation de ces outils. Leur aspect ludique n'est pas inconnu des utilisateurs. Beaucoup consomment du temps et des ressources à naviguer dans ce monde sans limites atteignables qu'est le réseau mondial Internet, au gré de leur curiosité plus que des besoins impliqués par leur travail ou leur fonction. La mise sur le marché de nombreux jeux ou films sur cédérom pourrait encore amplifier ce phénomène.

La mondialisation de la disponibilité des réseaux mettra en concurrence les personnes compétentes, quelle que soit leur localisation. Le travail et l'emploi vont alors se répartir plus largement et les niveaux de salaire s'équilibrer sur une base mondiale. Nos étudiants, futurs “nomades électroniques” devront devenir capables d'affronter un tel niveau de concurrence.

La sécurité des serveurs locaux et des micro-ordinateurs branchés sur un réseau est à la fois difficile à assurer et indispensable. Cette difficulté augmente avec le nombre et la compétence des pirates qui infestent le monde des réseaux informatiques. Les atteintes à l'intégrité des données par

exemple pouvant devenir graves, il est nécessaire de consommer temps et ressources pour la protection de l'équipement et des données. La confidentialité des transferts d'informations pose également problème, surtout pour les applications de courrier électronique, la consultation de données personnelles, par exemple bancaires, etc. Les moyens de cryptage, qui peuvent apporter une solution à ce problème, en créent un autre au niveau de la nécessaire surveillance de l'utilisation de ce media pour des activités illicites. Il nous reste à former nos étudiants, et aussi tous les autres utilisateurs, à une éthique de l'utilisation de ces nouvelles technologies, à leur faire intégrer un code de bonne conduite et de comportements acceptables sur ces moyens de communication qui permettent un dialogue entre de nombreuses personnes qui ne se rencontreront jamais.

Enfin, une réflexion doit être développée à propos de l'extension du “dialogue homme-machine”. Si les applications deviennent “conviviales”, “interactives” et destinées au plus grand nombre, le mode de dialogue proposé ne peut remplacer le dialogue humain entre l'enseignant et l'enseigné. Les conséquences pédagogiques de l'utilisation à grande échelle de ces applications devraient être évaluées avant leur généralisation.

Les nouveaux comportements induits chez les utilisateurs par les nouvelles technologies de l'information vont-ils renforcer leur capacité d'analyse, leur esprit critique, leur créativité, leur capacité à vivre en harmonie dans la société mondialisée par les autoroutes de l'information ?

# DE “L' EDUCATIONAL TECHNOLOGY” A LA TECHNOLOGIE POUR L'EDUCATION

**Marcel LEBRUN[1] , Renata VIGNANO[2]**

## AVANT-PROPOS

Les outils et les produits des technologies nouvelles de l'information et de la communication sont chaque jour plus nombreux, plus rapides, plus performants.

A l'origine de l'interpellation dont le texte qui suit est le fruit, il y a la recherche des raisons et du sens d'une telle course effrénée ; nous nous posions ces questions en tant que “citoyens du monde”, en tant que chercheurs universitaires, en tant qu'enseignants à l'université aussi. Loin des éternelles dichotomies entre hommes et techniques, relations sociales et machines, recherche de sens et recherche d'efficience, notre regard initial sur la problématique de la technologie pour l'éducation sera volontairement “cosmopolite” au sens que P. Levy (1990) lui donne[3] ; l'idée d'éducation que nous ajoutons à son propos d'écologie cognitive et que nous souhaitons enrichir par nos propositions ne peut s'accomoder d'un point de vue étroit ou fragmentaire.

Nous croyons important d'insister sur le lieu de notre interrogation, l'Université ; ses trois missions de formation, de recherche et de service à la société constituent le substrat de notre propos.

---

[1]Université Catholique de Louvain, Faculté de Psychologie et des Sciences de l'Éducation, Département des Sciences de l'Éducation, Unité DIES, Voie du Roman Pays, 20, B-1348 Louvain-la-Neuve, Belgique.

[2]Università Cattolica di Milano, Facoltà di Magistero, Dipartimento di Pedagogia, Largo A. Gemelli, 1, I-20123 Milano, Italie.

[3]P. LEVY, *Les technologies de l'intelligence. L'avenir de la pensée à l'ère informatique,* Paris , Seuil, (1990).

Nous souhaitons nous interroger **sur le pourquoi, le comment et le pour-quoi** de l'utilisation des outils des technologies nouvelles de l'information et de la communication dans l'enseignement et surtout dans l'apprentissage.

* S'agit-il d'un besoin commandé par une société plus avide des produits que soucieuse des processus et des acteurs ?

* S'agit-il seulement de préparer nos étudiants, nos futurs professionnels, nos chercheurs, nos enseignants à piloter ces outils ?

* S'agit-il d'une aubaine réelle pour la formation si ce n'est pour l'éducation de nos étudiants ?

En réinscrivant ces différentes questions (Pourquoi ? Comment ? Pour-quoi ? ) dans le contexte large dont nous ne pouvions, comme universitaires, faire l'économie, il nous est apparu que l'interactivité de ces outils pouvait contribuer à l'acquisition de compétences transversales (organisation des connaissances, démarches de résolution de problèmes, participation et gestion d'un travail en collaboration, développement de projets personnels …) et plus loin à l'autonomie des étudiants[4]. Le développement de ces compétences devient impérieux pour l'épanouissement des savoir-être et savoir-devenir des étudiants et plus largement des personnes dans une société en complexification croissante[5].

Dans cet article, nous retracerons ce chemin parcouru à la recherche du rôle, de la fonction et des finalités des outils que la science déposa progressivement sur les marches d'une humanité en devenir. D'horizons dépassés en tierces places à découvrir, de connaissances maîtrisées en possibles à défier, la technologie propose un esquif au nageur, ce tiers-instruit dont M. Serres nous parle[6]. A ce voyageur ainsi qu'à notre lecteur

---

[4]R. VIGNANO, & M. LEBRUN, *Interazione e autonomia nelle situazioni pedagogiche all'università.,* Pedagogia & Vita, 1994.

[5]M. LEBRUN, & R. VIGNANO, *Quality in higher education : toward a future harmony,* Higher Education, 1994.

[6]M. SERRES, ***Le Tiers-Instruit,*** Paris, 1991.

nous proposons une boussole - éducation est son nom - pour s'orienter dans la mer des Sargasses de la société complexe.

Notre propos de réintégrer l'homme dans “l'educational technology”, tout comme celui de réintégrer l'homme dans la science est une exploration difficile et périlleuse dont les sentiers ne sont pas encore balisés : *Nul n'est plus désarmé que le scientifique pour penser sa science*[7]. Ce regard élargi et ardu mais nécessaire que nous proposons au lecteur n'a pour seule ambition que de tenter de réconcilier ces pôles, ces dichotomies de la science et de la conscience que nous avons épinglés plus haut.

Dans le prochain article, nous proposerons une série d'exemples dont le fond (le contenu scientifique) et la forme (le feu d'artifice dont la technologie l'orne) ont été maintenus dans un cadre aussi simple que possible afin que les considérations pédagogiques et didactiques, que nous avons voulu mettre en évidence dans cet article, transparaissent le mieux possible.

---

[7] E. MORIN, ***Science avec Conscience,*** Editions du Seuil, Paris, 1990, p.20.

## 15. Introduction

*Devant la multiplication et le renouvellement des savoirs, leur distanciation par rapport aux besoins des hommes, les auteurs posent la question du sens de ces savoirs et partent à la recherche du rôle des outils technologiques pour une éducation dans la société complexe.*

Dès son origine, l'homme a cherché une réponse à ses **besoins** par la création d'**outils** ; ces outils et les **savoirs** liés à leurs créations et utilisations ont progressivement modifié **les relations entre les individus, les groupes d'individus**.

Il est loin le temps où quelques règles transmises par la tradition orale suffisaient à maintenir la cohésion et organiser la vie de la tribu néolithique. Ce caractère immédiat et local des relations humaines s'est rapidement complexifié …

Des caractéristiques qui dépassaient souvent la “fonction” de l'outil se sont cumulées autour de l'outil même : nous nous référons, par exemple, aux techniques de construction de l'outil, aux modalités sociales de partage de l'outil, à son efficacité dans le contexte économique, à son ergonomie sur le lieu de travail, à son développement, à la transmission des savoirs et des savoir-faire associés , etc.

Il ne nous appartient pas de reconstruire ici l'évolution des sociétés et des savoirs, mais nous pouvons facilement imaginer que les outils inventés ont permis à l'homme d'augmenter son pouvoir sur la nature, de multiplier ses contacts avec d'autres hommes, tout en rendant son savoir et ses relations sociales de plus en plus complexes. En augmentant son savoir sur la nature, il s'est sans doute aussi progressivement extrait du contexte “naturel” ; en augmentant son emprise par son savoir, il s'est sans doute également singularisé dans le contexte “social”.

**Plus de savoir … plus d'outils … plus de pouvoir … plus de relations … mais surtout une complexification progressive de tous ces facteurs et de leurs interactions.**

Par conséquent, la fonction assumée par les outils et plus tard par le savoir à propos des outils devient de plus en plus cruciale dans les relations interpersonnelles. Ce savoir est devenu à son tour de plus en plus complexe : il se multiplie, se spécialise, s'éloigne souvent du lien direct avec les "besoins" auxquels il cherchait à répondre, de son lieu d'origine, de sa fonction initiale.

Maîtriser ce savoir devient bientôt l'affaire de "spécialistes" … l'homme de la rue y a de moins en moins accès ; d'une certaine façon, le savoir finit par graviter autour de lui-même … les spécialistes du savoir parlent entre eux et la référence aux besoins des hommes devient de moins en moins évidente. **Reste l'outil, devenu instrument ou média, mais que peut en faire l'homme … ?**

Une perspective interpellante et inquiétante se dégage tout au long du chemin que nous avons rapidement parcouru :

Le paradigme dominant de la société actuelle est celui de la complexification, indiquant en même temps la richesse et la multiplication des facteurs intervenants mais aussi la **perte progressive** - en termes de **finalité** et de **responsabilité** - de l'homme comme élément central de la société et du savoir.

C'est par rapport à ce constat que nous dresserons quelques considérations au sujet de la "société complexe" et des "savoirs complexes".

Notre intention est d'y repérer des éléments de réflexion qui pourront nous permettre de construire solidement le cadre dans lequel nous situons nos préoccupations spécifiques : celui de l'enseignement et de l'apprentissage et en particulier la question du rôle des nouvelles technologies de l'information et de la communication dans le **processus de formation** et - nous insistons sur ce point - **d'éducation** de nos jeunes.

Dans les points 2 et 3 qui suivent, nous accomplirons le chemin qui nous a conduit de considérations à propos de la **société complexe aux savoirs complexes** qu'elle produit, qu'elle nécessite et qui la caractérisent.

## 16. De la société complexe

*La complexité de la société, caractérisée par des relations de plus en plus enchevêtrées des différents éléments (personnes, savoirs, outils …) qui la constituent, peut conduire à une véritable aliénation de ces acteurs, à une difficulté pour eux de se mettre en projet dans cette société.*

Notre question concerne la nature et le **sens** - signification et direction - de cette complexité : celle-ci qualifie-t-elle un contexte où la pluralité et la différenciation des éléments et de leurs interactions actuelles et potentielles sont telles que la désorientation, le relativisme, le "mal-à-l'être" en sont les conséquences inévitables ? Ne serait-il pas possible et nécessaire de valoriser plutôt les opportunités que cette même société offre afin de construire une "soi-disant utopie" de planète des hommes ?

S'agirait-il d'une entropie inéluctable du système[8] (social, éducatif …) ou alors d'une abdication ou d'une déresponsabilisation des acteurs concernés ?

Gérer une telle complexité ne pourra se faire par des lois et des règles édictées du contexte que nous qualifions d'extérieur car il a quelque part éjecté l'homme. Tenter de réduire les différences au sein d'un même "modèle normatif" ne fera soit que les niveler soit que les exacerber.

Les outils actuels de l'information et de la communication nous permettent "d'exploiter" ces richesses et ces différences ; cela ne pourrait-il pas aider l'homme, notre étudiant, à mieux se reconnaître dans la société complexe et à mieux la gérer ? Mais une information et une communication toujours plus sophistiquées, plus performantes aussi, pourront-elles seules permettre à l'homme de se retrouver dans une telle dialectique d'identification et de différenciation ?

Pour permettre à l'homme de se retrouver dans cette complexité, de se "retrouver" dans l'image que les médias lui envoient, il est bien sûr

---

[8] C. LEVY-STRAUSS, Tristes Tropiques, Cité par J. NEIRYNCK, ***Le huitième jour de la création : Introduction à l'entropologie,*** Lausanne, 1990, Presses polytechniques et universitaires romandes, 1955.

nécessaire qu'il puisse disposer d'une information large et accessible. La multiplication, la circulation et la gestion des connaissances sont des besoins importants pour nos sociétés. Est-ce suffisant ?

Cette seule perspective nous laisse en fait perplexes. Savoir plus, savoir mieux, savoir comment, savoir "pourquoi" peut-être … mais qu'en-est il du **savoir "pour-quoi"** ? N'y a-t-il pas là le danger d'une **illusion fondamentale**, qui croit pouvoir réaffirmer la centralité de l'homme uniquement par la puissance des moyens à sa disposition, en évacuant ainsi la question prioritaire qui est celle concernant les finalités et les responsabilités par lesquelles ces mêmes moyens doivent être orientés ? Notre réflexion sur ces "objectifs éducatifs à rechercher" complète les propositions de P. Lévy (1990) pour lequel les développements techniques ne déterminent pas nécessairement les développements de la société mais fournissent plutôt des occasions pour ce développement : "En écologie cognitive, il n'y a pas de causes et d'effets mécaniques, mais des occasions et des acteurs"[9].

**Dès lors, le "savoir-être" et le "savoir-devenir" de nos sociétés ne découlent pas de façon automatique de l'augmentation des savoirs.**

Pour en revenir au contexte résolument pédagogique dans lequel nous avons souhaité inscrire notre propos, croirait-on que les "grand-messes" du savoir de nos auditoires ou encore l'introduction massive des ordinateurs dans les classes pourraient suffire, à elles seules, à développer le savoir-être et le savoir-devenir de nos étudiants ?

De telles ambitions demandent un recentrage plus essentiel ; le "devenir-orienté" de notre société complexe ne pourra se construire qu'à partir d'une régulation encore plus fondamentale. Celle-ci implique :

* une ré-actualisation des raisons d'être et des rôles des êtres qui sont origines et moteurs de la société même ;

---

[9] P. LEVY, ***Les technologies de l'intelligence. L'avenir de la pensée à l'ère informatique,*** 1990, p. 169.

* une pro-motion de ces raisons et rôles par la confrontation critique des produits du “progrès” avec les besoins de la société complexe (scientifiques, économiques, sociaux … mais aussi éducatifs).

En d'autres termes, nous croyons qu'il est possible d'éviter la “dérive” conduisant de la complexification à la fragmentation jusqu'à l'absolu des individualismes, par la recherche d'un terrain d'entente et de coopération possible sans pour cela y dissoudre les différences.

Où pourrions-nous, hommes de la société complexe, trouver ce qui peut permettre à notre devenir, souvent erratique et fragmenté, de se muer en un “devenir-orienté” tout en valorisant la richesse de la pluralité et des diversités ?

## 17. Aux savoirs complexes

*Les savoirs de la science et les outils de la technologie apportent à l'homme quantité de reponses, de solutions. Face aux risques énoncés plus haut, les auteurs s'interrogent sur la nature et l'origine des questions et des problèmes auxquels une connaissance approfondie et un choix responsable de ces savoirs et outils permettraient de répondre.*

Besoins générant des outils, outils nécessitant et générant des savoirs, savoirs générant eux-mêmes de nouveaux besoins, de nouveaux outils, de nouveaux savoirs ... que de risques encourus d'y perdre l'homme, que de risques d'asservissement à tenter de le réinscrire dans des modèles qui n'ont été rendus possibles qu'en l'excluant. Des résistances sont toutefois encore bien présentes : que l'on se souvienne du tollé provoqué par la tentative d'intégrer la culture (peut-être plus fidèle à notre image que la “science”) dans les accords économiques du Gatt !

Les outils de la technologie que les savoirs complexes nous renvoient “comme un juste retour” sont-ils à même de permettre à l'homme d'accéder à ces savoirs complexes que nécessite la société complexe ?

Après avoir décrit la société complexe et son risque entropique mais aussi son opportunité d'humanité et avant de répondre à la question du rôle

médiateur éventuel de l'outil technologique, c'est le **statut même du savoir, de la science et de la technique qui retiendra notre attention**.

L'histoire du développement social (et aussi économique et politique) des collectivités humaines présente bien souvent des négligences sur le plan de l'attention à la personne humaine ; un phénomène analogue et intrinsèquement lié à cette dynamique de complexification semble avoir caractérisé aussi le développement du savoir, de la "science".

Nous avons vu qu'aux besoins de l'homme ont répondu, de manière intentionnelle ou incidente, des outils qui ont prolongé son emprise sur la nature, sa sphère d'influence sur d'autres territoires, sur d'autres hommes. A ces extensions progressives, se sont greffés des savoirs de plus en plus complexes. Mais ce **savoir, créé par l'homme**, garde-t-il sa vocation originelle d'un **savoir pour l'homme ?**

Une lecture critique de l'histoire de ce savoir, inventé par l'homme, révèle que celui-ci - qu'il soit théorique ou pratique - s'en est de plus en plus éloigné ; comme le clame E. Morin commentant la "tâche aveugle" d'Husserl, "la science s'est fondée sur l'exclusion du sujet"[10] et nous ajoutons que sa complexité croissante n'en a rendu que de plus en plus hypothétiques les retombées pour l'homme. N'est-ce vraiment que pour pouvoir se cuire, sans beurre, un oeuf sur le plat que l'homme a été sur la lune ?

Nous pourrions parler de la science fondamentale, ce gigantesque atlas des savoirs conceptuels dont les frontières sont sans cesse repoussées, de cette science qui quelque part anticipe les possibles au départ de ses modèles.

L'homme invente, l'homme anticipe … Il s'agit moins d'un savoir ontologique ou encore "extérieur" qui serait accessible à l'homme par la découverte et l'observation de la nature que d'une construction effectuée par l'homme lui-même.

---

[10] E. MORIN, ***Science avec Conscience,*** Paris, Editions du Seuil, 1990, p. 125.

La question des finalités (le pour-quoi, le pour-qui ?) de la science fondamentale nous amène au plan de la science appliquée et de la technique. La technique devrait sans doute utiliser le grand livre des connaissances pour résoudre les problèmes qui se posent dans la société en y trouvant des réponses concrètes.

Par exemple, le cédérom, extraordinaire véhicule d'informations, nous amène sur un disque de quelques grammes un savoir encyclopédique qui illuminera l'écran vidéo de notre ordinateur domestique ; quelques “clic” et le monde est à notre portée nous disent d'alléchantes publicités. Répond-t-il à un réel besoin, sommes-nous capable d'utiliser ce formidable potentiel sans nous assoupir, gavés d'informations ? La technique ne résoudrait-elle dès lors moins les problèmes existants qu'elle ne susciterait de prétendus problèmes en fonction des solutions dont elle dispose ? Avec J. Neirynck (1990) nous posons la question : *La technique est la réponse, mais quelle est la question ?*[11].

**La technique poserait-elle donc elle-même les questions ? Ou alors, qui devrait poser les questions ?**

L'arbre de la connaissance est profondément enraciné dans l'homme mais ses fruits ne lui appartiennent plus. Les produits de la science semblent être le résultat d'une fuite en avant, d'une auto-justification, d'une volonté de créer le besoin sans être à même de rencontrer les besoins des hommes.

Nous retrouvons ainsi les questions du “pour-quoi” et du “pour-qui” que nous avons évoquées. Cet effort de ré-actualisation et de pro-motion auquel nous attachions le futur de nos sociétés trouve son complément dans une analogue “prise en charge” que l'homme doit mettre en oeuvre en tant qu'acteur et producteur responsable de son savoir.

A contre courant d'une science détemporalisée, dépersonnalisée, déshumanisée, et des “grandes parades” de la technique, des voix se lèvent de plus en plus fréquemment afin de retrouver l'homme dans le monde que ces sciences et techniques décrivent et dans lequel elles projettent leurs

---

[11] J. NEIRYNCK, ***Le huitième jour de la création : Introduction à l'entropologie,*** Lausanne, Presses polytechniques et universitaires romandes, 1990.

produits[12]. La **"nouvelle alliance"** recherchée affirme comme un problème en soi l'appartenance de l'homme à ce monde ; c'est une interpellation féconde dont la science et la technique ne peuvent faire abstraction sans risquer de devenir les cathédrales du désert d'un savoir qui masque par son culte sa perte de sens.

Il y a, nous semble-t-il, bien longtemps que la science a renoncé à son paradigme déterministe qui faisait craindre un réductionnisme mécaniste du "fonctionnement humain" ; de la mécanique quantique à la génétique, la reconnaissance et la gestion des possibles ont supplanté la rigidité des équations.

Que nos considérations ne soient pas prises comme l'apologie d'une philosophie du "retour aux origines" ou du mythe d'une innocence perdue qui alimente les rêves d'une humanité se résignant désormais à son aliénation. A aucun moment, notre intention n'est celle de nier les mérites de la science et des nouvelles technologies et surtout l'énorme potentiel que celles-ci mettent à notre disposition. Ce que nous avons voulu mettre en relief par l'analyse que nous avons tracée dans ces pages est l'abondance, l'inflation des "réponses" existantes et possibles pour lesquelles les hommes ne connaissent pas ou plus les questions et ne savent pas toujours les poser.

La question essentielle que nous posons est celle de la possibilité d'une nouvelle alliance entre l'homme et "l'educational technology" : **une technologie pour l'éducation des hommes**.

**En synthèse des propos précédents :**

* Ce que nous suggérons à la réflexion critique des lecteurs est notre refus de la spirale inéluctable de dissolution du goût d'être et d'extériorisation des responsabilités et notre réaffirmation de la possibilité et de la responsabilité d'être acteur de son devenir et du devenir de la société.

* Ce que nous proposons est de voir comment et à quelles conditions les outils de la technologie de l'information pourraient contribuer

---

[12] I. PRIGOGINE, & I. STENGERS, ***La nouvelle alliance,*** Paris, Gallimard, 1986.

à une réappropriation de la science par l'homme (pour-qui ? ) pour vivre dans une société complexe (pour-quoi ? ).

* Au-delà de l'information, de l'instruction, de la formation aux outils mêmes, notre propos est celui d'une possible éducation ; notre cadre sera celui de l'enseignement, notre lieu celui de l'école au sens large.

**Les technologies peuvent-elles dès lors nous suggérer une nouvelle éducation ?**

Dans les points 4 et 5 suivants, nous rechercherons à définir le rôle **de la technologie** et sa contribution potentielle à **l'éducation des hommes**.

## 18. De la technologie ...

*Après avoir passé en revue différents aspects (modalités, potentialités, limites, …) de l'intrusion des technologies dans l'enseignement, les auteurs définissent et inscrivent la technologie et en particulier son rôle médiateur dans une relation didactique finalisée au développement des personnes de la société complexe.*

En inscrivant notre problématique dans le lieu de l'école, creuset de la société, nous la resituons également dans un contexte de relations.

A quelles conditions donc les **outils de la technologie de l'information et de la communication** pourraient-ils contribuer à une nouvelle **relation aux savoirs** en l'articulant dans une **relation entre les personnes ?**

L'expérience antérieure nous le montre : les méthodes du retour de la technologie dans un contexte donné, de surcroît s'il est éducatif, ne sont pas indifférentes. L'immersion des outils de la technologie (rétroprojecteur, audiovisuel, ordinateur …) à l'école n'a pas toujours tenu ses promesses d'ouverture et d'efficacité ; il s'agissait bien souvent d'un contenu (comment utiliser l'outil, ses fonctionnalités …) qui venait se greffer, se juxtaposer à un programme déjà surchargé. L'enthousiasme des pionniers du LOGO, langage d'exploration et de découverte de l'informatique, s'est émoussé par

le peu de cas que les apprentissages ultérieurs, généralement cloisonnés et normatifs, en faisaient.

Cependant des recherches nous montrent le rôle catalyseur de l'ordinateur lorsqu'il est inscrit dans des méthodes pédagogiques organisées autour de modèles de l'apprentissage coopératif et autour de modèles constructivistes de l'appropriation des savoirs[13]. Une méta-recherche menée par E. Bialo et J. Sivin, couvrant les années 1986 à 1990, sur l'efficacité de l'utilisation des ordinateurs à l'école, montre l'impact positif de ceux-ci sur la motivation des apprenants et leurs attitudes envers l'apprentissage et les savoirs et envers eux-mêmes aussi. Cette motivation et ces attitudes contribueraient toutes deux à l'amélioration de leurs performances[14].

Si de nombreuses recherches s'accordent avec la recherche précédente qui nous informe sur les effets de l'utilisation des ordinateurs à l'école, plus rares sont celles qui tentent de dénicher les causes - circonstances ou variables cachées - qui expliquent ces effets. Déjà en 1985, R. E. Clark et S. Leonard approfondissent ainsi la méta-analyse (128 références) de J. Kulik et ses collaborateurs[15] et démontrent l'importance des facteurs personnels et surtout relationnels et méthodologiques qui supplantent les caractéristiques intrinsèques de l'outil même. Nous laissons parler les auteurs dans leurs conclusions :

*Computers make no more contribution to learning than the truck which delivers groceries to the market contributes to improved nutrition in a community. Purchasing a truck will not improve nutrition just as purchasing a computer will not improve student achievement. Nutrition gains come from getting the correct "groceries" to the people who need*

---

[13] K. KUBOTA, ***Applying a Collaborative Learning Model to a Course Development Project,*** Document présenté à : the Annual Convention of the Association for Educational Communications and Technology, Orlando, Florida, 1991.

[14] E. BIALO, & J. SIVIN, ***Report on the Effectiveness of Microcomputers in Schools,*** Washington, D.C. : Software Publishers Association.

[15] J. KULIK, C. KULIK, & P. COHEN, *Effectiveness of Computer-based College Teaching : A Meta-analysis of Findings,* **Review of Educational Research,** 1980.

*them. Similarly, achievement gains result from matching the correct teaching methods to the student who needs it*[16].

Utiliser les produits technologiques du savoir pour développer une nouvelle relation aux savoirs de la société complexe est possible si nous nous dégageons de la seule apparence de l'outil et de son signifiant, le média "per se", pour atteindre le signifié qu'il peut révéler en l'inscrivant au coeur même de la relation didactique.

M. J. Atkins dans son analyse critique de recherches récentes témoigne des avantages didactiques du substrat offert par les médias au niveau de l'apport de l'information, de la simulation de micro-mondes, de la transparence dont ils tapissent les murs de la classe … ; elle souligne cependant les lacunes évidentes au niveau de la description du contexte pédagogique dans lequel les outils s'insèrent, au niveau des rôles attribués aux enseignants et aux apprenants, au niveau aussi des valeurs qui mobilisent et sous-tendent la volonté éducative des concepteurs de logiciels, des chercheurs, des décideurs de curriculum : l'intérêt pour la société est-il de nature "acceptation / reproduction" ou "challenge / transformation" [17] ?

Comme nous l'avons vu, dans les systèmes d'instruction et de formation de nos sociétés, le savoir a progressivement assumé un caractère transcendant sur les besoins, les outils, les machines, les relations humaines ; cette caractéristique en a fait d'une façon croissante la clé de voûte, presque exclusive, du système de formation même.

Au fur et à mesure que certains outils (le livre, l'audiovisuel …) se rendaient de plus en plus disponibles et performants, on vit dans ceux-ci l'opportunité de rapprocher le savoir et l'homme. Ces outils firent bien souvent l'abstraction ou l'économie du tissu relationnel dans lequel ils auraient dû s'inscrire, se ré-inscrire.

---

[16] R. E. CLARK, & S. LEONARD, ***Computer Research Confounding,*** Document présenté à : the Annual Meeting of the American Educational Research Association, Chicago, Illinois, 1985 p. 15.

[17] M. J. ATKINS, *Evaluating Interactive Technologies for Learning,* **Journal of Curriculum Studies**, 1993.

Cependant, l'amplification des savoirs complexes de la société complexe et de ses “machines” allait elle-même faire resurgir de manière plus aiguë ce substrat relationnel latent. Bardé de diplômes, le jeune universitaire dans sa recherche d'un emploi se voit interrogé sur sa tête bien faite plutôt que sur sa tête bien pleine.

Cette approche critique que nous avons développée au sujet des produits de la technologie et de leur utilisation orientera nos réflexions : nous ne parlerons ici ni d'une **technologie de l'instruction** soucieuse de la planification optimale des opérations à mettre en place pour élaborer un produit dit éducatif, ni encore d'une **technologie de la formation** visant à structurer le déroulement d'une leçon afin d'en tirer la plus grande efficacité : les manuels de l' “educational technology” ou de l' “instructional design” regorgent de ces conseils[18]. Sans minimiser l'importance de ces connaissances, nos préoccupations se situent plutôt dans une perspective pédagogique et didactique. Nos considérations concernent une possible **technologie pour l'éducation**.

Les produits (que les destinataires n'ont pas “voulu”, qui n'ont pas nécessairement été élaborés dans une optique éducative …) que le savoir nous lègue, ces outils technologiques de et pour la société complexe peuvent-ils se prétendre d'une quelconque utilité pour l'éducation ?

**Mais qu'est-ce donc que la technologie ?**

Parmi d'autres définitions, nous épinglons celle de Galbraith : La technologie serait l'application systématique des connaissances scientifiques ou autres connaissances organisées à la résolution de problèmes pratiques[19].

---

[18]Par exemple : M. D. MERRIL, R. D. TENNYSON, & L. O. POSEY, ***Teaching Concepts : An Instructional Design Guide,*** (2nd ed.). Englewood Cliffs, New Jersey, Educational Technology Publications, 1992.

[19]J. K. GALBRAITH, ***The New Industrial State,*** New York : A mentor book, p. 11. La traduction de la définition est proposée par J. lapointe, & P. Gagné, ***La savoir d'expérience et le savoir intuitif en technologie de l'éducation : contributions décisionnelles de savoirs négligés,*** In L. Sauvé (Ed.), 1992 *; La technologie éducative d'hier à demain:,* Actes du VIII Colloque du Conseil interinstitutionnel pour le progrès de la technologie éducative, Québec, 1992, pp. 275-286.

Ainsi la technologie de l'information viserait à résoudre un problème pratique d'information. Une partie de la réponse, une partie seulement eu égard à notre problème éducatif, résiderait dans les outils que cette technologie nous propose : le livre et surtout l'écrit, la radio et surtout la parole et le son, le téléviseur et surtout le visage et l'image, l'informatique et enfin le multimédia qui marie ces diverses composantes scripto-audio-visuelles.

Outre les connaissances scientifiques requises pour construire et faire fonctionner l'outil et que nous avons choisi de ne pas retenir ici, d'autres connaissances s'avèrent pour le moins pertinentes dans le contexte où nous voulons intégrer l'outil : elles ont pour noms communication, ergonomie, convivialité, design d'écran, …. Dans les faits, elles visent principalement à réorganiser ou à vulgariser les savoirs, à **transformer le savoir savant en savoir (à) enseigné(r)** en se souciant peu, semble-t-il, des personnes (qu'en feront-elles ici et après ?) et des contextes qu'elles vivent, qu'elles déterminent et avec lesquels elles interagissent.

En amont des questions concernant les contenus, les supports qui “matérialisent” ou “véhiculent” ces contenus, les caractéristiques concernant les individus qui apprennent ou qui enseignent et concernant les activités qui les réunissent - apprentissage et enseignement - doivent être prises en compte : les connaissances pédagogiques et didactiques constituent des champs relativement éloignés des préoccupations immédiates des technologues. Cependant des ouvrages récents[20] manifestent le souci d'ancrer mieux l' “instructional design” dans les perspectives tracées par les théories de l'apprentissage.

Enfin l'écrit, le son et l'image sont mariés … enfin on peut interagir avec le savoir … enfin “le Power-PC est plus humain qu'un Macintosh”.

Est-on sûr que quelques boutons de plus sur l'écran de l'ordinateur (qui n'a pas réellement envahi nos écoles au contraire de ce que nous

[20]Par exemple : M. FLEMING, & W. HOWARD LEVIE (Eds.), ***Instructional Message Design : Principles from the Behavioral and Cognitive Sciences,*** Englewood Cliffs, New Jersey, Educational Technology Publications, 1993.

annonçaient les futurologues des années 60) peuvent, à eux seuls, transformer notre relation au savoir de la société complexe des hommes ?

Il nous semble dès lors important de réfléchir à l'impact des médias non pas seulement comme une manifestation tangible des connaissances dans l'univers de l'homme mais comme une occasion d'appropriation du savoir par l'homme : **le média peut-il nous provoquer à explorer le savoir, à élucider les processus qui l'ont élaboré, à nous reconstruire le savoir, à poser enfin nous-mêmes les questions … ?** Si les médias véhiculent des réponses à des questions que nous, perpétuels apprenants, ne nous sommes pas encore posées, pouvons-nous les utiliser pour interroger les savoirs ?

Cette démultiplication des savoirs, des points de vue sur le savoir, des voies d'accès au savoir constituerait alors le substrat fécond sur lequel pourraient se développer les savoir-faire, savoir-être et savoir-devenir[21] requis pour gérer mieux et pour vivre mieux la société complexe, pour finalement mieux s'y mettre en projet.

**Cette éducation pour être et devenir avec la société complexe nous suggère-t-elle une technologie pour l'éducation ?**

## 19. A l'éducation

*Un examen des concepts d'interactivité et d'interaction qui affublent généralement les médias proposés par la technologie mène les auteurs à revendiquer le sens plein de ces termes dans la relation dynamique des êtres qui, en construisant les savoirs à l'aide des outils médiateurs de ces mêmes savoirs, se mettent en projet et finalement s'éduquent.*

A l'aube de la société complexe, la tradition orale suffisait pour la transmission des savoirs nécessaires : l'apprentissage à l'outil par l'outil dans le contexte local (nous dirions "sur le terrain") et relationnel se faisait "naturellement" dans le cadre de communautés restreintes. L'extension de l'emprise de l'homme sur la nature mais aussi sur le territoire et sur les

---

[21] J. -M. De KETELE, *L'évaluation du savoir-être* In J. -M. De Ketele (Ed.), ***L'évaluation : approche descriptive ou prescriptive ?,*** Bruxelles-Paris : De Boeck, 1986, pp. 179-208.

relations, par les outils et surtout par les savoirs progressivement développés autour des outils, allait donner une place de plus en plus prépondérante aux savoirs par rapport aux savoir-faire. De spécialisations en spécialisations, les savoirs se complexifiaient et se distanciaient des besoins locaux et immédiats. Le contexte relationnel allait lui aussi nécessiter de nouveaux savoirs qui se manifestèrent, par exemple, dans la lecture et l'écriture : des lieux nouveaux (l'école), des médiateurs (l'enseignant) s'avéraient ainsi indispensables pour l'apprentissage de ces savoirs.

D'abstractions en abstractions, le regard du savoir sur l'outil allait donner lieu à de nouveaux savoirs, à de nouveaux outils. Si les premiers outils correspondaient de façon immédiate aux besoins des hommes, les nouveaux, revisités par le savoir, s'en éloignèrent parfois pour mieux les anticiper, parfois aussi pour les créer. Les savoirs issus de la nécessaire “gestion” des sociétés allaient progressivement s'abstraire et se techniciser eux aussi en assujettissant parfois les individus et en normalisant souvent leurs relations. Les “techniciens” qui tentaient de réintégrer ces savoirs dans la sphère de l'homme en proposant des outils pour répondre aux nouveaux besoins devaient réapprendre et faire réapprendre à gérer l'information, à gérer les différences ... L'informatique et les télécommunications se pointaient à l'horizon porteuses de nouveaux concepts : information, communication, interaction, ouverture sur le monde des techniques … des hommes aussi ?

Au besoin de formation, polarisée sur le savoir, va-t-il se substituer un besoin d'éducation : comment être dans la société complexe avec ces outils, ces savoirs, ces outils d'organisation du savoir que sont les ordinateurs ?

L'outil qui nous parle de “relations”, de réseaux, d'interactivité nous permettra-t-il de **dépasser l'interactivité fonctionnelle** que propose le clavier ou l'écran pour **atteindre une interactivité relationnelle** permettant d'accéder à de nouveaux savoirs au travers des êtres qui les construisent, qui les vivent ?

Nous relions notre concept d'interactivité fonctionnelle aux modes d'interactivité “réactive” et “proactive” décrits par R. A. Schwier et E. R. Misanchuk (1993) : dans l'interactivité “réactive”, l'ordinateur attend de l'apprenant une “réponse précise” à un stimulus qu'il lui propose (logiciels

de type “drill and practice”, tutoriels …) ; dans l'interactivité “proactive”, l'apprenant entreprend une “construction” personnelle face à un contexte que l'ordinateur lui propose (logiciels de type simulation, modélisation …). Ces auteurs complètent ces deux modes par celui d'interactivité “mutuelle” dans laquelle l'apprenant et le système informatique “intelligent” s'adaptent mutuellement (intelligence artificielle, systèmes experts …)[22] ; nous élargissons ce dernier mode dans un concept d'interactivité relationnelle qui l'enrichit par les perspectives interpersonnelles auxquelles l'ordinateur convie les apprenants dans le cadre de travaux coopératifs.

La figure ci-dessous organise ces concepts d'interactivité : **l'interactivité constitue pour nous un état potentiel dynamisé par les situations pédagogiques et didactiques dans lesquelles les savoirs, et surtout les apprenants et les enseignants entrent en interaction.**

[22] R. A. SCHWIER, & E. R. MISANCHUK, ***Interactive Multimedia Instruction,*** Englewood Cliffs, New Jersey, Educational Technology Publications, 1993.

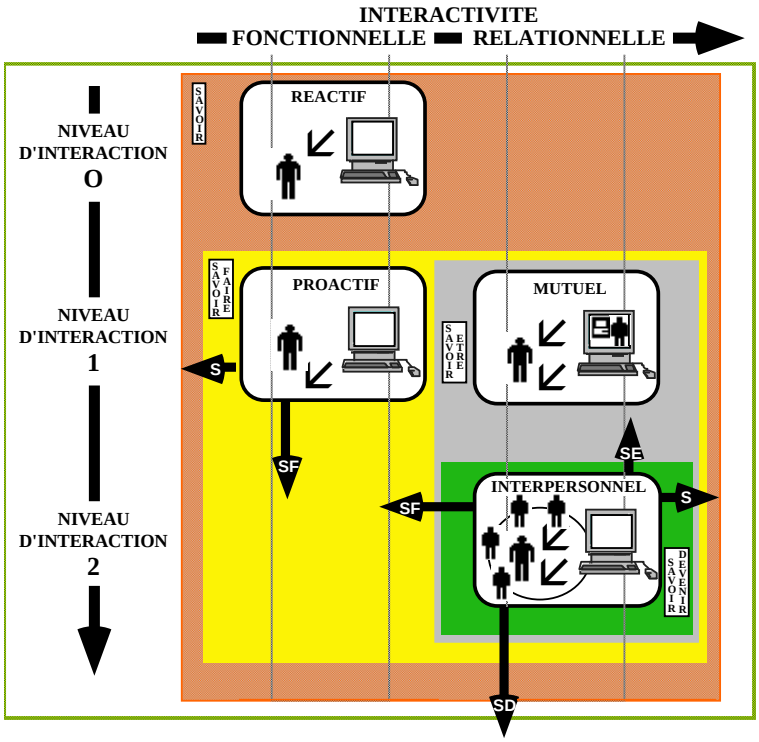



Figure 1: Organisation des concepts d'interaction et d'interactivité

Les trois niveaux d'interaction que nous présentons scandent un chemin le long duquel la place et l'initiative de l'apprenant sont de plus en plus fortes ; c'est aussi un chemin qui nous conduit d'un pôle centré sur l'outil, présentant des contenus spécifiques et des situations relativement fermées, à un pôle centré sur l'apprenant et son projet autour de situations complexes et ouvertes.

Ce chemin, fondé sur l'intégration progressive des savoirs (S) et des savoir-faire (SF), s'ouvre de plus en plus vers des savoir-être (SE) et savoir-devenir (SD) ; ces derniers s'exercent dans les relations interpersonnelles suscitées par des méthodes éducatives qui mettent en place des occasions de

développer les compétences transversales requises par la société complexe. Des exemples relatifs à chacune de ces “catégories” seront développés dans un prochain article des “Cahiers de la recherche en éducation”.

A titre d'exemple, nous voyons que le mode interpersonnel (case en bas à droite) s'appuie sur les quatre dimensions du savoir en les intégrant et contribue à développer (les quatre flèches sortantes) harmonieusement ces dimensions. Comment parvenir et faire accéder à cette éducation, à laquelle nous attribuons la tâche de réduire le décalage entropique entre savoir(s), savoir(s)-faire, savoir(s)-être et savoir(s)-devenir des hommes ?

Pouvons-nous, dans le cadre de l'enseignement, réellement chercher à recomposer ce puzzle, à réalimenter une intégration dynamique et progressive entre ces dimensions, à actualiser cette utopie de la planète des hommes ?

La réponse ne se trouve dans aucune “définition” illusoirement définitive de l'éducation que nous pourrions injecter à cette étape de nos réflexions. Le débat éternel sur la nature de l'éducation n'est pas non plus ce qui peut effectivement nous aider à maîtriser mieux cette complexité dans laquelle nous avons décelé les symptômes d'un “mal-à-l'être” diffus. Plutôt, reconnaissons ce besoin “pragmatique” d'éducation qui, tout en intégrant l'instruction et la formation mais les dépassant par une perspective de sens bien plus puissante, peut répondre aux besoins et aux aspirations des hommes de la société complexe.

Ces interrogations sur le “comment” de l'éducation conduisent notre attention sur les méthodes d'enseignement dans lesquelles l'instruction, la formation et l'éducation devraient trouver leurs articulations mutuelles et dans lesquelles aussi enseignants et apprenants se retrouvent.

Notre propos n'est pas de nous joindre à ceux qui chantent le “requiem” de l'école, au nom de son inefficacité endémique, de son retard chronique face aux “commandes” du monde professionnel et économique, de sa lourdeur à s'adapter aux rythmes de la modernité ou, encore, de son encyclopédisme qui étoufferait la créativité et la richesse potentielle des étudiants (mais aussi des enseignants …). Nous sommes bien conscients que les institutions éducatives, de l'école maternelle à l'université,

foisonnent d'initiatives pédagogiques innovantes qui témoignent de la vitalité de ceux qui y oeuvrent, de leur exigence, de leur volonté et de leur capacité de changement.

Néanmoins, nous assistons encore souvent à des “cours” qui ne donnent qu'un savoir détemporalisé, décontextualisé, dépersonnalisé, un savoir “aseptisé” qui fait abstraction du cheminement “humain” - souvent fait d'hésitations, d'erreurs, de questionnements multiples, de longues périodes d'obscurité - par lequel il a été progressivement élaboré. Les situations didactiques ressemblent trop souvent à de prestigieux monologues où le “savoir savant” est délivré tout au long de voies royales, sans que les expériences de la vie “concrète” quotidienne puissent le questionner, le mettre en rupture mais aussi le faire retrouver. Il est là, prêt à être “donné” plutôt que réellement enseigné c'est-à-dire mis en état d'être appris, prêt à être redit plus qu'à être vécu.

**Nous retrouvons dans le cadre de l'enseignement et de l'apprentissage cette même disjonction artificielle entre savoir, savoir-faire et savoir-être : l'accumulation des savoirs reste gagnante sur l'intégration de ceux-ci dans le développement des comportements et des attitudes des étudiants.**

Cette mise en vitrine de contenus singuliers et de savoirs fossilisés à laquelle l'enseignement est trop souvent réduit peut-elle vraiment se prétendre éducative ? Ce “savoir qui vient d'en haut”, détaché du tissu relationnel et du contexte des besoins, des attentes, des contraintes et des aspirations qui l'ont généré peut-il encore prendre sens, faire sens, être sens ?

L'étudiant risque de se trouver en présence d'une multitude de pièces de quelque vague puzzle : chaque spécialiste lui explique en long et en large sa pièce de prédilection mais personne ne l'aide à reconstituer l'image d'ensemble permettant de situer chacune des différentes pièces dans le tout où elle s'insère. La spécialisation ne suffit pas, ne suffit plus , “… elle serait

plutôt un poids gênant sur sa nuque qu'une aile qui lui permettrait de s'élever"[23].

La faillite d'un certain type d'éducation qui laisse nos jeunes avec "l'âme désarmée"[24], incapables d'affronter les réalités de la vie et les diversités des cultures - qui deviennent de plus en plus difficiles à saisir et à gérer - est sous nos yeux. Des fleuves d'encre, de mots et d'images nous parlent de la crise des valeurs, de la "me-generation", d'une adolescence "éternelle" de beaucoup de jeunes qui repoussent de plus en plus la transition critique vers l'âge adulte où ils "devraient" se prendre en charge ; ou encore, ils nous parlent des exigences ambiguës du monde professionnel pour des "meneurs" d'idées, de projets, d'hommes et pas seulement pour des exécuteurs de consignes, même hypercompétents ; ou encore, ils dévoilent les statistiques tragiques de la criminalité juvénile, du suicide des adolescents, de la recherche de paradis artificiels, … encore une fuite face à un "mal-à-l'être" auquel on ne trouve pas d'autres réponses.

Sommes-nous trop ambitieux (ou peut-être trop "pédagogues" …) en affirmant que le "réarmement de l'âme" pourrait être soutenu par un enseignement, une éducation qui puisse concrètement aider les étudiants à s'approprier des connaissances et à développer des compétences réellement utiles et nécessaires à la définit ion et à l'accomplissement de leur projet d'étude, de leur projet professionnel et surtout de leur projet personnel dans la société complexe[25] ?

A l'encontre de ces disjonctions entre personne et société, entre savoir-être et contenus, nous proposons leur conjonction par le développement dans le cadre même du système d'enseignement de compétences transversales non seulement comme un produit à atteindre mais comme un

---

[23]F. NIETZSCHE, ***Sur l'avenir de nos établissements d'enseignement,*** Paris, Gallimard, 1973, p. 132.

[24]R. BLOOM, ***L'âme désarmée. Essai sur le déclin de la culture générale,*** Montréal, Guérin littérature, 1987.

[25]R. VIGNANO, ***Psicologia ed educazione in Lawrence Kohlberg : Un'etica per la società complessa,*** Milano, Vita & Pensiero, 1991.

processus ouvert, construit tout au long des études, sans cesse réactualisé et visant à la promotion des personnes.

Dans les trois derniers points de ce document, nous décrirons certaines caractéristiques **des méthodes d'éducation** pour la société complexe. C'est à l'apprenant cependant que reviendra la tâche de s'exercer **aux méthodes pour s'éduquer** lui-même. Quel rôle attribuer **aux médias** dans cette perspective ?

## 20. Des méthodes d'éducation

*Par delà les îlots de savoirs éparpillés ou juxtaposés, les auteurs insistent sur l'importance des compétences transversales qui les relient entre eux et qui les relient aux préoccupations et problèmes des personnes qui vivent la société complexe. C'est à l'école que revient la promotion de ces démarches et méthodes d'investigation et d'ouverture.*

Force nous est de constater que le développement de ces compétences transversales ne constitue pas un objectif effectivement poursuivi dans nos écoles. **Mais où sont alors les occasions d'apprendre et d'exercer activement ces compétences ?** Cela devrait-il se faire **ailleurs ?**

L'école se repose-t-elle dès lors sur un "ailleurs" où ces compétences seraient effectivement acquises, construites, mises en oeuvre ? Si cet "ailleurs" (la famille, la communauté locale…) était autrefois le ciment qui unissait ces savoirs aux savoir-être et aux savoir-devenir, l'éclatement de la société complexe auquel nous assistons ne le permet plus.

La réintégration et la relocalisation des savoirs de l'école :

* dans d'autres savoirs que la société propose de manière parallèle (journaux, télévision, média…)

* dans les besoins, problèmes et relations complexes que cette société requiert demandent aujourd'hui d'autres moyens, d'autres méthodes.

Il ne nous est pas possible dans cet article de décrire les avantages et les inconvénients des diverses méthodes d'enseignement ; cependant, on met souvent en évidence la méthode du “problem-solving” comme une occasion d'actualiser les savoirs structurés de l'école dans la structuration des démarches requises pour résoudre “au mieux” des problèmes (et non des exercices) qui se posent en dehors de l'école. Woods (1987) préconise que ces démarches ne restent pas accessoires ou latentes face à l'avènement de la réponse attendue et qu'elles soient enseignées à part entière ; il ne néglige cependant pas le fait qu'une réelle démarche par résolution de problèmes nécessite une conjonction importante de nombreux savoirs de natures et d'origines diverses[26]. Où l'étudiant se les construit-il ? Des outils peuvent-ils l'aider à manipuler, à structurer les savoirs sans qu'un enseignement systématique de ceux-ci ait lieu ?

Pourquoi certains étudiants se débrouillent-ils mieux que d'autres plus démunis ? Le système “éducatif” ne favorise-t-il pas une caste de ceux qui ont la chance, par leur milieu, par leurs expériences d'acquérir ces compétences transversales, de les construire, de les mettre en oeuvre ?

**Est-ce l'aveu d'une école qui accepte, qui se résigne à n'être que le temple du savoir ?**

**Est-ce encore, face à la complexité, une école ?**

Si la question d'une école plus “éducative” surgit en ce moment, n'est-ce pas parce qu'elle s'est progressivement éloignée de la société, de ses besoins, de ses outils ? Les recherches pédagogiques que l'on vante parfois sans trop y croire souvent, la publicité tapageuse des écoles pour de “nouvelles pédagogies”, l'étalage des moyens des salles d'informatique trop peu utilisées ne sont-ils que le décorum d'une bonne conscience tranquille visant à cacher l'étouffement de la signification et du sens, sous l'inflation des savoirs éparpillés ?

---

[26] D. R. WOODS, *How Might I Teach Problem Solving ?,* New Directions for Teaching and Learning, 30, 1987, pp. 55-71.

## 21. Aux méthodes pour s'éduquer

*Si les méthodes éducatives sont facilitées par les outils technologiques, c'est à l'apprenant que reviendra in fine la tâche de s'éduquer ; c'est lui qui passager dans l'institution accomplira le voyage dans la société complexe, continuera à s'éduquer. Comment les méthodes proposées par l'enseignant étofferont-elles le bagage de notre voyageur ?*

**Une nouvelle médiation entre les savoirs de l'école et ceux de la société complexe, par l'exercice des compétences transversales soutenues à leur tour par les outils technologiques de l'information et de la communication, doit dès lors être promue par l'école même.**

Au-delà des outils, le besoin d'éducation que nous avons détecté nécessite aussi des méthodes pédagogiques profondément ancrées dans l'interaction entre les étudiants, entre les étudiants et l'enseignant utilisant ensemble des outils à potentiel hautement interactif, des méthodes insistant plus sur les démarches de construction des savoirs que sur la distribution de savoirs construits. Notre proposition trouve un soutien dans les conclusions de la méta-recherche dont nous avons parlé plus haut[27] : ce ne sont pas tant les caractéristiques propres de l'outil qui sont importantes mais la manière dont il est soutenu et intégré par l'environnement éducatif de la classe et de l'institution.

Il s'agit de situer les médias - fruit du savoir complexe de la société complexe - dans la relation didactique, celle qui unit les enseignants et les apprenants dans la re-création de savoirs riches de sens.

Il serait illusoire de circonscrire les méthodes d'éducation dans des définitions grandiloquentes et dans des recettes passe-partout. Cela signifierait vouloir "abstraire" des processus qui se situent et se réalisent dans des contextes concrets. Nous retomberions ainsi dans la même dynamique perverse que nous avons dénoncée : celle d'un "savoir sur l'éducation" détaché du terrain des besoins et des relations sur lequel il s'ancre, des finalités qui le justifient.

---

[27] E. BIALO, & J. SIVIN, ***Report on the Effectiveness of Microcomputers in Schools, 1990,*** pp. 12-13.

Plutôt, nous suggérerons quelques pistes qui toutes contribuent au développement des étudiants au travers des situations pédagogiques interactives mises en place. En particulier, nous montrerons comment fournir aux étudiants des occasions d'intégration de connaissances et des moyens permettant des éclairages variés d'un concept donné afin d'en faire ressortir la richesse, le relief, … la complexité.

Sans négliger les informations ou les connaissances nécessaires à l'entrée en situation (mode réactif de la figure 1), un enseignement plus inductif et plus participatif serait d'un précieux secours dans cette problématique[28] afin d'apprendre à l'étudiant :

* à se poser un problème (mode proactif de la figure 1) ;

* à trouver soi-même dans l'arsenal des méthodes, des modèles et des théories l'approche la plus pertinente (mode proactif) ;

* à vérifier ses solutions par des méthodes alternatives, à comparer son approche à celles suivies par d'autres apprenants (mode mutuel) ;

* à reconnaître et à contrôler soi-même les limites et le degré de validité de l'approche choisie en replongeant la situation pédagogique dans le contexte large dont elle n'est qu'une “image” (mode mutuel) ;

* à développer son propre projet au sein de la collaboration, à s'impliquer et à se responsabiliser face à la tâche, etc (mode interpersonnel).

Voici quelques uns parmi les objectifs qui nous semblent les plus pertinents et les plus urgents pour l'éducation des hommes de la société complexe et qui devraient catalyser les nombreux efforts produits dans le

---

[28] M. LEBRUN, Possibilités et méthodologies d'intégration d'outils informatiques dans l'apprentissage des sciences, ***Recherche en éducation, théorie et pratique, 7,*** 1991, pp. 15-30.

cadre des “initiatives pédagogiques” certes méritantes de l'enseignement actuel.

Les lignes qui précèdent mettent en évidence notre souci de recentration des objectifs éducatifs sur la personne de l'étudiant en tant qu'acteur de son apprentissage et futur acteur dans la société. Des critiques à l'égard de cette approche et des différentes “pédagogies” qui s'y rapportent sont régulièrement émises : “elle est sans doute plus captivante pour les étudiants mais ce n'est pas nécessairement un gage d'efficacité” ; “elle suscite peut être leur motivation mais il s'agit d'une implication superficielle, d'une adhésion émotionnelle à un univers ludique plutôt que d'une démarche rigoureuse d'approfondissement intellectuel”. Cependant, l'expérience le montre, une telle approche pose des exigences non négligeables à la fois aux étudiants et aux enseignants.

Les premiers ne sont plus seulement des spectateurs, des récepteurs passifs du savoir mais ils doivent participer activement et personnellement à la construction de celui-ci : émettre des propositions, les développer, les argumenter, gérer des incertitudes … voici des tâches astreignantes auxquelles il n'est pas facile de convier les apprenants, parfois réticents à sortir des habitudes, du train-train quotidien, des routines sécurisantes du savoir “clé sur porte”, à prendre en charge des activités “normalement dévolues au professeur”.

Les seconds manifestent parfois la crainte de perdre le contrôle des opérations, de s'engager dans des voies dont ils “savent” l'inopportunité, l'inadéquation, de perdre un temps précieux, de voir leurs certitudes chanceler … finalement de se sentir dépossédés, désinvestis de leur fonction. Nous nous demandons, avec Ph. Marton[29], si ces craintes et ces résistances ne doivent pas être attribuées à la faiblesse des aspects pédagogiques et méthodologiques de la formation donnée à ceux qui se préparaient - alors encore apprenants pour la société complexe - à devenir les “professionnels” de l'enseignement.

---

[29] Ph. MARTON, ***La formation et le perfectionnement des maîtres aux nouvelles technologies de l'information et de la communication*** In L. Sauvé (Ed.), 1992 ; *La technologie éducative d'hier à demain,* Actes du VIII Colloque du Conseil interinstitutionnel pour le progrès de la technologie éducative, Québec, 1992, pp. 255-260.

Ne s'agit-il pas là, pour les uns et les autres, de ces points de rupture, de ces tierces places, dont parle M. Serres[30], dans lesquelles l'apprenant et l'enseignant s'exposent et s'investissent, dans lesquelles les certitudes se dissolvent, se régénèrent … un tiers-instruit ou encore un tiers-éduqué ?

Des modes d'application réalistes et adaptables sont possibles ; à titre d'exemple, nous soulignons :

* le rôle des exercices, travaux pratiques, projets personnels ou de groupe, etc., qui offrent plus de place à l'apport personnel de l'étudiant ;

* l'utilisation pédagogique de l'ordinateur, des multimédia, etc., et de leurs propriétés dynamiques permettant la recherche par essai-erreur, le questionnement préalable et nécessaire à l'élaboration de réponses ;

* l'ouverture à des activités “transversales” (par exemple, l'utilisation des outils bureautiques, base de données, traitement de textes, tableurs …, la recherche documentaire …) par lesquelles l'étudiant puisse aborder non seulement des contenus mais aussi faire l'expérience des démarches, des méthodes, des questionnements, des incertitudes, des “va-et-vient”, etc., qui accompagnent toute tentative de modélisation, toute recherche, toute construction des sciences ;

* des critères et des pratiques d'évaluation cohérentes avec les objectifs envisagés ; la promotion des compétences transversales s'accorde mal avec des méthodes d'évaluation qui se réduisent à une mesure ponctuelle (“l'examen”) d'un savoir redit.

Si l'enseignant, le médiateur, le média peuvent convier l'apprenant au voyage, c'est l'apprenant lui-même qui va voyager, qui tôt ou tard va devoir sortir de l'école.

La métaphore suivante illustrera notre propos : le passage par l'auto-école s'avère indispensable pour apprendre l'outil (la voiture), les règles de

---

30 M. SERRES, ***Le Tiers-Instruit,*** Paris : Francois Bourin, 1991.

la circulation (le code), les savoir-faire et savoirs exercés dans un contexte artificiel ou simulé. Un des buts de cet apprentissage “accompagné” est aussi de permettre au conducteur de savoir-être (le code n'exclut pas la courtoisie …) et de savoir-devenir (faire face à des aléas, à des situations imprévues …) sur le terrain réel de nos campagnes et de nos grandes cités. Bien au-delà des connaissances sur le véhicule et sur le code, au-delà aussi de son savoir-faire de conducteur, l'apprenant devra être capable d'exercer de multiples compétences transversales toutes significatives de la manière dont l'outil, son véhicule, s'est intégré dans le tissu complexe de la société : identifier ses besoins, choisir un véhicule, accomplir les formalités pour le faire immatriculer et assurer mais aussi l'utiliser rationnellement, savoir y renoncer, garder le goût pour les promenades champêtres et surtout prendre conscience de ses responsabilités et les assumer.

**L'exercice de ces compétences transversales est rendu possible par les outils interactifs qui illuminent le savoir en le faisant sortir de l'école, en le vivifiant par la mise en contraste, en contexte, en relation. Pourront-ils enfin permettre aux êtres de mieux savoir, vivre et devenir, en un mot, de s'éduquer dans la société complexe ?**

## 22. Aux médias

*Par leurs caractéristiques d'interactivité exploitées dans l'interaction de la situation pédagogique, les médias constituent un terrain fertile pour éveiller, exercer, développer et promouvoir les compétences transversales nécessaires pour s'éduquer dans une interaction constructive avec la société complexe.*

La définition usuelle de média “tout support de diffusion massive de l'information” (dictionnaire Petit Robert, 1991) ne peut nous satisfaire pour différentes raisons que nous avons déjà abordées : information ne rime ni avec formation ni avec éducation, diffusion massive ne rime pas avec enseignement de qualité ; support d'apprentissage ne rime pas avec apprentissage de l'apprenant. Il ne s'agit pas pour nous de dresser ici la liste de tous les outils existants et de leurs caractéristiques techniques ; nous

renvoyons le lecteur à des ouvrages récents[31] qui les décrivent en analysant les particularités dont il est important de tenir compte dans le choix du support.

Ce que nous voulons faire est de voir à quelles conditions ces différents outils, porteurs d'informations, peuvent être aussi des outils d'éducation. A ce propos, comme nous l'avons dit, il est opportun de situer les médias dans la relation didactique, en y actualisant leurs différentes potentialités :

* une possibilité de prendre en compte ou de partir des intuitions, des conceptions implicites, des expériences antérieures de l'apprenant afin de les faire évoluer ;

* un regard, une lecture et une écoute pluriels et démultipliés sur les savoirs ;

* une occasion de reconstruction personnelle des savoirs, des processus qui les ont fait naître, des processus qu'ils permettent de mettre en place ;

* une actualisation des savoirs dans le contexte large (scientifique, économique… mais aussi de la vie quotidienne) dont ils sont issus et qu'ils déterminent ;

* un exercice de compétences transversales opérant sur les multiples dimensions (fonctionnelle, relationnelle …) de ces savoirs ;

* un auto-développement de comportements et d'attitudes permettant de mieux être, mieux vivre, mieux devenir dans la société complexe.

Ces opportunités didactiques (loin des dichotomies apparentes liées aux taxonomies, nous insistons sur leur nécessaire complémentarité) scandent à nouveau la progression de plus en plus intégrative que nous avons décrite autour de la figure 1 : **de la fonctionnalité** de l'outil qui donne accès aux

---

31 Par exemple : R. A. SCHWIER, & E. R. MISANCHUK, ***Interactive Multimedia Instruction,*** 1993.

informations et aux connaissances et qui incite à les **reconstruire jusqu'à la perspective relationnelle** dans laquelle ces savoirs et habiletés prennent sens et contribuent ainsi à l'édification du projet de la personne.

Ces potentialités des médias rejoignent des caractéristiques de situations pédagogiques qui favorisent l'apprentissage : à la frontière des théories constructivistes, cognitivistes et développementalistes, elles sont des constituants de ce qui est appelé dans la littérature anglo-saxonne "*situated learning*" ou encore "*anchored instruction*"[32].

## 23. Conclusion

Les médias constituent ainsi un haut lieu d'interactivité potentielle entre les diverses composantes, toutes complexes, que nous avons évoquées : savoirs et éducation, société et relations.

Cependant ces potentiels ne peuvent se révéler et s'actualiser par l'outil seul. Les craintes démesurées exprimées par les enseignants sur le fait que l'ordinateur puisse les remplacer, les espoirs fous que l'apprenant puisse enfin pouvoir apprendre tout seul, manifestent la puissance surfaite, quasi animiste à laquelle l'outil ne peut prétendre.

Loin des tendances d'écartèlement des pôles du triangle didactique - savoir tout puissant, enseignant dépossédé, apprenant enfin autonome - nous pensons plutôt aux médias comme un "**facteur de dialogue**" entre ces pôles. C'est ainsi que nous avons complété le concept d'interactivité fonctionnelle de l'outil par celui de l'interactivité relationnelle des partenaires de la relation didactique.

Le contenu d'information - issu de la société complexe et de ses savoirs - n'est plus que le substrat sur lequel s'appuient et se développent les savoirs et savoir-faire des apprenants dans une relation éducative qui accentue les

---

[32] D. M. GAYESKI, ***Multimedia for Learning : Development, Application, Evaluation,*** Englewood Cliffs, 1993 ; New Jersey : Educational Technology Publications ; CTGV *The Cognition and Technology Group at Vanderbilt,* 1993, Anchored Instruction and Situated Cognition Revisited. ***Educational Technology 3,*** pp. 52-70.

savoir-être et savoir-devenir, porte ouverte sur le mieux-vivre dans la société complexe.

Au carrefour de ces dimensions différentes mais toutes présentes dans l'expérience personnelle et interpersonnelle, les médias constituent un terrain fertile pour éveiller, exercer, développer et promouvoir des compétences transversales. Ces dernières, comme nous l'avons vu, sont nécessaires pour que l'apprenant puisse se re-construire l'articulation dynamique des différents savoirs et continuer ainsi à s'éduquer dans une interaction constructive avec la société complexe par le truchement des outils qu'elle lui propose.

**A la vision entropique de la société complexe nous proposons ainsi une vision néguentropique de l'éducation.**

# Transmission des savoirs et régulation

**Dominique VERPOORTEN**

**Faculté de Communication, Université Catholique de Louvain-La-Neuve**

> *Il existe un marché du savoir comme il existe un marché des matières premières, un marché des technologies, un marché des biens et services, un marché financier, un marché du travail. Le terme marché doit être pris ici au sens noble de milieu d'échanges d'informations en permanentes interactions. Comme en tout marché, aux signaux d'interactions qui résultent de la compétition doivent s'ajouter des contraintes fortes exprimées par les règles du jeu dont la puissance publique est responsable. Ces règles doivent tenir compte aujourd'hui du fait que le marché du savoir n'est plan national mais mondial* (A. DANZIN, *La croissance autrement*).

## 24. Introduction

Ce document de travail vise à offrir une première mise en lumière des processus de déformalisation des lieux, des temps, des objectifs, des outils, des méthodes, des évaluations et des acteurs qui ont cours actuellement au sein du secteur de la formation, de l'enseignement et de l'éducation.

Pour nous donner une chance de tenir au-dessus de ce gouffre de complexité et de perplexités, notre fil conducteur sera celui des Applications Pédagogiques des Technologies de l'Information (APTI). Nous voyons ces dernières comme un levier d'interrogation, un point d'entrée au

sein d'un domaine de spéculation plus vaste qui touche à la transmission du savoir et aux relations qu'entretient celle-ci avec la forme du lien social au sein des sociétés post-industrielles. Nous ne pouvons donc que souscrire à l'idée de ce "réexamen complet" que l'OCDE appelle de ses voeux et y inscrire notre démarche et notre travail.

> *La révolution de l'information offre de nouvelles possibilités dans l'enseignement comme dans d'autres secteurs de la société. En vérité, elle a un caractère universel qui justifie un réexamen complet des programmes d'études relatifs aux connaissances de base. Etant donné que les nouvelles technologies de l'information offrent de nouvelles perspectives pour l'enseignement et l'apprentissage, ce réexamen devrait englober également l'organisation des systèmes scolaires et des classes, ainsi que le contenu et les buts de la scolarisation* (OCDE, *Technologies de l'information et apprentissage de base*).

## ***Plan de l'exposé***

Il existe donc selon nous un sens et un intérêt à amorcer une réflexion couplant des questions de régulation à des questions de technologies de l'éducation. Ce sens et cet intérêt seront évoqués à trois niveaux.

1) La classe dans sa vie quotidienne constitue en elle-même un niveau de régulation à part entière. Le recours à des instruments comme l'ordinateur ou le multimédia y modifie la nature des relations entre l'enseignant, l'élève et le savoir. Le présent document visant plutôt à tester l'intégration de la question éducative au sein de l'appareil d'hypothèses forgé par le centre, nous n'aborderons pas ici ce niveau. Une recherche sur le terrain, dès le mois d'octobre, lui sera spécifiquement dévolue.

2) Le second niveau touche au système éducatif institutionalisé dans son ensemble et dans ses relations avec les différents acteurs qui entendent faire valoir des prétentions à son égard. Cette

réflexion prend place au sein d'un champ beaucoup plus vaste qui concerne les relations de l'école avec la société.

3) Les nouveaux lieux d'apprentissage constituent un troisième niveau. Ils témoignent d'une déformalisation massive du secteur éducatif qui est sorti du “modèle de la chasse gardée” étatique. Il n'est pas possible actuellement de préciser les relations que ces nouveaux foyers de transmission seront appelés à jouer avec le second niveau. C'est dans le tissage de ces relations que la puissance publique aura sans doute un rôle déterminant à jouer, au sein de ce que d'aucuns nomment déjà la “learning society”. Ce troisième niveau intègre des notions de gestion non standardisées, contrairement au niveau 2 qui développe une perspective en termes de régulation instituée. Ce niveau est également propre à interroger le rapport de l'individu aux diverses matrices d'apprentissage qui lui sont proposées.

Il nous paraît prématuré de nous lancer dans une réflexion sur les formes de contraintes de service public qui pourraient avoir cours dans le domaine des APTI. Nous préférons à ce stade procéder à un défrichage sociologique et à un premier détour par les questions de normativité, qui, à défaut de déboucher sur des recommandations concrètes sont au moins susceptibles de “cartographier les enjeux”.

Nous présenterons tout d'abord le discours général que tient l'Union Européenne au sujet de ces APTI. Nous tâcherons de le relier aux modèles de légitimation auxquels il s'alimente. Nous verrons ensuite en quoi la réalisation pratique de ce discours est susceptible de modifier la donnée actuelle en matière de systèmes éducatifs. Enfin, nous baliserons le terrain très partiellement défriché de quelques interrogations relatives aux conséquences possibles de ces transformations sur le rôle de l'Etat et sur l'organisation pratique de la réflexion normative en matière d'éducation.

## 25. Le discours de l'Union : le "gap" et le "challenge"

En dehors de quelques travaux ponctuels portant sur des aspects particuliers du processus éducatif, la première étude d'envergure menée, à l'échelon spécifiquement européen, sur les transformations de l'éducation et de la formation date de 1987-1988. Elle est l'oeuvre de la European Round Table of Industrialists. Partant du point de vue des industriels, cette étude se donne pour tâche d'identifier les problèmes principaux liés à l'éducation et à la formation en Europe. Une partie du rapport est consacrée à une réflexion sur les possibilités qu'ouvrent en ce domaine les technologies de l'information.

### 25.1 Les prétentions de la sphère économique

Le principe d'un regard porté sur l'éducation à partir de l'instance du marché ainsi que le lancinant appel à l'utilisation des APTI pour combler le "gap" entre la demande et l'offre de formation vont se retrouver dans les rapports ultérieurs : Irdac, Panel Report, EETI, Delta, Idate, Review Board Report, etc ... Ceux-ci déclinent à peu de choses prêt le même discours programmatique[1] dont nous présentons la structure dans ce paragraphe.

Le discours européen sur les APTI fait de l'alignement sur le marché la prémisse et la conclusion de son raisonnement. Ce n'est pas tellement qu'il y ait eu appropriation sauvage du terrain de réflexion par la sphère économique et industrielle ; simplement, l'éducation constitue un terrain déserté par les visions d'ensemble et, en l'absence d'autres "prétendants", le marché s'efforce de suggérer à l'enseignement des objectifs qui rentrent dans sa logique et servent son fonctionnement. Ces objectifs, qui consistent

[1] Si ces rapports s'alignent les uns sur les autres, leur propos entre aussi en forte résonnance avec le discours tenu dans le document américain du Computer System Policy Project qui s'assigne pour tâche de baliser le développement de l'industrie nationale de l'information et qui consacre un chapitre aux potentialités des télécoms "nouvelle mouture" en matière d'éducation.

globalement en une “optimalisation des ressources humaines”[2], font par ailleurs classiquement partie des missions conférées à l'éducation, si ce n'est que, ici, elles ne paraissent plus avoir aucun contre-poids. Ceci trouve son origine dans la désaffectation des projets d'éducation reposant sur les deux métarécits identifiés par J.F. LYOTARD : *l'émancipation du citoyen et la réalisation de l'Esprit* (encore qu'on en puisse observer la résurgence dans certains aspects du programme européen). Reste donc, comme “ressource d'horizon”, la performativité généralisée qui, invoquée dans le cadre d'une conception systémique de la société, conduit à faire de l'enseignement un sous-système, vis-à-vis duquel le sous-système économique manifeste des vélléités de “capture”.

> *The education and training system must play a significant role in meeting the needs of european industry for a highly skilled workforce* (Telematics RTD panel report).

> *Competitive advantage can be gained by raising employees level of education and thus their competence* (5th Review Board DG XIII).

Les prétentions de l'industrie à intervenir dans la sphère éducative se légitiment donc de la liaison établie et constamment invoquée entre

2 Ces prétentions de l'industrie sont partiellement légitimes. Elle estime devoir insister sur la "formation à la vie réelle". Toutefois, cette dernière ne se limite pas à un contenu unilatéral lié à l'acquisition de compétences professionnelle. Reste donc la question d'une éducation tenant compte d'autres formes de légitimation.

amélioration de l'éducation et maintien de la productivité européenne[3] portée par une industrie de plus en plus “knowledge intensive”. L'insistance est donc portée sur l'intégration de l'éducation à un “défi” industriel qu'elle doit à la fois porter et sur lequel elle doit en même temps s'aligner.

## 25.2 Les technologies pour l'éducation

Un des leviers majeurs de cette adaptation de l'éducation aux nouveaux besoins est l'intégration des nouvelles technologies dans le processus d'enseignement.

> *The essential social aim of the telematics in education and training programme is to widen acces to advanced learning services and to increase their effectiveness. The telecommunications infrastructures trough which these services are provided should therefore be responsive to individual learnings needs and specific users groups : SME, experts and teleworkers* (ERT, *Education and european competence*).

L'éducation est d'emblée pensée selon un spectre très large qui déborde de loin les lieux et les méthodes d'enseignement tels que l'Europe les a développés depuis 500 ans. Le mouvement procède d'une déformalisation du monde éducatif par une délocalisation des savoirs et une multiplication des lieux de transmission.

---

[3] Cette tendance est déjà stigmatisée par F. NIETZSCHE, dans la *Première conférence sur l'avenir de nos établissements d'enseignement*. Elle entraîne, selon lui, une extension (néfaste) de la culture : *Cette extension est l'un des dogmes d'économie politique les plus chers au temps présent. Autant de connaisssance et de culture que possible - donc autant de production et de besoins que possible -, donc autant de bonheur que possible - voilà à peu près la formule. Cette direction pourrait à peu près définir la culture comme le discernement grâce auquel on se tient "au sommet de son époque", grâce auquel on connaît tous les chemins qui permettent de gagner de l'argent, grâce auquel on possède tous les moyens par lesquels passe le commerce entre les hommes et entre les peuples. La véritable tâche de la culture serait alors de créer des hommes aussi "courants" que possible, un peu comme on parle d'une "monnaie courante".*

### 25.3 “Lifelong learning education” et télécoms

L'évocation de la transformation actuelle est chapeautée par un concept de “lifelong learning education” qui devient le “sésame ouvre-toi” de la compétitivité retrouvée et donc du maintien du bien être de 330 millions d'Européens[4]. Entre l'enseignement reçu dans des établissements relevant de la sphère publique et l'apprentissage en autodidacte dans la sphère privée viennent s'interposer un maillage de demandeurs et d'offreurs de connaissances qui contribuent à faire de celle-ci un produit ou un service et de l'éducation un marché ; marché qui se développera partiellement en synergie avec les réseaux de télécommunication.

> *Learning infrastructures should build upon and be embedded within existing and emerging multiple purpose telematic infrastructures* (Delta, *Information technologies and telecommunications for education and training*).

Le discours sur les APTI reprend ici à son compte les insistances qui ont prévalu en matière d'accès au réseau. Le réquisitoire se présente toutefois comme légèrement décalé par rapport à la problématique générale des télécoms car, déjà, on a assimilé l'éducation télématique à un service. L'UE réfléchit en ce domaine, au-delà de la notion de service universel reprise dans son acception technologique, et cela, dans la droite ligne de l'évolution anticipée par la cellule Telecom.

> *La notion de service, alors limitée à la fourniture de capacités sur le réseau, doit s'orienter vers la satisfaction de demandes nouvelles exprimées par le marché* (Cellule Telecom, note de synthèse).

---

4 L'idée qu'un système d'enseignement puisse correspondre à la réussite humaine d'une population n'est pas pour autant complètement évacué : *We refuse a European competitiveness model based on low wages and low skills. Therefore, the only valid alternative for Europe to survive and to remain competitive in world markets lies in a strong capacity for innovation and quality. This can only be achieved with a highly and broadly skilled workforce* (IRDAC, Quality and relevance, the challenge to European Education).

C'est à ce point que l'on commence à danser d'un pied sur l'autre. La mutation quantitative et qualitative réclamée pour l'éducation est issue de deux sphères de normativité différente. Le discours prend une configuration d'entrelacement. Le premier fil en est la classique préoccupation fonctionaliste de l'accès qui rejoint, par le détour de la motivation individuelle à s'instruire (et l'on sent les différents rapporteurs à la fois très préoccupés et très perplexes devant cette question qui appelle une "construction de la demande") rejoint les préoccupations vis-à-vis du maintien de la compétitivité. Cette perspective induit les insistances sur les "relevant training information readily available", les "on-line facilities", les "just-in-time" programmes of instruction.

A côté de cela, on relève des amorces d'un discours sur les APTI qui réactive le métarécit de la démocratisation de l'enseignement et de l'émancipation par le droit à l'éducation[5] : discours sur les "disabled", les "remote regions" et les "far reaching potential learners".

> *Can telematics based learning be provided at a cost affordable to all learners and not just large organisations ? Can equality of access be extended to all European citizens, and not just to those in favoured locations ? In the European context, the transnational telecom tarifs play an important role in supporting new and wider applications in DET or in obstructing them. More tansparency is asked as far as the telephone service and the leased lines are concerned, because they might be the basic telematic infrastructure for the exchange between ressource and study centres and for the delivery and tutoring*

[5] Finalement, l'approche la moins mise en valeur est celle qui concerne le rapport de la socialisation à la citoyenneté, terrain dont André Berten, JM Ferry et la ERT ont commencé le "déminage". Les Etats-Unis sont les seuls à mettre d'emblée en rapport la question de l'accès et celle de la recherche d'une citoyenneté informée, requérant l'accès aux TI. Le dernier rapport de la ERT revalorise aussi cet aspect de la question. La cellule Télécom itou : *L'accès à l'information devient un droit de l'homme. Il est un droit pour chaque citoyen. La cohésion sociale tant au niveau du contexte national qu'à l'échelle mondiale requiert que tous les citoyens, où qu'ils vivent, puissent bénéficier des plus essentiels services de l'information à un prix abordable.*

*in rural and remote regions* (Review Board Report, *Information and telecommunication technologies applied to education and training*).

### 25.4 Discours différents pour programme semblable

Quoiqu'il en soit, et dans tous les cas de figure des discours de légitimation, le programme des applications reste inchangé. Qu'il s'agisse de l'objectif fonctionnel lié au fonctionnement du marché ou de l'objectif démocratique lié au partage de l'espace public télématique, l'injonction est à la réalisation d'une mise à disposition de tous des ressources des TI “at any time, whenever and wherever it is required”.

## 26. Ecole, Etat et TI

Voyons à présent, et dans un mouvement qui nous rapproche d'hypothèses énoncées en termes de régulation, à quelles transformations l'évolution actuelle des modes et des lieux de transmission des savoirs expose les pouvoirs publics.

### 26.1 Les écoles sont-elles des institutions qui fonctionnent finalement sur une logique du contrat ou bien accomplissent-elles nécessairement une mission de service public qui les écartent de ce type de normativité ?

En premier lieu, on peut remarquer que les différents rédacteurs des rapports sur l'éducation et l'enseignement ont conscience de la limite de leur champ de manoeuvre. A part la ERT qui s'aventure, dans des recommandations générales, faites aux Etats au sujet de leurs réseaux nationaux d'enseignement, les autres rapports contournent ces pouvoirs et focalisent les discours relatifs aux APTI et à leur extension sur trois types d'apprenants : “autonomous learners in higher education”, “workers in SME”, and “highly skilled professionals”.

Au niveau de l'enseignement de base, ils se contentent pour la plupart de souligner que l'introduction des nouveaux outils technologiques serait une bonne familiarisation avec l'environnement professionnel et qu'il faudrait améliorer les performances de l'enseignement de base car, de sa qualité dépend la capacité de l'individu à entrer dans des schèmes de formation continue.

Les rapporteurs évitent donc de s'enferrer dans un débat sur les missions de l'école, devenues floues et favorisent une stratégie de contournement par la bande des Etats et de leurs prérogatives en matière d'enseignement, contournement auxquels se prêtent les nouvelles technologies. Le questionnement qui se profile là derrière, et qui n'est que très rarement abordé, est celui des différentes matrices de socialisation et des conséquences sur l'existence sociétale d'une déformalisation générale des modalités de l'apprentissage. Le monde économique estime aujourd'hui qu'il est de son devoir d'en prendre une partie en charge (et il est étonnant de constater une résurgence dans cet environnement d'un comportement qu'on aurait peut-être qualifié de “paternaliste” au 19ème siècle. A moins que les rapports éducation-industrie ne se donnent la forme du sponsoring) :

> *Industrial culture is not presented in the school systems. Because education and training have not been able to adapt to all the changes in the business environment and the needs of business life, industry has been recently forced to take a bigger responsibilité for training. The whole field of education and training should be changing radically. This should be met by a shift in the allocation of public ressources used in education and training. In most European countries, education administration is heavily centralized, which creates bureaucracy and inflexibility in practice and even prohibits renewal. The needs of business life and industry are not respected enough and the fixed interaction mechanism between business life and education is missing* (ERT, *Education and European competence*).

D'un côté, les industriels se disent forcés à mettre en place des procédures de qualification de leur personnel. D'un autre côté, on peut supposer qu'ils souhaiteraient se décharger au maximum des coûts afférents à l'éducation sur les structures publiques. La transformation oblige à repenser la question du coût et des contributions respectives des secteurs publics et privés.

### 26.2 Qu'implique, pour l'organisation de l'espace public démocratique, une extension du droit de regard d'agents extérieurs sur la sphère éducative ?

Dans le domaine de la transmission des connaissances, on observe une volonté d'intégration croissante savoir/technique/économie. Il s'agit d'un phénomène qui a de fortes implications relativement à la signification socialement instituée du savoir : l'école n'a plus le monopole en matière éducative. Les Etats se voient confrontés à une décentralisation générale du système scolaire. La porte est ouverte à d'autres modèles d'apprentissage. La télématique ouvre un marché de l'éducation qui risque fort d'entrer directement en concurrence avec l'école. Le souci grandissant de l'adéquation formation-emploi contribue à la dépossession par l'Etat de son monopole car, à première vue, qui peut mieux assumer cette adéquation que les offreurs d'emploi eux-mêmes ? L'education peut désormais s'envisager comme un projet d'entreprise et comme un projet de société. Dans ce kaleidoscope en gestation, la question de l'éducation commune se repose, ainsi que la spécificité de la contribution des nouveaux acteurs au processus éducatif général.

> *If we reason in terms of lifelong learning, the various educational programs become more interdependant. They will have progressively to be part of a system. Those who practise or manage education should not only be concerned by one segment but also by the others segments that form an integrated system. A systemic approach is necessary if Europe wants to create lifelong opportunities. Each element of the "Education Chain" will influence all the others. The quality of the chain will be that of the*

*weakest link*[6] (P. COCHINAUX & P. de WOOT, *Moving towards a learning society*).

A quoi “obligent” les insistances du monde industriel ? Quid de la responsabilité sociale des milieux économique en matière d'éducation ? L'établissement d'une communauté de destin entre l'école et l'industrie doit-elle uniquement se légitimer du principe du marché ? Comment la question de la concurrence se pose-t-elle sur un marché de l'éducation ? Quelle répartition de quelles tâches entre public et privé ?

### 26.3 Le service éducatif bat-il en brêche l'idée d'un service public en matière d'éducation ? Que signifie une communication et une éducation sous forme de marché à large éventail offert au choix du consommateur ?

Nous voulons absolument éviter ce que J.M. FERRY nomme la “métaphore du siège”, c'est-à-dire un discours d'urgence et d'angoisse fondé sur l'idée d'une menace imminente sur un objet précieux. L'industrie n'est pas un ogre qui veut avaler tout rond le secteur éducatif. Elle est simplement un pouvoir qui entend s'intégrer à la définition des objectifs éducatifs et du rapport entre le savoir et la communauté. A côté de l'interdisciplinarité que réclame l'organisation du savoir sur ses nouveaux supports, on voit se profiler le besoin de canaux de discussion entre le secteur privé et les agents publics de manière à organiser les prétentions de chacun au sujet de l'enseignement.

*S'il reste des nostalgiques de l'élitisme républicain, ou de la valeur universelle de certains*

---

[6]Il s'agit là d'une vision humaniste sur l'éducation dérivant sans doute de ce que les auteurs désignent comme *a European blend of capitalism*. Dans un rapport antérieur de la ERT Education working group, on trouve l'évocation d'une autre manière de concevoir le système : *European education is aimed at removing weaknesses, whereas in the United States the emphasis has been on intensifying and bringing out one's strenghts. Latter approach is necessary to motivate for learning.*

> *savoirs auxquels on accède par la seule abstraction émancipatrice, si certains espéraient encore, il y a quelques années, mobiliser les forces sociales autour d'un projet alternatif de société et d'école contre le socialisme gestionnaire et le libéralisme, la plupart des réthoriques réformatrices actuelles en matière d'enseignement ne pensent pas le changement en termes radicaux. Elles l'envisagent plutôt comme une adaptation aux nouveaux publics qui se cotoient dans l'espace scolaire et s'y trouvent pour une durée de plus en plus longue, et comme une recentration de l'école sur ses missions propres par la passation de nouveaux compromis avec les groupes et les institutions qui s'occupent autrement de formation et de socialisation* (A. VAN HAECHT*, Les nouvelles manières de connaître*).

Attention. Intervenir de cette manière, c'est accepter l'introduction d'une normativité qui ne prenne pas naissance dans des structures formelles instituées une fois pour toutes. C'est procéder à l'institutionalisation de ressources de la société civile dont on ignore la teneur avant de provoquer le processus de leur explicitation, de leur confrontation et de leur rationalisation. C'est aussi reconnaître au monde vécu un fond dormant et potentiellement riche, remplissant une fonction d'équilibration systématique par rapport aux modèles de normativité.

Ces “consortiums de réflexion” auraient pour objectif de définir la mesure selon laquelle le changement social en matière d'éducation est censé s'aligner sur le changement industriel et technologique et dans quelle mesure il est normal qu'un système d'enseignement présente une certaine rigidité par rapport aux demandes d'appropriation dont il fait l'objet. Ce genre de lieux permettrait peut-être aussi de laisser s'exprimer un réalisme partagé qui s'accomoderait d'une éthique démocratique conciliant sens de l'utilité, souci de socialisation et processus de production de la citoyenneté.

> *Pour d'aucuns, l'école serait entrée dans une “période post-critique” depuis 1980 et il en serait*

> *résulté la nécessité d'une réflexion sur les valeurs, plus spécialement les valeurs communes qui peuvent guider le pilotage national de systèmes scolaires décentralisés et différenciés (JL. DEROUET, in A. VAN HAECHT).*

La définition de ce “pilotage national” convoque une interrogation sur les modes contemporains de socialisation. On socialise désormais à des choses différentes car il n'existe plus d'idée de la société comme un tout et l'on semble dans l'impossibilité de fixer un aboutissement à ce processus, excepté dans une perspective de la “constitution” d'un sujet “décentré”, d'une identité post-nationale (version philosophique et politique) ou dans une perspective de “configuration” du sujet aux exigences du système (version économico-industrielle). Cette problématique invite à s'interroger sur la contribution singulière de la sphère école dans le processus de socialisation et pose la question de la rupture ou de la continuité entre normativité scolaire et normativité professionelle ?

### 26.4 Comment développer des systèmes de “mise en phase” de l'offre et de la demande en matière d'APTI ? Faut-il étendre la définition du service universel au domaine de l'éducation télématique ?

Dans son rapport sur la société de l'information, le Conseil de l'Europe résume son projet par trois recommandations :

> *Fostering an entrepreneurial mentality - developping a common regulatory approach -no more public money, subsidies or protectionism.*

Dans ces circonstances, la volonté de déléguer au secteur privé le soin de faire profiter le systéme éducatif de la révolution télématique est clairement affirmée. Toutefois, il semble que les investissements dans ce domaine soient en régression.

> *Le marché du multimédia, longtemps attendu, est aujourd'hui une réalité : on l'estimait pour l'Europe,*

> *hardware et software confondus, à plus de 3 millions de dollars en 1992 ; les projections les plus optimistes atteignent les 40 millions de dollars pour 1996 (Inteco) ; selon Ovum, le marché des équipements proprement dits qui s'élevait en 1991 à 526.000 dollars pourrait atteindre plus de de 9 millions de dollars en 1997. Sur le plan de sa segmentation, il semble que les applications liées au marché éducatif et aux fonctions kiosques vont baisser au profit de la messagerie, le management de données, la domotique, les applications professionnelles. Ces marchés risquent d'être dominés par les fournisseurs nord-américains qui représentent aujourd'hui 75% de l'offre. Cette multiplicité des acteurs et leur dimension en terme industriel et de marché constitue une menace pour l'indépendance de l'Europe (*R. DELMAS*, La dimension européenne du multimédia).*

L'Etat devra sans doute encadrer le processus. La question se pose d'un environnement de régulation légale capable d'encourager le secteur privé à investir le domaine. Là encore, une réflexion centrée sur l'équipement technologique est une occasion de reposer la question du coût et des acteurs de l'éducation dans son ensemble.

> *Les moyens qu'il faudra mobiliser pour préparer la jeunesse aux défis du siècle prochain nécessitent une dilatation considérable des budgets du poste "Education-Post formations". L'ordre de grandeur à prévoir pour la période 2000-2020 est le doublement par rapport aux niveaux en vigueur entre 1970-1980. Jamais l'Etat ne parvien- dra à prélever par l'impôt le financement de la gratuité des enseignements dans un moment où les besoins de la justice, de l'immi-gration, des retraites et de la santé se montreront par ailleurs très exigeants. Il devient indispensable que les intéressés eux-mêmes, les familles et les*

*professions soient directement associés à l'alimen tation des flux financiers (...) La régulation des systèmes éducatifs ne pourra donc pas échapper à un cadre de contraintes communautaires décidées par concertation. A défaut, les contraintes résulteront de la concurrence sauvage pour les qualifications de la main d'oeuvre selon la loi d'un marché du savoir qui va se développer quoique l'on fasse (*A. DANZIN*, La croissance ? ).*

### 26.5 APTI : la victoire de l'autodidacte ?

On touche ici à la liaison entre apprentissage institutionalisé et apprentissage autonome. Quelles pourraient être les procédures de reconnaissance des autodidactes et des nouveaux canaux d'apprentissage qu'ils empruntent ? Se pose ici le contentieux lié à la délivrance des diplômes et la question des procédures d'évaluation de la qualité des apprentissages. Les auteurs des divers rapports regrettent à ce sujet le trop grand nombre d'examens différents qui nuit à une intégration européenne de l'éducation.

### 26.6 Quel compromis entre décentralisation et intégration ?

*Fondamentalement, l'introduction des nouvelles technologies de l'information dans l'éducation pose le problème de l'innovation dans les méthodes d'enseignements et les structures. Le domaine est une bonne illustration des règles de maîtrise de la complexité. On ne peut pas échapper au processus essai-erreur-correction d'erreur, ce qui implique une grande liberté accordée aux acteurs pour prendre des initiatives, émettre des hypothèses de travail, les confronter à l'expérience, les corriger selon les résultats et procéder par des améliorations successives dans une démarche qui comporte un*

> *grand nombre de tâtonnements. D'où la nécessité de structures qui donnent toutes leurs chances aux corrections cybernétiques.*

Puisque le mot d'ordre est à la flexibilité et à l'adaptation permanente, puisque les implantations massives des APTI dans le cadre de plans gouvernementaux ont toujours été décevantes, il vaut peut-être mieux changer de stratégie. D'une provocation du changement par règle formelle édictée à un niveau déterminé de pouvoir, il faut passer à une gestion des initiatives et des encouragements. Dans cette perspective, le mode de la fondation vaudrait une étude.

## 27. Conclusion

**Du service public au service du public. De l'accès au savoir à son appropriation.**

L'entrelacement entre les questions technologiques et les questions normatives et sociales est très serré dans les discussions relatives aux APTI. Qu'il soit utilisé dans un contexte pédagogique ou un autre, nous concevons l'ordinateur comme un mode d'accès inédit à des significations. Il laisse présager d'un rapport au monde vécu tourné vers la transmission et d'une transmission se vivant dans des structures permettant à chacun d'être l'enseignant ou l'enseigné de tous. Dans ce contexte, toute communication peut recevoir une valence d'édification, de “source” de savoir, notion dont la déformalisation s'alimente à la revalorisation du monde vécu, au travail massif des médias et à une crise de légitimité des lieux et des temps publics de l'éducation, on se dirige vers une conception des messages en termes de “denrées cognitives” (V. Engel) et de mise en forme de ces messages selon une pragmatique des particules de langage (J.F. Lyotard), qui justifient la recommandation “*de tout mettre en ouvre pour maintenir ouvertes les voies de communication, quel que soit le contenu de ce qui est communiqué*” (P. Breton et S. Proulx) et de “*favoriser l'accès de tous aux banques de données, appelées à devenir la nature de l'homme*” (J.F. LYOTARD).

Avec les APTI surgissent des interrogations plus fondamentales touchant aux modes d'organisation du rapport entre divers acteurs sociaux

liés par des prétentions sur la définition d'un objet social. Si, en matière d'enseignement, comme en beaucoup d'autres, on passe bel et bien du “service public au service du public”, et donc d'une conception de l'intérêt général qui transcende les singularités individuelles à une autre qui résulte de l'agrégation des intérêts privés, il s'agira, pour ces acteurs, de repenser ce que signifie “servir” dans cette nouvelle configuration. En matière de TI, la réflexion peut être menée au niveau des infrastructures. C'est tout le sens d'une démarche qui concerne la question de l'offre d'un service universel. Elle peut aussi s'orienter dans une perspective qualitative qui prendrait tout son sens en marquant la distinction entre l'accessibilité à un apprentissage et son appropriation effective. Et là, toute la question de l'école publique et de sa formation de base est reposée. Cette distinction entre accessibilité et appropriation empêche également le développement d'un faux égalitarisme se satisfaisant d'une réflexion sur les seules modalités formelles d'accès aux informations.

# Le réseau Info-Muse de la société des musées québécois

**Françoise SIMARD**

**Coordonnatrice du Réseau Info-Muse, Société des musées québécois**

## 28. L'origine

Le Réseau Info-Muse existe depuis six ans. Il a pour mission d'assurer la présence d'un réseau d'échange d'informations sur le patrimoine québécois, répondant aux besoins des institutions muséales et de la collectivité. Le réseau est chapeauté par la Société des Musées Québécois (SMQ), organisme associatif sans but lucratif voué a la promotion et au développement des institutions muséales. La SMQ est donc l'organe par excellence de circulation de l'information muséale. Elle compte plus de 1000 membres, dont 200 membres institutionnels.

Le Réseau Info-Muse est né de la volonté des membres de la SMQ de se regrouper pour former un réseau automatisé de partage d'informations. Devant cette volonté, la SMQ s'est associée au Réseau Canadien d'Information sur le Patrimoine (RCIP) pour mettre sur pied un service qui répondrait aux besoins des musées dans ce secteur. Un comité composé de professionnels provenant de différents musées intéressés par la gestion automatisée s'est formé en 1990 afin de poser les balises du réseau Info-Muse. Grâce à l'obtention de fonds du ministère du Patrimoine canadien et du ministère de la Culture et des Communications du Québec, et après un an de travail assidu, la SMQ était en mesure de procéder à l'engagement d'une équipe de travail.

Une belle histoire de collaboration commençait alors, amenant plusieurs dizaines d'organismes et de professionnels du milieu à participer à la mise sur pied et au développement du Réseau Info-Muse.

## 29. La mise en place

Tout d'abord, il fallait s'assurer que les institutions muséales parlent le même langage. Le premier mandat du Réseau fut donc de développer des outils de standardisation des contenus et des procédures de gestion de collections. Des formulaires permettant de consigner les renseignements de façon structurée furent conçus, ainsi qu'un Guide de documentation, donnant des renseignements sur la nature de l'information à consigner sur les fiches, et sur la façon d'enregistrer cette information. Un Guide de gestion des collections a ensuite été développé, présentant les différentes activités reliées a l'utilisation des objets dans un contexte muséal, avec pour objectif d'aider les gestionnaires à documenter de façon standardisée ces activités.

Puis, une formation a été mise sur pied, englobant toutes les étapes de l'orchestration d'un système documentaire à partir de la conceptualisation d'un projet de catalogage jusqu'aux techniques de normalisation du vocabulaire, dans l'optique d'automatiser les collections et de favoriser un échange d'information plus efficace. Par ailleurs, pour soutenir les institutions dans leur projet, Info-Muse dispense en continu des services conseils à ses usagers.

L'équipe du Réseau Info-Muse a également procède à une analyse approfondie de 25 logiciels spécialisés en gestion de collections. A la suite de cette étude, la SMQ a convenu de recommander les logiciels Micromusée et SNBase de la firme française Mobydoc. Ces logiciels sont munis d'un module d'exportation permettant de partager des données via la base de données commune.

## 30. L'autoroute de l'information et les nouvelles technologies

A l'aube de l'année 1995, il devint évident que pour assurer la survie et l'expansion du Réseau Info-Muse, celui-ci devait sans tarder prendre le virage technologique et conjuguer avec de nouveaux enjeux technologiques comme l'implantation de systèmes internationaux d'échange d'informations.

Ainsi, la SMQ se tourna-t-elle vers le Fonds de l'autoroute de l'information (FAI) afin d'aider les institutions muséales à emprunter la

bretelle d'accès à l'autoroute de l'information. Relevant du ministère de l'Industrie, du Commerce, de la Science et de la Technologie et du ministère de la Culture et des Communications du Québec, le FAI a été créé par le Gouvernement du Québec afin de stimuler les entreprises et les organismes à développer des infrastructures et des contenus québécois sur l'autoroute de l'information.

Le projet accepté en juillet 1995 s'échelonne sur trois ans et vise a permettre aux institutions muséales d'accéder a l'inforoute, d'une part en facilitant l'automatisation des collections, et d'autre part en leur permettant d'avoir accès à de l'information et de la partager via le Réseau Info-Muse.

### 30.1 L'informatisation des collections

Le partage d'information sur les collections à travers un réseau d'échange électronique passe évidemment par l'informatisation des données. La SMQ souhaite aider les musées à acquérir un système informatique afin de réaliser ce travail. Pour la SMQ l'autonomie des institutions au niveau de la gestion automatisée des collections est un principe très important. Alors que près de la moitié des musées du Québec ont déjà entrepris l'informatisation de leurs collections, plusieurs institutions régionales continuent à utiliser un système documentaire manuel. En plus de ralentir la vitesse (et donc la productivité) du travail quotidien de gestion des collections, le potentiel de diffusion du patrimoine est limite aux activités muséales traditionnelles (expositions et publications).

Le projet permettra d'aider 95 institutions a acquérir un logiciel de gestion de collections. L'argent alloué à chaque musée englobe le prix d'achat de la version allégée du logiciel recommande par la SMQ. Evidemment, le montant attribué à chaque institution est minimal et les institutions désirant acquérir une version plus élaborée devront débourser les coûts supplémentaires. Les institutions désirant s'équiper avec un autre logiciel que celui recommandé par la SMQ ont également droit à l'aide financière, dans la mesure ou elles s'engagent à télécharger des données dans la base commune.

### 30.2 La mise en réseau des institutions

L'étape deux du projet est la mise en réseau des institutions. Il s'agit de mettre sur pied une équipe volante pour procéder au branchement et à la formation in situ des institutions désirant accéder au Réseau Info-Muse. Cette équipe conseillera également les institutions pour l'achat de matériel de communication plus performant (modem, carte graphique, etc ...). La formation et le branchement in situ permettront d'éviter les frais de formation et de séjour du personnel muséal, qui peuvent être élevés pour les institutions des régions éloignées. Grâce a l'équipe volante, les frais à débourser par les participants se limitent à l'achat de matériel de communication. Le RCIP est un important partenaire puisqu'il assume les frais relies à la gestion technique de la base de données commune et offre gratuitement un compte accès Internet aux institutions qui contribuent aux bases de données communes.

### 30.3 Les résultats escomptés

En mettant en place l'infrastructure d'un réseau concerté de communication et d'échange d'informations muselle par voie électronique, la SMQ veut augmenter les échanges entre les centres urbains et les régions. La principale préoccupation de la SMQ est d'éviter la formation d'un réseau muséal à deux vitesses, dans lequel les institutions régionales seraient tenues a l'écart des nouvelles possibilités de diffusion et accès a l'information.

Si les institutions des grands centres urbains ont déjà réalisé en grande partie le catalogage et l'informatisation de leurs collections, celles situées en région manquent souvent de ressources pour réaliser un tel programme. Le projet vise à moderniser les modes de gestion et de diffusion de l'information, en aidant ces institutions à s'équiper de logiciels de gestion de collections, en formant leur personnel a l'utilisation des outils de mise en réseau et en dispensant des services conseil sur l'acquisition de produits et services reliés a l'inforoute.

En participant au Réseau Info-Muse, les institutions muséales pourront partager de l'information sur leurs collections via une base de données commune contenant des données exclusivement en français ; elles pourront

également accéder à des bases de données de référence en muséologie et à un service de messagerie électronique. Le projet de la SMQ permettra d'accroître le contenu francophone disponible sur l'autoroute de l'information et d'en faire une meilleure diffusion. Il aura pour conséquence d'augmenter le nombre de musées contribuant à la base de données et de hausser le nombre et la diversité des données relatives aux collections québécoises disponibles sur le réseau.

La diversification des voies d'accès et des modes de transmission de l'information améliorera la performance des musées au niveau de la diffusion, autant au Québec qu'au sein des réseaux internationaux, tout en permettant des économies substantielles au niveau des frais de communications. Ce projet aura un impact important sur l'implantation de procédures plus performantes et sur la professionnalisation des méthodes de travail dans les institutions muséales, notamment celles situées en région.

### 30.4 L'imagerie numerique

Sur les réseaux de transmission électronique comme l'Internet, l'image est le moyen par excellence pour capter rapidement l'attention des utilisateurs. Kodak Canada s'est associe à la SMQ pour participer au succès de l'intégration des musées québécois à l'inforoute, en favorisant l'adoption d'une méthodologie et de normes communes qui aideront les institutions dans leur démarche d'informatisation et de numérisation des collections. Grâce a cette collaboration, la SMQ produira un Guide d'informatisation et de numérisation des collections, suite logique à la démarche des deux autres guides du Réseau Info-Muse. De plus, Kodak offrira aux usagers du Réseau Info-Muse, à taux préférentiel, un premier disque compact (Photo C. D.) de leurs collections.

En trois ans, ce projet aura propulsé la communauté muséale québécoise sur l'autoroute de l'information. Le défi de cet important projet est sans contredit de toujours demeurer à l'écoute des besoins de base des institutions muséales, tout en faisant preuve de créativité et en demeurant à l'affût des nouvelles possibilités technologiques offertes aux membres.

Le succès d'une telle entreprise repose sur l'intérêt et le dynamisme de tous les intervenants, et sur la volonté des institutions muséales québécoises

de créer un véritable réseau de diffusion d'informations patrimoniale via l'autoroute de l'information.

At DAD, we provide
solutions to the challenges of
modern communication


# DIGITAL AGE DESIGN

# DEUXIEME PARTIE

# QUEL CADRE JURIDIQUE POUR INTERNET ?

Il y a ceux qui pensent que les nouvelles technologies créent des situations, des contentieux et des infractions juridiques inédits et réclament en conséquence un cadre légal et criminel nouveau et propre à la sphère des nouvelles technologies de l'information. Il y a ceux qui considèrent au contraire que les questions juridiques que posent les technologies de l'information peuvent se résoudre dans le cadre des textes existant en matière de protection de la vie privée, de droits d'auteurs ou d'atteinte à la pudeur. C'est ce débat qui est abordé dans cette seconde partie. Nous remercions ici particulièrement nos amis québecois pour l'apport qu'ils ont bien voulu, par leurs textes, apporter à cette réflexion dans le champ du droit.

# LES ACTIVITES INFORMATIONNELLES ILLICITES DANS LES NOUVEAUX ENVIRONNEMENTS ELECTRONIQUES

**Mylène BEAUPRE et Sophie HEIN[1]**

*L'intérêt que suscite les nouveaux environnements électroniques comme lieu d'échanges et de communication repose en partie sur la facilité avec laquelle il semble désormais possible d'accéder à une multitude d'informations sur tous les sujets. La circulation de l'information, dans un environnement comme l'Internet, apparaît plus libre que jamais. Cependant, l'exercice de la liberté d'expression a toujours été assorti de certaines limites et responsabilités. En fait, toutes les sociétés tolèrent un certain degré de "censure" dans leurs communications.*

*Pour les juristes, le défi soulevé par ces réseaux de communication "transfrontières" est majeur puisque l'État, comme acteur et véhicule du droit, semble y perdre en légitimité. Comment adapter le droit à ces nouveaux environnements ? Comment répond le droit aux inquiétudes manifestées à l'égard de la circulation de certaines informations, comme la pornographie ou les appels à la violence ? L'encadrement juridique actuel des diverses activités informationnelles se transpose-t-il aisément dans ces environnements électroniques ? Il s'agit de quelques-unes des questions abordées dans cette étude.*

---

[1]Mylène Beaupré, M. A. King's College, London et Sophie Hein, LL. M. Université de Montréal, sont agentes de recherche au Centre de recherche en droit public (C. R. D. P.) de l'Université de Montréal. Ce texte s'inscrit dans le cadre d'une étude en cours plus importante sur le cadre juridique des nouveaux environnements électroniques au Québec, dirigée par Pierre Trudel et financée par le Fonds Autoroute de l'Information du Gouvernement du Québec et le C. R. S. H.

## 31. Introduction

Les nouveaux environnements électroniques facilitent la circulation de l'information. Parce que ceux-ci se caractérisent par la convergence des techniques de communication traditionnelles, les distinctions entre les différents modes de communication apparaissent pour le moins fragiles. En effet, par exemple, l'incitation à la haine et les propos racistes n'ont pas la même portée selon qu'ils sont adressés à une seule personne, dans le contexte d'une conversation en face à face ou par téléphone, ou qu'ils sont l'objet d'une émission de télévision ou de radio. La différence est également importante selon que l'on soit en situation d'échange de lettres personnelles ou de publication dans un journal à grand tirage.

De plus, ce qui caractérise la communication par réseaux ou la création de sites de communication voués à de telles questions, c'est qu'il devient possible par une action relativement simple (aussi simple que la parole, et parfois aussi prompte) de transmettre son message à plusieurs centaines, voire des milliers de personnes à la fois. Un autre point caractéristique à ces nouveaux environnements est la difficulté de saisir le support du message ou d'en restreindre la circulation.

De façon plus précise, c'est un bilan des principales activités informationnelles qui, en vertu du droit québécois et canadien, constituent des activités illicites qui sera ici réalisé. Ces activités peuvent être divisées en quatre catégories : les activités qui corrompent les moeurs et portent atteinte à l'ordre public, celles qui portent atteinte à la dignité et à la sécurité des personnes, celles qui portent atteinte à la vie privée et enfin, les activités qui portent atteinte à la bonne administration de la justice.

Plusieurs instruments juridiques peuvent fonder l'illicéité de certaines activités qui ont lieu sur l'inforoute[2], mais le point de mire demeure le droit

[2]Le terme "inforoute" est utilisé pour désigner de façon générale les environnements électroniques où sont susceptibles de se développer des relations de communication. C'est la forme raccourcie de l'expression "autoroute de l'information", une traduction des *Information Highways* américaines.

criminel[3]. En ce sens, on abordera ici les questions relatives aux “services pour adultes” qui peuvent comprendre du matériel obscène, pornographique, violent ou indécent, les jeux (à l'argent), les communications harcelantes et les informations dangereuses, à caractère haineux, diffamatoire ou menaçant. Bref, cette étude vise principalement à recenser les différents crimes relatifs à la communication d’information et à soulever les questions qui resteront à analyser.

## 32. La liberté d’expression

En abordant le thème de l’illicéité des activités informationnelles, l’une des premières questions qui se posent concerne le contrôle de celles-ci sur les réseaux d’information. Il est en effet légitime de se demander si on a *“moralement le droit d'empêcher un individu de faire chez lui (c'est-à-dire sans causer de tort à personne) ce qu'il pourrait faire impunément en se rendant dans un autre pays ou dans un autre État ?”*[4]. Cette question situe la problématique centrale de la présente étude. L'élément du “tort” causé à la société ou à d'autres individus, par la circulation de certaines informations, notamment les personnes les plus vulnérables, comme les enfants, semble déterminant dans le contexte qui nous préoccupe. Un État peut-il légitimement venir dire à des individus ce qu'ils peuvent ou non faire ou regarder dans leur salon ? Surtout que dans le contexte de l'Internet, la relation de l'usager du réseau avec ses comparses en est essentiellement une de lecture ou de visualisation, d'écriture ou de création, bref de communication.

On pourrait penser, de façon générale, que les informations illicites sont celles qui portent atteinte à la dignité humaine, aux bonnes moeurs et à la morale, mais surtout, les activités seront illicites dans la mesure où elles sont prévues comme tel dans la loi. Le crime se définit cependant comme un *“manquement très grave à la morale ou à la loi”*[5].

---

[3]Le droit criminel relève de l'autorité législative fédérale et trouve sa principale source dans le *Code criminel*, LR. C. (1985), c. C-46, ci-après désigné "C. cr.".

[4]André SALWYN, *Les droits et libertés de l'internaute Le Devoir* , 3 mai 1995, B3.

[5]Petit Robert 1.

Or, parce que l'information est vivante, qu'elle est l'objet de la liberté d'expression et de communication reconnue à l'humain et garantie par la Constitution et les conventions internationales, elle semble plus difficilement pouvoir être considérée comme l'objet d'un crime. Cette question méritera sans doute d'être abordée plus en détail. En effet, elle nous place au coeur de la problématique du juste équilibre entre la garantie du droit à la liberté d'expression et la protection des intérêts collectifs, c'est-à-dire particulièrement la sécurité, la protection des valeurs morales et le respect de la dignité des personnes, des groupes et des peuples.

Plusieurs critères peuvent aider à qualifier le caractère dommageable de certaines informations. Ainsi, on peut se demander comment l'information est apparue à l'usager. Si l'information est apparue à l'écran, à la demande de l'usager, suite à un choix en fonction de ses propres intérêts, il apparaît pour le moins difficile pour l'État ou toute autre entité d'intervenir. En effet, dans ce cas, l'usager consent à ce que de telles informations lui soient rendues accessibles et en ce sens, il exerce en toute légitimité sa liberté de choix.

D'ailleurs, pour marquer d'un certain sceau contractuel l'accès à certaines informations, des fournisseurs d'informations mentionnent parfois à l'entrée de leur site la nature des informations qui y sont présentées, un peu à la manière de la catégorisation des films diffusés à la télévision. Une telle mention pourrait avoir également comme effet de protéger le gestionnaire du site d'informations en signifiant que si des gens y accèdent, cela est le fruit de leur propre volonté[6].

Si l'information illicite arrive à l'écran d'un usager par hasard, ou à la suite d'une interrogation par mots-clés, on peut certainement imaginer que, selon les valeurs propres à cet usager, l'information aura un impact différent. En outre, si l'accès à cette information se fait par courrier électronique, c'est-à-dire qu'un tiers envoie du courrier à un usager dont le contenu est qualifié d'illicite, deux situations peuvent être envisagées : celle où la transmission est faite suite à une manifestation préalable de l'intérêt de l'usager (abonnement), dans ce cas on pourrait reconnaître le consentement

[6]C'est d'ailleurs une pratique utilisée par les fournisseurs d'accès au matériel pornographique.

de l'usager et l'existence d'un certain rapport contractuel ; ou au contraire, si la transmission a été réalisée sans le consentement de l'usager, on pourra reconnaître plus aisément que des dommages peuvent résulter de cette transmission.

Une autre question intéressante liée à cette problématique est celle de l'opportunité de recourir au régime de responsabilité pénale ou criminelle plutôt qu'au régime de responsabilité civile lorsque des informations ont créé des dommages. Peu importe le régime choisi, il sera intéressant de s'interroger sur les critères à appliquer pour la qualification de l'information illicite : ceux du lieu de transmission ou ceux du lieu de réception ? Considérant le caractère international des réseaux de communication et la diversité des valeurs morales et culturelles, cette question se pose avec acuité.

Enfin, un élément déterminant dans l'évaluation des dommages ou du préjudice pouvant résulter de l'accès à certaines informations sera lié à la qualification de l'espace, public ou privé, où a lieu cet accès et du nombre de personnes qui peuvent y accéder[7].

Au Québec, la liberté d'expression fait l'objet d'une double garantie constitutionnelle et supra-législative, par le biais de l'article 2*b)* de la *Charte canadienne des droits et libertés*[8] et de l'article 3 de la *Charte des droits et libertés de la personne*[9]. Il ne peut être porté atteinte à ces droits que par une règle de droit qui soit justifiée dans une société libre et

---

[7]À cet égard, on peut se reporter à l'article de David J. GOLDSTONE, *The Public Forum Doctrine in the Age of the Information Superhighway (Where Are the Public Forums on the Information Superhighway ?),* 46 Hastings Law Journal, 1995, pp. 335-402.

[8]Chacun a la liberté d'expression, y compris la liberté de presse et des autres moyens de communication.. Selon l'interprétation dominante, le mot "expression" couvre "toutes les activités qui transmettent ou tentent de transmettre une signification, indépendamment de la nature du contenu de l'expression". Toutefois, dans *Dolphin Delivery*, la Cour aurait retenu *que la violence et les menaces de violence seraient exclus de la portection de l'al. 2b).*

[9]L. R. Q., c. C-12.

démocratique[10]. Les trois fondements à la liberté d'expression retenus au Canada sont *la recherche de la vérité* ; *la nécessité que les citoyens soient informés pour participer aux débats politiques et sociaux*, et enfin, *l'épanouissement individuel*[11].

Rappelons que la Charte canadienne ne peut être invoquée qu'à l'égard d'une action étatique ("governement or state action") et non à l'encontre de particuliers ou d'entreprises privées[12]. Toutefois, dans certaines circonstances, la Cour suprême du Canada a accepté d'examiner la constitutionnalité d'une règle de *common law*, invoquée dans un litige privé, par le biais de la pondération de principes et de valeurs[13].

L'application de la Charte canadienne sur les réseaux d'information est ainsi l'un des principaux défis auxquels le droit est aujourd'hui confronté. En effet, à ce jour, les universités ne sont pas considérées comme des acteurs gouvernementaux dont les règlements pouvaient tomber sous l'application de la *Charte*[14]. Or, celles-ci demeurent d'importants opérateurs de réseaux et jouent un rôle actif dans l'établissement de

---

[10]Texte de l'article premier, la clause limitative de la *Charte canadienne* (voir également art. 9. 1 de la Charte québécoise) :

> 1. La *Charte canadienne des droits et libertés* garantit les droits et libertés qui y sont énoncés. Ils ne peuvent être restreints que par une règle de droit, dans les limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique.

[11]Ces trois objectifs ont été énoncés par la Cour suprême la première fois dans l'affaire *Ford* c. *Procureur général du Québec*, [1988] 2 R. C. S. 712, 765-767 ; rappelés aussi dans *R. c. Zundel*, [1992] 2 R. C. S. 731, 752.

[12]Tel que prévu à l'article 32 de la *Charte canadienne* et interprété dans l'affaire *SDGMR* c. *Dolphin Delivery Ltd.,* [1986] 2 R. C. S. 573.

[13]Sur cette question on peut se reporter avec intérêt à l'affaire *Hill* c. *Église de Scientologie*, no 24216, 20 juillet 1995 ; accessible également à :

http://www.droit.umontreal.ca/CSC/arrets/recent/word/manning.fr.word

[14]Voir l'affaire *McKinney* c. *Université de Guelph*, [1990] 3 R. C. S. 229.

certaines règles de conduite sur les réseaux de communication desservant leurs étudiants. Le fait que les universités puissent s'engager dans des actions de censure pourrait modifier l'interprétation qui a été donnée jusqu'alors[15]. D'ailleurs, aux États-Unis, certaines actions des universités sont déjà qualifiées de "gouvernementales"[16].

Cependant, en ce qui concerne la *Charte des droits et libertés de la personne*, on sait que celle-ci peut être invoquée à l'encontre d'une partie privée, lorsqu'il y a atteinte à un droit garanti. D'ailleurs, cela donne à la Charte québécoise une effectivité à laquelle ne semble pas pouvoir aspirer la Charte canadienne. Le juge Sopinka a écrit à ce sujet :

> *Given that much of the world of electronic communications is controlled privately, without any governement regulation, the Charter may be an ineffective tool to protect this type of free speech*[17].

Ainsi, nous pensons que la Charte québécoise est en mesure de devenir un instrument efficace pour combler les lacunes de la Charte canadienne. Toutefois, on peut également envisager que cette dernière puisse recevoir une réinterprétation susceptible d'élargir son champ d'application pour couvrir les universités et peut-être même d'autres entités à caractère non gouvernemental.

En supposant que la liberté d'expression trouve son application dans les

---

[15] V. Hon. John SOPINKA, *Freedom of Speech and Privacy in the Information Age*, (November 26, 1994), *Symposium on Free Speech in the Information Age*, University of Waterloo, accessible à :

gopher://insight.mcmaster.ca:70/00/org/efc/doc/sfsp/sopinka

[16] *Ibid*. Le juge Sopinka cite entre autres les affaires suivantes : *Waters v. Churchill*, 114 S. Ct. 1878 (1994) ; *Gary E. Widmar et al. v. Clark Vincent et ali*, 454 U. S. 263 ; 102 S. Ct. 269 (1981) ; *Police Department of Chicago v. Mosley*, 408 U. S. 92 ; 92 S. Ct. 2286 (1972) ; *Cox v. Louisiana*, 379 U. S. 536 ; 85 S. Ct. 453 (1965) ; *Healy v. James*, 408 U. S. 169 ; 92 S. Ct. 2338 at 2345 (1972) ; *Tinker v. Des Moines Independent School District*, 393 U. S. 503 ; 89 S. Ct. 733 at 736.

[17] J. SOPINKA, précité, note 15.

réseaux d'information, puisqu'elle est consacrée dans plusieurs documents internationaux[18], on reconnaît aussi, du même coup, que toutes les sociétés tolèrent un certain degré de censure dans leurs communications. L'avènement de l'inforoute, par la facilité d'accéder à une vaste diversité de contenus, suscite un grand nombre de questions sur les limites de la tolérance de la population du Québec et de ses régions à l'égard de certains contenus. En effet, la notion de "crime" est intimement liée à ce qu'un groupe d'individus considère comme portant atteinte à l'équilibre social et à la sécurité individuelle et collective. Autrement dit, ce qui appartient au domaine du crime doit avoir été retiré de la sphère protégée de la liberté d'expression, pour des motifs sérieux[19].

Aux États-Unis, depuis les années'30, l'interprétation du Premier Amendement a été particulièrement réfractaire à une réglementation fondée sur le contenu du discours[20]. Dans l'affaire *Texas v. Johnson*, la Cour suprême américaine a rappelé que le "noyau dur du premier amendement, c'est que le gouvernement ne peut pas interdire l'expression d'une idée pour le seul motif que la société trouve celle-ci offensante ou désagréable"[21]. On exige donc un intérêt collectif important pour justifier la suppresion d'une liberté individuelle.

Dans un exposé sur la liberté d'expression et la protection de la vie

---

[18]Qu'il suffise de mentionner la *Déclaration universelle des droits de l'Homme* ou le *Pacte international relatif aux droits civils et politiques*..

[19]Voir notamment sur cette question l'article d'André VINCENT, *La liberté d'expression et les limitations imposées par l'État*, Développements récents en droit criminel *(1994)*, Cowansville, Éd. Yvon Blais, pp. 15 et suiv. L'auteur rappelle les différentes décisions importantes en cette matière entre 1989 et 1994.

[20]Voir sur l'histoire du Premier Amendement aux États-Unis, l'étude de David YASSKY, "*Eras of the First Amendment*" (1991) 91 *Colum. L. Rev.* 1699 ; il divise en trois périodes principales l'évolution de l'interprétation du Premier Amendement.

[21]Il s'agit d'une traduction personnelle de l'extrait suivant *: If there is a bedrock principle underlying the First Amendment, it is that the Government may not prohibit the expression of an idea simply because it is that the society finds the idea itself offensive or disagreeable* ; *Texas v. Johnson*, 109 S. Ct. 2533 (1989), 2544. Dans cette affaire, un individu avait été arrêté pour avoir brûlé le drapeau américain ; en défense, il invoque l'atteinte à sa liberté d'expression.

privée à l'heure de l'inforoute, le juge Sopinka estime que l'Internet est devenu l'affiche du siècle dernier[22], et qu'en ce sens, la facilité d'accès et d'expression à ce moyen de communication peut multiplier les cas de transmission d'informations obsènes ou à caractère haineux. Il écrit :

> *Computer networks allow individuals to publish almost anything behind a veil of virtual anonymity. Furthermore, systems operators themselves may find such material offensive and undesirable. Both of these factors raise the spectre of an increase in censorship of electronic mail as part of administrative policy and as a cautionary step to avoid potential civil or criminal liability. The consequences on free expression could be dramatic as the decision to allow or suppress certain forms of expression is left in the hands of the private organization or the university out of which the electronic mail originates. This places a tremendous amount of control over expression in the hands of the few. Does this problem of determining the source of the offensive e-mail justify prior censorship of the message ? Should the administrative organs in charge of e-mail systems be entitled to determine what others may or may not see ? How are we to ensure that the censorship merely extends to certain types of illegal expression and does not prohibit messages with which one simply disagrees or finds distasteful ? These are only some of the questions raised by free speech and e-mail.*[23]

Le droit criminel est un des modes de répression et de censure de certaines informations. Le choix de ce qui constitue un crime au Québec et au Canada appartient au Parlement fédéral, en vertu de l'article 91(27) de la

---

[22]Faisant ainsi référence à l'affaire *Ramsden* c. *Peterborough (Ville),* [1993] 2 R. C. S. 1084.

[23]J. SOPINKA, précité, note 15.

*Loi constitutionnelle de 1867*[24]. La Commission de réforme du droit du Canada a déjà souligné que le droit criminel ne devrait être utilisé qu'en dernier ressort. Trois conditions avaient alors été énoncées :

> *D'abord, l'action doit causer un tort, soit à d'autres personnes, soit à la société en général ou, dans des cas spéciaux, à ceux qui ont besoin qu'on les protège contre eux-mêmes. Ensuite, le tort qu'elle cause doit être grave. Enfin, le tort doit être d'un type pour lequel le remède le plus efficace est le droit pénal. Ces conditions limiteraient le droit pénal aux crimes de violence, de malhonnêteté et aux autres infractions qui ont toujours retenu l'attention des gens. Toutes les autres infractions qui, sans être véritablement répréhensibles, sont prohibées parce que cela constitue la meilleure façon de régler le problème qu'elles posent, ne doivent pas figurer au Code criminel. On doit les considérer seulement comme des quasi crimes ou des contraventions.*[25]

---

[24]Le droit criminel, c'est le droit pénal du gouvernement fédéral, c'est-à-dire une branche du droit public ayant pour objet de réglementer, par l'imposition d'une peine, la répression de comportements qui sont considérés comme portant atteinte à l'ordre social. Le droit pénal se distingue du droit civil sur plusieurs points. D'abord, le droit pénal cherche à punir la commission d'infractions dans l'objectif de prévenir d'autres comportements illicites ; c'est alors l'État qui assume les frais de la poursuite des infractions. Quant au droit civil, il vise essentiellement la réparation des dommages qu'a subis une personne suite à la commission d'actes fautifs.

[25]COMMISSION DE RÉFORME DU DROIT DU CANADA, *Rapport : Notre droit pénal (Our criminal Law)*, Ottawa, Information Canada, 1976, p. 28. Voir aussi Hélène DORION, *La protection de l'information,* (1992) 23 *R. G. D.* 197, où elle écrit, à la page 227 :

Cet extrait rappelle que le contenu du droit criminel devrait être limité aux comportements les plus graves et en ce sens, on peut penser que certains crimes actuellement reconnus pourraient être dépénalisés[26]. Dans les plus récents jugements de la Cour suprême cependant, on reconnaît que la compétence en matière de droit criminel est de nature plénière et qu'elle a toujours été définie largement. Elle se caractérise essentiellement par la détermination de certaines interdictions, assorties de sanctions pénales. Toutefois, ces interdictions doivent être fondées sur un "objectif public légitime" et le "mal" ou "l'effet nuisible" à contrer doit être identifié[27]. Le

> Le droit criminel requiert des textes précis destinés à appréhender des comportements socialement nocifs bien définis : il en va de la liberté des individus. Le droit criminel n'intervient pas chaque fois qu'il est nécessaire d'assurer une certaine protection. Avant de prévoir des mesures pénales sur une question quelconque, des moyens autres que la création de crimes doivent s'avérer insuffisants et une conduite doit causer ou menacer de causer un préjudice sérieux aux individus ou à la société.

[26]La *dépénalisation* de certains comportements est un processus entamé dans plusieurs États, comme conséquence de l'insuccès de la logique traditionnelle du droit pénal. Il conviendra sans doute de se pencher plus amplement sur cette question sous l'angle de la protection de la liberté d'expression.

droit criminel vise à "supprimer le mal" ou "protéger l'intérêt menacé" et les principaux intérêts à protéger sont, de façon non exclusive, la *"paix publique, l'ordre, la sécurité, la santé, la moralité"*[28].

Donc, face à une activité qui suscite des controverses, on doit se demander si celle-ci constitue un mal ou un effet nuisible pour le public. Dans l'affirmative, et suite à l'identification de ce mal, on doit s'interroger s'il y a lieu d'interdire l'activité en question et de l'assortir de sanctions pénales. En d'autres termes, on devrait se demander si ce "mal" est suffisamment grave pour exiger l'intervention du droit criminel ? Ou ce mal pourrait-il être contré par des interventions provinciales, locales, fondées

---

[27]Juge LaForest, dans *RJR MacDonald* c. *Procureur général du Canada*, nos 23460 et 23490, 21 septembre 1995, par. 28. Le juge LaForest est dissident sur la conclusion d'inopérance de la *Loi réglementant les produits du tabac*, L. C. 1988. c. 20. Il considère toutefois que cette loi a été validement adoptée par la Parlement fédéral, par sa compétence en droit criminel. Sur cet aspect, il est appuyé par les juges L'Heureux-Dubé et Gonthier (qui souscrivent à la totalité de son opinion), ainsi que par les juges Iacobucci, McLachlin, Lamer et Cory. Rappelons en outre que cette loi abordait trois aspects principaux de la réglementation des produits du tabac qui ont été reconnus comme portant atteinte à la liberté d'expression des producteurs de tabac. D'abord, elle interdit de façon générale la *publicité* des produits du tabac (à la télévision ou dans les journaux) ; elle limite également dans une très large mesure la *promotion* de produits du tabac en relation avec d'autres activités culturelles ou sportives ; et enfin, elle oblige les producteurs de tabac à indiquer sur leurs produits les substances toxiques qui y sont contenues, en plus d'un avertissement sur l'un des nombreux risques encourus par le consommateur des produits du tabac. Le juge Major, pour sa part a qualifié la loi fédérale d'*ultra vires* dans la mesure où les infractions créées ne répondent pas au critère suivant :

> [L]'activité que le Parlement souhaite réprimer à l'aide d'une sanction pénale doit présenter *un risque de préjudice grave et important pour la santé du public, sa moralité ou sa sécurité*. S'il existe une gamme de comportements entre celui qui est le plus grave et celui qui l'est moins, ce ne sont pas tous les préjudices ou dangers pour la société qui sont suffisamment graves et importants pour justifier l'application du droit criminel.

[28]Citation tirée du *Renvoi sur la margarine*, 1949 R. C. S. 1.

sur d'autres objectifs que la “stigmatisation” des auteurs ?[29].

Une controverse particulière se soulève lorsque le crime constitue une forme d’expression. En effet, à certaines reprises, la Cour suprême du Canada a dû interpréter certains crimes par rapport à la protection de la liberté d’expression. La légitimité de la criminalisation des discours peut ressortir de plusieurs théories. Ainsi, le fait que le comportement manifesté dans la communication constitue lui-même un crime ou incite au crime justifiera l’intervention de l’État pour limiter la propension de ces informations ; le fait que le contenu du discours ne poursuit aucun des objectifs ou des rationalités de la liberté d'expression (épanouissement personnel, participation publique et recherche de vérité) peut également favoriser la création de limites aux discours. Toutefois, on doit reconnaître que plusieurs formes de discours ne poursuivent aucun de ces objectifs. Ainsi, dans l'affaire *Keegstra*[30], la Cour a souligné que la propagande haineuse “contribue peu” à l'une de ces valeurs. Dans l'affaire *Butler*[31], la Cour écrit que l'expression de pornographie est surtout motivée par le “profit économique”, ne s'inscrivant pas ainsi dans les objectifs nobles de la liberté d'expression[32].

---

[29]En fait, la définition élargie du droit criminel semble soulever certaines difficultés idéologiques. Le droit criminel n'est pas la pierre angulaire de notre droit ; il est un moyen pour le fédéral d'intervenir sur des questions qui sont souvent de nature locale. D'ailleurs, la liberté laissée aux procureurs généraux des provinces révèle la particularité de certaines provinces face aux interdits. Par ailleurs, le choix de la criminalisation de certaines activités devrait pouvoir se poser en parallèle avec la théorie de l'"intérêt national", c'est-à-dire on devrait se demander si le mal est suffisamment important (ou la menace suffisamment dangereuse) pour appeler une intervention uniforme pour l'ensemble du territoire canadien ou s’il y aurait plutôt lieu d'agir en fonction des intérêts propres à la localité où le problème ou la menace sont le plus sérieux.

[30]*R. c. Keegstra,* 1990, 3 R. C. S. 697.

[31]Cette affaire traite de l'interdiction de publication, de distribution ou de mise en circulation de matériel obscène, *R. c. Butler*, 1992 1 R. C. S. 452.

[32]Pourtant, le profit économique était l'objectif central des compagnies de tabac dans leur contestation de constitutionnalité de la *Loi réglementant les produits du tabac*, bien qu'elles aient invoqué la volonté de créer une relation d'information avec leurs clients. Voir *RJR MacDonald*, précitée, note 26.

Que peut-on penser des discours ou des formes d'expression qui sont vouées au divertissement, à l'expression artistique, aux discours nuisibles et à la publicité ? L'objectif de tels discours devrait-il, par leur exclusion de la sphère traditionnelle de valeurs, être considéré illégal et justifier l'intervention législative, même sous la bannière du droit criminel ? La sphère protégée ne pourrait-elle pas être élargie ?

Enfin, un argument intéressant, formulé par le juge Major dans l'affaire relative aux produits du tabac, qui invite à la décriminalisation de certains discours, c'est le fait que malgré qu'il existe une telle interdiction au Canada, celle-ci ne s'applique pas aux publications étrangères. Il écrit :

> *On peut difficilement imaginer comment la publicité en faveur du tabac produite par les États-Unis ou d'autres pays et distribuée au Canada par voie de publications devient en quelque sorte criminelle lorsqu'elle est produite et distribuée par des Canadiens*[33].

Cet argument reflète sans doute une réalité incontournable devant le phénomène des nouveaux moyens de communication. Comment et pourquoi criminaliser un discours prononcé par des personnes qui sont citoyennes d'un État alors que ce discours peut être légalement tenu par des étrangers ?

Enfin, il y a lieu de poser ici un commentaire à l'effet que dans l'élaboration ou la découverte du cadre juridique de l'inforoute, il devient utile de voir ce moyen de communication comme un outil intéressant pour l'amélioration des rapports interpersonnels et les relations entre l'État et ses citoyens et entre les entreprises et ses clients. À notre avis, l'une des façons pour l'État d'intervenir sur l'inforoute, c'est sans doute d'adopter des normes de droit relatives à son encadrement, mais c'est surtout de prendre une place sur ce réseau, c'est-à-dire de se présenter comme un acteur important et un fournisseur de services. L'inforoute est porteuse de plusieurs changements et est susceptible d'apporter des solutions à un certain nombre de problèmes concrets. Et un des problèmes les plus importants, c'est sans doute le

---

[33] *RJR MacDonald*, précitée, par. 215.

fonctionnement du système de justice[34].

## 33. La corruption des moeurs et l'atteinte à l'ordre public

La corruption des moeurs et l'atteinte à l'ordre public apparaissent comme des justifications traditionnelles à l'intervention de l'État pour limiter la circulation de matériel obscène, pornographique, séditieux et pour limiter les jeux et loteries. Ces différentes activités de communication sont susceptibles de se dérouler sur l'inforoute.

### 33.1 Le matériel obscène et pornographique

Au Canada, la possession simple de matériel obscène est licite. Par contre, au moyen de l'article 163 C. cr., le législateur en interdit la production, l'impression, la publication, la distribution, la vente, l'exposition à la vue du public ou toute possession à de telles fins. Dans le cadre de ces activités, seul le matériel pornographique qualifié d'obscène est banni[35]. Sous ce thème, nous aborderons d'abord l'état du droit canadien en cette matière (3. 1. 1) pour ensuite dégager les principaux enjeux juridiques soulevés par la circulation de ce genre de matériel dans les réseaux d'information (3. 1. 2), enfin, la question de la pornographie juvénile sera

---

[34]Certaines questions se posent d'ailleurs au chapitre de la sanction d'emprisonnement pour des crimes d'expression. En effet, en matière de discours, les sanctions prévues sont le plus souvent situées autour du maximum de deux années d'emprisonnement. Or, dans les faits, l'emprisonnement est souvent plus court et l'entretien des pénitenciers (peine de moins de deux ans) est assumé par la province, pour des crimes fédéraux. Des alternatives à l'emprisonnement mériteraient sans doute d'être trouvées pour de tels crimes. Sur cette question, on pourrait lire avec intérêt André NORMANDEAU, *Pour un système pénal sérieux, intelligent et taillé sur mesure en Amérique* (avr. - juin 1995) 2 *Rev. sc. crim.* 404 ; également, Deidre GOLASH et James P. LYNCH, *Public Opinion, Crime Seriousness, and Sentencing Policy* (1995) 22 *Am. J. Crim. L.* 703.

[35]Le matériel pornographique, c'est du matériel à caractère sexuel explicite. On peut penser que la représentation d'actes de bestialité ou d'inceste seraient qualifiés d'obscènes par les tribunaux, d'autant plus qu'ils constituent des actes interdits en vertu des art. 155 et 160 C. cr.

abordée (3. 1. 3).

### 33.1.1 L'état du droit canadien en matière d'obscénité et de pornographie

L'article 163 C. cr. a donc pour objet et pour effet de limiter la libre circulation du matériel obscène. En interdisant ce type d'activité expressive, le législateur viole, de ce fait, le droit à la liberté d'expression, reconnu par l'article 2b) de la *Charte canadienne des droits et libertés*[36] (la Charte).

Dans l'affaire Butler[37], la Cour Suprême du Canada (la Cour) a statué que bien que l'article 163 contrevienne à l'art. 2b) de la Charte, cette violation constitue une limite raisonnable à la liberté d'expression, justifiée dans le cadre d'une société libre et démocratique, parce qu'elle vise à éviter qu'un préjudice[38] soit causé à la société, et en particulier aux femmes.

Selon le juge Sopinka pour la majorité, cette violation serait d'autant plus justifiée puisque le genre d'expression que l'on cherche à promouvoir par le matériel obscène n'est pas du même calibre que les autres genres d'expression qui touchent directement à “l'essence” des valeurs relatives à la liberté d'expression[39]. Le juge appuie cette conclusion sur le fait additionnel

---

[36]L. R. C. (1985). App. II, no 44, Ann. B.

[37]*R. c. Butler* [1992] 1 R. C. S. 453.

[38]Voir *R. c. Butler*, p. 495 :

> Notre compréhension des préjudices causés par ce matériel a évolué considérablement depuis lors ; toutefois, cela ne déroge pas au fait que l'objet de ce texte législatif demeure, comme c'était le cas en 1959, la protection de la société contre les préjudices découlant de l'exposition au matériel obscène.

[39]Ces valeurs étant celles qui ont trait à la recherche de la vérité, à la participation au processus politique et à l'épanouissement personnel.

que le matériel visé constitue une expression motivée, dans la vaste majorité des cas, par le bénéfice économique[40].

Le préjudice que provoque la circulation de matériel obscène a été défini par le Comité permanent de la justice et des affaires juridiques dans son *Rapport sur la pornographie* :

> *Le danger évident et incontestable de ce genre de matériel est qu'il encourage certaines tendances malsaines au sein de notre société canadienne. Il met l'accent sur les stéréotypes masculins et féminins au détriment des deux sexes. La dégradation, l'humiliation, la soumission et à l'en croire, la violence dans les relations humaines seraient tout à fait normales et acceptables*[41].

Le juge Anderson de la Cour d'Appel de la Colombie-Britannique décrit le préjudice particulier causé aux femmes comme étant la mise en cause de leur *droit à l'égalité*. Il considère que si l'on veut parvenir à une véritable égalité entre les hommes et les femmes, on ne peut ignorer la menace que présente pour l'égalité le fait d'exposer le public à certains types de matériel violent et dégradant. Le matériel qui représente les femmes comme une catégorie d'objets d'exploitation et d'abus sexuels aurait une incidence négative sur "*la valorisation personnelle et l'acceptation de soi*"[42].

D'après la Cour, le Parlement a considéré que la conjonction particulière d'une représentation et de son contenu, qui constitue l'objet de l'article 163 du Code, a pour effet de présenter une image déformée de la sexualité humaine, susceptible de provoquer des changements d'attitude

---

[40]Dans l'arrêt *Rocket c. Collège royal des chirurgiens dentistes de l'Ontario*, [1990] 2 R. C. S. 232, à la p. 247, la Cour a statué qu'un motif d'expression de nature économique signifie qu'il se pourrait que des restrictions imposées à l'expression *soient plus faciles à justifier que d'autres atteintes*. Voir *R. c. Butler*, p. 499-501.

[41]Canada. Chambre des communes. Comité permanent de la justice et des affaires juridiques. *Rapport sur la pornographie*. No. 18 (22 mars 1978).

[42]Nous traduisons. *R c. Red Hot Video Ltd*. (1985), 45 C. R. (3d) 36 (C. A. C. -B.)..

préjudiciables et des comportements antisociaux[43]. Bien qu'il soit difficile d'établir l'existence d'un lien direct entre le matériel obscène et le préjudice causé à la société, la Cour a estimé qu'il existe un lien suffisamment rationnel entre l'objectif et la sanction pénale, qui, d'une part, montre la désapprobation de notre société à l'égard de la diffusion de matériel qui risque de victimiser les femmes et, d'autre part, restreint l'influence négative que ce genre de matériel risque d'avoir sur les attitudes et les comportements.

De façon générale donc, la Cour a estimé que la diffusion de matériel obscène est préjudiciable à la société parce qu'elle est susceptible de provoquer chez elle des changements d'attitude et des comportements antisociaux nocifs. Selon la Cour, une telle qualification de ce qui constitue un préjudice[44] se justifie en fonction des valeurs de la société canadienne, qui considère que l'égalité entre ses membres, la dignité de tous ses membres, la suppression de la violence, le libre choix et la réciprocité constituent la base de toutes les relations humaines, sexuelles ou autres[45]. Finalement, la Cour a jugé que la prévention d'un préjudice constitue un objectif moral valide en vertu de l'article 1 de la Charte. D'ailleurs, le juge Gonthier affirme que le fait d'éviter qu'un préjudice soit causé à la société n'est qu'un exemple d'une conception fondamentale de la moralité. Il considère que l'un des objectifs majeurs de la moralité est d'éviter qu'un préjudice soit causé[46].

Le critère central à ce crime concerne la définition de l'obscénité. En vertu de l'article 163 (8) C. cr. est réputée obscène, toute publication qui a

---

[43]R. c. BULTER, p. 514, juge Gonthier, dissident.

[44]Tel que défini au paragraphe précédent, le préjudice en cause est la provocation chez la société de changements d'attitude et de comportements antisociaux nocifs.

[45]Canada, Chambre des communes, Comité permanent de la justice et des affaires juridiques, *Rapport sur la pornographie* No. 18 (22 mars 1978). On a fait état des mêmes valeurs dans Canada, Comité spéciale d'étude de la pornographie de la prostitution ; *La pornographie et la prostitution au Canada,* Rapport du comité spéciale d'étude de la pornographie et de prostitution, vol. 1. Ottawa ; Approvisionnements et Services, 1985.

[46]*R. c. Butler*, p. 524.

pour caractéristique dominante l'exploitation indue des choses sexuelles, ou de choses sexuelles et de l'un ou plusieurs des sujets suivants, savoir : le crime, l'horreur, la cruauté et la violence. En d'autres mots, pour qu'un ouvrage soit réputé obscène, l'exploitation des choses sexuelles doit non seulement en constituer la caractéristique dominante, mais elle doit également être "indue".

Afin de déterminer quand l'exploitation des choses sexuelles est "indue", les tribunaux ont formulé des règles pratiques, la plus importante étant celle de la "norme sociale de tolérance". Le Juge Dickson, dans l'arrêt *Towne Cinema*, résume le critère adopté par la Cour suprême du Canada pour définir cette norme :

> *[...] la norme applicable est la tolérance et non le goût. Ce qui importe, ce n'est pas ce que les Canadiens estiment convenable pour eux-mêmes de voir. Ce qui importe, c'est ce que les Canadiens ne souffriraient pas que d'autres Canadiens voient parce que ce serait outrepasser la norme contemporaine de tolérance au Canada que de permettre qu'ils le voient.*[47]

Dans l'affaire *La Reine c. Butler*[48] la Cour suprême a précisé que le critère de la norme sociale de tolérance tient compte "*des normes de tolérance de l'ensemble de la société et non pas seulement des normes de tolérance d'une fraction de la société*[49]". En conséquence, la norme en cause est une norme sociale nationale de tolérance (la norme sociale de tolérance).

Toutefois, il est intéressant de noter que dans les faits, le seuil de tolérance des Canadiens peut varier en fonction de la région ou même des villages où ils se trouvent. Par exemple, le seuil de tolérance des Montréalais est-il le même que celui des Saskatoonois ? Une définition

---

[47] *Towne Cinema Theatres Ltd.* c. *La Reine* [1985] 1 R. C. S. 494. Juge Dickson, pp. 508-509.

[48] [1992] 1 R. C. S. 453.

[49] *R. c. Butler,* p. 476.

régionale ou locale de la “norme de tolérance” ne serait-elle pas plus conforme à la réalité ?[50] D'ailleurs, aux États-Unis, les tribunaux américains appliquent une “norme sociale communautaire de tolérance” en cette matière[51].

De plus en plus, la jurisprudence reconnaît que le matériel qui exploite les choses sexuelles de façon “dégradante ou déshumanisante” échoue nécessairement face au critère de la norme sociale de tolérance[52]. On estime que le matériel qui “dégrade” ou “déshumanise” les personnes représentées excède la norme sociale de tolérance, et ce, même en l'absence de cruauté et de violence[53].

Selon la Cour, notamment, le matériel dégradant ou déshumanisant place des femmes (et parfois des hommes) en état de subordination, de soumission avilissante ou d'humiliation. Il est contraire aux *principes d'égalité et de dignité* de tous les êtres humains. Ce genre de matériel

---

[50]D'ailleurs, les codes de conduite propres aux télécommunautés (ou "cybercommunautés", terme retenu par les auteurs V. BELL et D. DE LA RUE, *Gender Harassment on the Internet* :

http://www.gsu.edu/~lawppw/lawand.papers/harass.html) trouvent ici une pertinence et une validité. La participation des usagers à la définition de cette norme de tolérance pourrait susciter d'intéressants débats pouvant mener à la reconnaissance de plusieurs niveaux de tolérance.

[51]Ce critère a été appliqué, par exemple, dans l'illustre affaire des conjoints Thomas. Cette cause, qui a été portée en appel, concerne la déclaration de culpabilité et la condamnation respective à deux ans et trois ans et demi de prison, par une Cour Fédérale du Tennessee, d'un couple d'opérateurs de Babillard Électronique qui, à partir de la Californie, ont téléchargé du matériel pornographique pouvant être télédéchargé au Tennessee. Le matériel a été jugé obscène en appliquant le critère de "la norme sociale communautaire" du Tennessee qui est moins permissif que celui de la Californie. Cette affaire a proposé que ce soit la norme du lieu de réception du matériel qui s’applique et non celle du lieu d’émission. Neil J. FRIEMAN, *Is there a Court in Cyberspace ?* accessible à l'adresse suivante sur le Net :

http:/www.commlaw.com/pepper/Memos/InfoLaw/internet.102094.html

[52]*R. c. Doug Rankine Co*. (1983), 9 C. C. C. (3d) 53 (C. cté Ont.)..

[53]*R. c. Ramsingh* (1984), 14 C. C. C. (3d) 230 (B. R. Man.), et *R. c. Wagner* (1985), 43 C. R. (3d) 318 (B. R. Alb.)..

échoue le test de la norme sociale de tolérance parce qu'il est jugé nocif pour la société, particulièrement pour les femmes[54]. On constate le lien évident qui existe entre l'établissement de ce critère et les rationalités de l'article 163, décrites précédemment.

Certains moyens de défense peuvent être invoqués à l'encontre de ce genre d'accusation, dont celui fondé sur la valeur artistique du matériel en cause. C'est le critère des “besoins internes”[55]. Il constitue la dernière étape dans l'analyse de la question de savoir si l'exploitation des choses sexuelles est indue. Il s'applique seulement si une oeuvre renferme du matériel sexuel explicite qui, en lui-même, constituerait une exploitation indue des choses sexuelles. Il sert à déterminer si l'exploitation des choses sexuelles joue un rôle légitime lorsqu'on l'évalue en fonction des besoins internes de l'oeuvre elle-même. Il faut se demander si l'exploitation des choses sexuelles est justifiable dans le développement de l'intrigue ou du thème et si, d'après l'ensemble de l'oeuvre, elle ne représente pas simplement de l'obscénité pour de l'obscénité.

Ainsi, les tribunaux doivent déterminer du mieux qu'ils peuvent ce que la société canadienne tolérerait que les autres voient en fonction du degré de préjudice qui peut en résulter. Dans ce contexte, le préjudice signifie qu'il prédispose une personne à changer d'attitude et à agir de façon antisociale, par exemple, le fait pour un homme de maltraiter une femme physiquement ou mentalement. Le comportement antisocial en ce sens est celui que la société reconnaît officiellement comme incompatible avec son bon fonctionnement. Plus forte sera la conclusion à l'existence d'un risque de préjudice, moins grandes seront les chances de tolérance[56]. La Cour utilise la norme sociale de tolérance pour évaluer le risque de préjudice. Selon le juge Gonthier, dans ce contexte, il doit exister un rapport entre la tolérance et le préjudice. Elle doit signifier qu'il y a non seulement tolérance du matériel, mais aussi tolérance du préjudice que ce matériel est susceptible

---

[54] *R. c. Butler,* p. 479.

[55] *Brodie c. The Queen,* [1962] R. C. S. 681..

[56] *R. c. Butler,* p. 485.

de causer[57].

La marge qui sépare le matériel pornographique du matériel obscène au Canada peut être tracée de façon conceptuelle. Mais elle demeure évolutive. Ainsi, le matériel pornographique fait référence à des choses sexuelles explicites. Le matériel obscène fait référence au matériel pornographique qui répond aux critères de l'article 163 (8) du Code. Dans l'affaire *Butler*, le juge Sopinka, propose une division du matériel pornographique en trois catégories :

a) Les choses sexuelles explicites, acompagnées de violence, qui constituent généralement une “exploitation indue des choses sexuelles” au sens du par. 163(8) du Code, selon le préjudice qui peut être démontré ;

b) les choses sexuelles dégradantes ou déshumanisantes, qui constituent une “exploitation indue des choses sexuelles” lorsqu'elles créent un risque de préjudice important, lequel peut être évalué par rapport au seuil de tolérance de la société, en application du critère de la “norme sociale de tolérance” ;

c) les chose sexuelles explicites, non accompagnées de violence, qui ne sont ni dégradantes ni déshumanisantes.

Selon le juge Sopinka, le matériel pornographique qui correspond à la troisième catégorie n'est généralement pas considéré obscène car il risque peu de causer préjudice[58]. Bien qu'il soit d'accord avec ce modèle de classification de la pornographie, le juge Gonthier apporte une précision quant à la troisième catégorie. Il considère qu'indépendemment de son contenu, le “mode de représentation” du matériel pornographique est un facteur qui influence la probabilité de préjudice et la tolérance de la

---

[57] *R. c. Butler*, pp. 520-521.

[58] À titre d'exception, il mentionne la pornographie produite avec la participation d'enfants. D'ailleurs, selon le juge Gonthier, cette exception découle, de toute évidence, du risque élévé de préjudice que comportent la production et la diffusion de ce type de pornographie.

société[59]. En conséquence, contrairement au juge Sopinka, il considère que le risque de préjudice découlant du contenu ou de l'élément de représentation du matériel de la troisième catégorie n'est pas toujours faible. À titre d'exemple, il cite le cas d'une représentation explicite de relations sexuelles “ordinaires” entre deux personnes, qui tombe dans la troisième catégorie :

> *Si cette scène est décrite dans un livre, il y a peu de chances qu'elle suscite beaucoup d'inquiétudes [...]. Si cette scène est décrite dans une revue ou dans un film, la probabilité de préjudice augmente, mais demeure faible. Si cette scène est représentée sur une affiche, elle est déjà plus troublante. Si elle est représentée sur un panneau-réclame, j'irais alors jusqu'à dire qu'il peut bien s'agir d'une exploitation indue des choses sexuelles parce que la société ne tolère pas ce genre de représentation, en raison de son caractère préjudiciable.*
>
> *Le caractère préjudiciable, dans l'exemple du panneau-réclame, découlerait de l'immédiateté de la représentation, dans la mesure où le panneau-réclame se passe d'explication (par opposition à un passage dans un livre, dans un film ou dans une revue). Le message qu'il transmet est à la fois brutal et inévitable. Il déforme la sexualité humaine en la présentant au public, dépouillée de tout contexte. Il s'agit là bien entendu d'un exemple extrême ; toutefois il sert à démontrer que l'élément de représentation peut engendrer une probabilité de préjudice susceptible de donner lieu à l'application de l'article 163 du Code, et ce, même si le contenu de la représentation n'est pas choquant en soi*[60].

---

[59] *R. c. Butler,* p. 518.

[60] *R. c. Butler,* p. 518-19.

### 33.1.2 La pornographie sur l'inforoute

Au début de l'année 1995, l'Université Carnegie Mellon a publié une étude sur la pornographie et l'autoroute de l'information[61]. L'auteur, Marty Rimm, soutient que son travail constitue la première étude systématique du domaine. Son rapport présente des données sur la distribution et la consommation de matériel pornographique dans les environnements électroniques. Selon Rimm, l'étude rend compte du point de vue de ceux qui produisent la pornographie, puisqu'il a analysé le contenu du matériel diffusé ; et du point de vue de ceux qui consomment la pornographie, puisqu'il a étudié leurs habitudes de télédéchargement[62], tant au niveau de la fréquence que du contenu. Rimm avance que les données sur les habitudes de télédéchargement ont d'autant plus de valeur et de fiabilité qu'elles réflètent le matériel pornographique que les gens consomment “en fait”, et non pas ce qu'ils “disent” consommer.

Le rapport Rimm fait l'objet d'une grande controverse. On lui reproche, notamment, d'avoir fait de fausses représentations en extrapolant à l'ensemble de l'autoroute de l'information, l'interprétation de données relatives à une infime partie de ce domaine, soit soixante-huit Babillards Électroniques[63]. De plus, la méthodologie de recherche utilisée est

---

[61]Marty RIMM, *Marketing Pornography on the Information Superhighway : A Survey of 917 410 Images, Descriptions, Short Stories, and Animations Downloaded 8. 5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories*, 1995.

http://www2.infoseek. com/Titles?qt=Rimm+report+on+pornography

[62]Le terme "télécharger" est utilisé ici au sens du terme anglais "to upload". Selon nous, télécharger, c'est rendre disponible de l'information sur support électronique. Le terme "télédécharger" est utilisé ici au sens du terme anglais "download", c'est-à-dire, de prendre les démarches nécessaires pour recevoir de l'information rendue disponible sur support électronique.

[63]Donna L. HOFFMAN, Thomas P. NOVAK, *A Detailed Analysis of the Conceptual, Logical, and Methodological Flaws in the Article : Marketing Pornography on the Information Superhighway*, july 1995.

http://www2000.ogsm.vanderbilt.edu/rimm.cgi

et Mike GODWIN, *JournoPorn, Dissection of the ime Scandal* , 1995.

contestée, et, de ce fait, les résultats obtenus[64]. Les nombreux critiques de ce rapport soutiennent que les résultats ne sont absolument pas valides étant

---

http://www.hotwired.com/special/pornscare/godwin/html

[64]Voici un résumé des principaux résultats obtenus, tels que présentés par Marty Rimm , à la section V. de son rapport : *Summary of Significant Results of the Carnegie Mellon Study*, dans Marty RIMM, précité, note 61.

Les environnements électroniques constituent un nouveau mode de distribution et de consommation de matériel pornographique. Ce mode est utilisé, à une échelle mondiale, par les fabricants et les consommateurs.

A l'aide des environnements électroniques, il est possible de développer une nouvelle méthodologie permettant de rendre disponibles, à une plus grande échelle que celle permise par les méthodologies établies au préalable, des données concernant le matériel pornographique en circulation. Les trois principales composantes de cette nouvelle méthodologie sont : a) l'identification des habitudes de consommation ; b) l'identification du type de matériel pornographique consommé ; c) la comparaison annuelle des images rendues disponibles afin d'identifier les changements au sein du marché. Cette étude comparative peut être divisée en fonction des régions, des Babillards Électroniques (B. É.) ou des différentes catégories de matériel pornographique.

À travers les différents les réseaux électroniques tels le Usenet, le World Wide Web et les B. É. pour "adultes", le matériel pornographique à caractère pédophile et paraphile est rendu disponible. Il existerait des consommateurs pour ce type de matériel dans plus de 2000 villes situées dans tous les états des États-Unis, dans la plupart des provinces canadiennes et dans quarante pays étrangers, provinces, et territoires situés dans le monde.

71%du matériel pornographique circulant sur le Usenet provient de B. É. pour "adultes". Cette réalité suggère que les B. É. privés doivent être étudiés afin de comprendre l'augmentation explosive de la pornographie sur le Usenet.

À l'Université qui a fait l'objet de la présente étude, les Groupes de Discussion sur le Usenet, qui contenaient du matériel pornographique, constituent 13 des 40 Groupes les plus populaires. Ces statistiques, ainsi que celles disponibles à une échelle mondiale, suggèrent que la matériel pornographique sur le Usenet doit être étudié en fonction de l'intensité de l'activité, parce que l'étude de la quantité de B. É. mènerait à des chiffres erronément bas.

83,5% de toutes les images téléchargées sur le Usenet sont de nature pornographique. Cette réalité suggère que la nouvelle vague de produits multimédia, conçus pour rendre le Usenet plus "interactif", pourraient être alimentés, de façon importante, par le matériel pornographique.

donné qu'ils ont été obtenus de manière non scientifique[65]. Vu ce contexte, nous suggérons qu'il faut faire preuve de prudence face à ce rapport. En conséquence, nous n'en retenons que les idées générales suivantes, qui nous apparaissent incontestables.

---

Les images pornographiques à caractère paraphile, hébephile et pédophile constituent environ la moitié des six millions de télédéchargements comptés sur les B. É. privés "adultes". Par rapport à la quantité de matériel disponible, il y avait peu de demande pour les images *hard-core* et *soft-core,* alors qu'il y avait plus de demande pour les images paraphiles et pédophiles qu'il y avait de matériel disponible. La disponibilité de, et la demande pour, des images représentant des relations sexuelles vaginales était relativement petite. Ces chiffres mettent en valeur la différence importante entre les médias pornographiques de la presse écrite et les médias pornographiques du mode numérique.

La technologie cédérom permet aux B. É. "adultes" d'acquérir des bibliothèques importantes d'images à peu de frais. Les ordinateurs ont également permis aux consommateurs d'acquérir une vaste quantité de matériel pornographique à une fraction du coût du matériel circulant dans la presse écrite.

Un vide énorme existe entre la disponibilité de, et la demande pour, la plupart des types d'images pornographiques. Les fabricants de pornographie numérique n'ont toujours pas tiré profit des informations nouvelles qui existent, en grande quantité, au sujet de chaque consommateur.

Le *Amateur Action BBS,* B. É. ayant pris la tête du marché, se fonde sur trois modes de service à la clientèle : a) le déséquilibre dans le partage du pouvoir et la représentation disproportionnée de femmes se livrant à des actes pouvant être considérés dégradants ; b) le *marketing* trompeur c) l'exploitation des enfants.

Des questions importante cédérom s relatives au thème de la confidentialité sont soulevées par le phénomène de la vente, par les fabricants de matériel pornographique, de données relatives aux habitudes des consommateurs.

65 Ces critiques comprennent : Donna L. HOFFMAN, Thomas P. NOVAK, *A Detailed Analysis of the Conceptual, Logical, and Methodological Flaws in the Article,* Marketing Pornography on the Information Superhighway, july, 1995.

http://www2000.ogsm.vanderbilt.edu/rimm.cgi

Brian REID, *Critique of the Rimm study*, july, 1995.

http://www2000.ogsm.vanderbilt.edu/novak/brian.reid.critique.html

et Mike GODWIN, *Law of the Net* : Philip's Folly, despite warnings that the Rimm study was flawed, Time's "Cyberporn" author persisted in pushing the story that cast the Net in a negative light" (October 1995) Internet World 102.

Les environnements électroniques constituent un nouveau moyen pour visionner et pour faire circuler le matériel pornographique. De façon générale, en étant branché sur un réseau ouvert tel l'Internet, il est possible de visionner du matériel pornographique à partir de son écran d'ordinateur en sollicitant les Babillards Électroniques (B. É.) ou les Groupes de Discussion qui offrent ce service. Au moyen du courrier électronique, il est également possible d'envoyer ou de recevoir ce genre de matériel, soit par l'intermédiare des deux types de sites mentionnés ci-dessus ou de façon indépendante. En fait, des images à caractère sexuel explicite circulent dans les environnements électroniques. Marty Rimm y a même décelé de la pornographie infantile et du matériel qui traite de bestialité et de pédophilie.

Il est probable que les consommateurs de pornographie apprécient se livrer à cette activité à partir de leur écran informatique qui leur permet d'agir dans l'intimité de leur maison[66]. Ce mode d'accès est moins embarassant que celui, par exemple, de se diriger en public vers des boutiques spécialisées. Également, la possibilité de stocker le matériel pornographique sur une disquette ou sur le disque dur d'un ordinateur en permet la possession discrète.

La Cour de l'Ontario (division provinciale), dans *R. c. Pecciarich*[67] a rendu la première décision canadienne concernant la poursuite criminelle d'un opérateur de B. É. pour distribution de matériel pornographique. En vertu de l'article 163 du Code, Pecciarich a été accusé d'avoir distribué des images obscènes (premier chef) et de la pornographie juvénile (deuxième chef), à partir de son ordinateur personnel, en les téléchargeant sur le B. É. qu'il opérait, permettant qu'elles soient télédéchargées par les abonnés intéressés. Il a été déclaré coupable du seul chef relatif à la pornographie juvénile.

Cette décision est pertinente, au départ, parce qu'elle a permis d'établir

---

[66]Ann Wells BRANSCOMB, Ann Wells, *Internet Babylon ? Does the Carnegie Mellon Study of Pornography on the Information Superhighway Reveal a Threat to the Stability of Society ?*, 1995.

http://www.georgetown.edu/papers/brnscomb.txt

[67][1995] 22 O. R. (3d) 748.

que le fait pour un individu de télécharger du matériel obscène sur un B. É., permettant qu'il soit télédéchargé par les abonnés intéressés, constituait, en droit, de la distribution au sens de l'article 163 C. cr. Elle est également intéressante parce qu'elle soulève quelques-unes des nombreuses questions qui se posent dans le cadre de la circulation du matériel pornographique et obscène (ainsi que les autres activités illicites) dans les environnements électroniques[68]. Notamment, cette décision permet de mettre en lumière certaines des difficultés rencontrées en matière d'application de la loi, dans les contextes particuliers de l'identification des malfaiteurs et de la preuve.

Finalement, la défense a admis que le matériel était obscène. La poursuite n'a donc pas eu de preuve à offrir à cet effet. Il aurait été intéressant de savoir ce que le tribunal aurait fait du critère du mode d'expression suggéré par le juge Gonthier dans l'arrêt Butler. L'aurait-il reconnu comme un critère valide ? Vu qu'il se situe normalement dans l'intimité du domicile, un écran d'ordinateur constitue-t-il un mode d'expression servant à limiter la probabilité du préjudice pouvant être subi par la société ?

Le contexte des environnements électroniques engendre aussi des difficultés d'identification des malfaiteurs, étant donné la possibilité qu'ils ont d'agir à titre anonyme. Par exemple, l'accusé Pecciarich a tenté de

---

[68]D'ailleurs, une des questions qui se pose dans ce contexte est celle de l'application de la *Loi concernant les douanes* L. R. C. (1985), ch. 1 (2e suppl.) [C-52. 6]. Cette loi régit l'information qui entre au Canada sous une forme matérielle, par exemple, les livres ou les vidéos. En vertu de cette loi, les agents douaniers sont chargés de s'assurer que ce matériel qui entre au pays n'est ni haineux, ni obscène. Il est intéressant de se demander comment cette loi pourrait s'appliquer au matériel pornographique "transfrontalier" qui circule dans les environnements électroniques ? Est-ce que les agents douaniers seraient en droit d'intercepter ce matériel dans les circonstances où il pourrait être télédéchargé au Canada ? Quelles seraient les conséquences d'un tel droit d'interception, par exemple, face au droit à la vie privée ? Dans les circonstances où ce matériel est encrypté, comment les agents pourraient-ils vérifier son contenu ?

cacher sa réelle identité en agissant sous un pseudonyme : Recent Zephyr[69]. La poursuite a dû faire preuve de rigueur et d'habileté afin de prouver, à l'aide d'une preuve circonstancielle et de la théorie de l'inférence[70], que Recent Zephyr était bien Pecciarich.

La preuve circonstancielle était la suivante : 1) à l'endroit même où l'on s'attend à trouver le nom du créateur, de nombreux dossiers saisis dans l'ordinateur de l'accusé exhibaient le nom Recent Zephyr, laissant croire que l'alias était le sien ; 2) l'identificateur Recent Zephyr se retrouvait sur plusieurs documents (contenant de la pornographie juvénile) saisis sur la bande de sécurité de l'ordinateur de l'accusé ; 3) deux copies d'une même image pornographique juvénile, découvertes sur la bande de sécurité de l'ordinateur de l'accusé, exhibaient, sur la première, la signature de l'accusé, et sur la seconde, le nom Recent Zephyr. Bien que cette preuve documentaire constitue du ouï-dire, elle a été admise par le tribunal, non pas pour prouver son contenu, mais pour prouver l'identité de l'accusé, en établissant le lien entre le pseudonyme et sa personne. Le tribunal a conclu que l'accusé et le nom Recent Zephyr ont été si fréquemment reliés, et ce, de façon significative, qu'on pouvait logiquement inférer qu'il s'agissait de la même personne. Nous suggérons que si l'accusé avait fait preuve de diligence dans l'utilisation de son pseudonyme, la pousuite aurait eu beaucoup plus de mal à le relier à sa personne.

La qualité de la preuve disponible par rapport à une activité illicite décelée dans les environnements électroniques peut également causer problème. Elle est faible, souvent, parce que le contexte fait en sorte qu'elle est indirecte et qu'elle constitue du ouï-dire.

Par exemple, dans *R.* c. *Pecciarich*, la poursuite devait prouver que c'était bien l'accusé qui avait téléchargé le matériel pornographique sur le B. É. qu'il opérait. Vu l'insuffisance de la preuve sur le premier chef, il a été

---

[69]Un autre exemple est celui du pédophile américain qui, au moyen de techniques d'encryptage, a réussi à cacher son identité à ses victimes, avec qui il communiquait en mode électronique. Voir Henry R. KING, *Big Brother, The Holding Company : A Review of Key-Escrow Encryption Technology*, 1995. Rutgers Computer & Technology Law Journal p. 227.

[70]*R. v. Morrissey* (1995), 22 O. R. (3d) 514 (C. A.)

impossible de convaincre le tribunal que c'était l'accusé qui était responsable de cette activité. En conséquence, il a été acquitté d'avoir distribué du matériel obscène. La preuve était la suivante : 1) les dossiers contenant le matériel obscène ont été trouvé sur le B. É. opéré par l'accusé, 2) ces dossiers étaient accompagnés d'une date et de la phrase “Uploaded by Recent Zephyr”[71]. La Cour a rejeté la deuxième partie de la preuve, la jugeant inadmissible parce qu'elle constituait du ouï-dire.

Au moyen d'une preuve circonstancielle complexe, la poursuite a quand même réussi à prouver que c'était bien Pecciarich qui avait téléchargé les documents contenant de la pornographie juvénile sur le B. É. (deuxième chef). Malgré que l'ensemble de cette preuve constituait du ouï-dire, elle a été admise par le tribunal à titre d'admissions de la part de l'accusé comme quoi il avait lui-même téléchargé la pornographie juvénile[72].

Cette preuve était constituée, entre autres, de documents saisis dans l'ordinateur de l'accusé, dont les suivants. 1) Un document intitulé “UCP Code BBS and software presents a Recent Zephyr History Note” résumant comment, à l'aide d'un numérisateur, l'auteur a créé une série de textes et d'images informatiques représentant de la pornographie juvénile ; 2) un document intitulé “Recent Zephyr's Master File list” constituant une liste de tous les dossiers auxquels réfère le deuxième chef et une brève description de chacun et 3) un document intitulé “Recent Zephyr Software” invitant les

---

[71]"Téléchargé par Recent Zephyr" ; "Recent Zephyr" étant le pseudonyme adopté par l'accusé.

[72]McWilliams, P. K., *Canadian Criminal Evidence*, 3rd edition, p. 10310. On peut lire :

> Documents which are, or have been, in possession of a party will [...] generally be admissible against him as original (circumstantial) evidence to show his knowledge of their contents, his connection with, or complicity in, the transactions to which they relate, or his state of mind with reference thereoto. They will further be receivable against him as admissions (i. e, exceptions to the hearsay rule) to prove the truth of their contents if he has in any way recognized, adopted or acted upon them.

usagers à télédécharger le matériel, indiquant, par le fait même, son intention que ces dossiers soient distribués gratuitement. De plus, au moment de son arrestation, l'accusé a admis aux policiers qu'il était impliqué dans l'opération du B. É. et qu'il avait inscrit son nom sur certains des programmes téléchargés. Nous suggérons, encore une fois, que si l'accusé avait fait preuve de diligence, d'abord en ne faisant pas de déclaration aux policiers et ensuite, dans son mode de conservation des documents en cause, la poursuite aurait eu plus de mal à prouver qu'il était responsable du téléchargement de la pornographie juvénile.

À mesure que l'usage de l'Internet prend de l'importance, tant socialement que commercialement, Douglas Barnes[73] croit que les nations voudront étendre leur juridiction pour contrôler la source de ce qu'elles perçoivent comme illégal ou choquant. La réalité des environnements électroniques, notamment, le phénomène de la délocalisation des contrevenants[74], a des incidences en matière de juridiction. Où était le

---

[73]Douglas BARNES, *The Coming Jurisdictional Swamp of Global Internetworking, [Or, How I Learned to Stop Worrying and Love Anonymity)*, november 1994 :

http://www.communities.com/paper/swamp.html

[74]Un autre phénomène important, relié à la réalité des nouveaux environnements électroniques, est celui de la délocalisation du corps des délits. Dans le contexte, par exemple, des crimes économiques modernes, où les activités ne se passent pas dans un pays en particulier, mais plutôt quelque part sur les ondes électroniques des communications informatiques, il n'est pas toujours évident d'établir où un crime a été commis. La cause de Nick Leeson illustre les problèmes engendrés par la poursuite de personnes impliquées dans des activités criminelles économiques qui transcendent les frontières nationales. Cambiste dans le marché des devises japonaises, Nick Leeson travaillait à partir de Singapour. Ses activités ont eu pour effet de faire chuter la banque Barings en Angleterre, la plus vieille institution bancaire de ce pays. On allègue que Leeson lui aurait infligé des dettes de plus de 750 millions de livres sterling. Cette somme aurait été transférée de la Barings de Londres à Singapour au début de l'année 1995. Plusieurs théories sont appliquées par les pays afin d'établir s'ils ont juridiction sur un crime. Voir Geoff GILBERT, *Who has Jurisdiction for Cross-Frontier Financial Crimes ?* (1995) 2 Web *JCLI*

http://www.ncl.ac.uk/~nlawww/articles2/gilb2.html

contrevenant au moment du délit ? Quel droit s'applique à lui ?[75] Comment assurer sa comparution devant les tribunaux compétents ?[76] En vertu de quoi et selon quels mécanismes les pays peuvent-ils punir ceux qui violent leurs lois à partir de sites électroniques localisés à l'extérieur de leur juridiction ?

Une brève analyse de l'illustre cause américaine impliquant les opérateurs de B. É., Carleen et Robert Thomas[77], permet de situer le problème de l'applicabilité sur le territoire d'une juridiction de critères juridiques établis par une autre juridiction. Plus particulièrement, cette

---

[75]Michael Dierks nous rappelle que de façon générale, le droit criminel se concentre sur le lieu de l'activité illicite. Normalement, ce lieu correspond au lieu où se trouve le contrevenant. Par contre, nous savons que dans les environnements électroniques, il est possible que le *situs* de l'activité illicite ne soit pas le même que le *situs* de l'acteur Prenons l'exemple de deux pirates C et D. Imaginons que C habite le Québec et D, New York. Ces pirates pourraient réussir à utiliser, sans permission, les services d'un ordinateur X, situé en Ontario et à endommager les données stockées dans sa mémoire. De façon générale, C répond de la loi canadienne et D, de la loi américaine. Or l'activité de causer des "dommages" au contenu de X se passe au Canada. Dans ces circonstances, est-ce que D répond de la loi canadienne au même titre que C ? Voir Michael DIERKS, *Computer Network Abuse*, Spring 1993, 6 Harvard Journal of Law and Technology 307, 331.

[76]Cette question fait référence, inter alia, à celle de l'extradition. L'extradition est le procédé par lequel une nation livre un suspect à une autre nation qui prétend avoir juridiction pour le poursuivre. Comment les pays peuvent-ils mettre la main sur et/ou punir des malfaiteurs qui se trouvent à l'extérieur de leur juridiction ? Le principe sous-jacent aux États-Unis est "mala captatus bene detentus" ou "mauvaise capture, bonne détention". En d'autres mots, quand le but est de le faire trouver coupable, peu importe la manière qu'un suspect est amené devant la justice pour comparaître. Par exemple, dans une cause américaine récente, des chasseurs de prime ont reçu la somme de $20 000 du Drugs Enforcement Agency (DEA) pour enlever une personne située au Mexique, soupçonnée d'avoir participé à l'assassinat d'un de leurs agents. Selon Geoff Gilbert, en pratique, il faut se demander à quel point une personne irrite le pays et quelles sont les ressources que le pays veut y consacrer ? Il fait alors état des mesures les plus populaires pour faire appliquer la loi à une personne qui se trouve à l'extérieur de la juridiction territoriale d'un pays. Geoff GILBERT, *Who has Jurisdiction for Cross-Frontier Financial Crimes ?*, (1995) 2 *Web JCLI.*

http://www.ncl.ac.uk/~nlawwww/articles2/gilb2.html

[77]Voir note 51.

analyse constitue un prétexte opportun pour mettre à nouveau en cause la pertinence du critère de la norme nationale de tolérance qui sert à établir le caractère obscène du matériel pornographique circulant au Canada.

À partir de Milpitas, en Californie, les conjoints Thomas opéraient le B. É. “Amateur Action” (AABBS) sur lequel ils téléchargeaient du matériel pornographique pouvant être télédéchargé par les abonnés. Bien que physiquement localisé en Californie, on pouvait avoir accès au AABBS au moyen d'un appel téléphonique à partir de n'importe où dans le monde. La configuration du AABBS était celle d'un service pour “adultes seulement”. Les personnes demandant accès au AABS étaient informées de façon claire et sans équivoque qu'il contenait des images à caractère sexuel explicite pouvant choquer certaines personnes. Ceux qui désiraient néanmoins avoir accès à ce service pouvaient le faire moyennant la vérification de leur âge et le paiement du prix d'abonnement de $55,00.

De façon anonyme, un enquêteur du Tennessee s'est abonné au AABBS, a télédéchargé le matériel en question, et a fait entamer une poursuite contre les Thomas par laquelle ils ont été accusés d'avoir commis le crime fédéral de la distribution transfrontalière de matériel obscène[78]. Le 29 juillet 1994, ils ont été déclarés coupables dans la Cour fédérale du District de Western Tennessee[79]. Cette cause a été portée en appel.

Afin de déterminer si du matériel pornographique est obscène, contrairement aux tribunaux canadiens qui appliquent une norme sociale nationale de tolérance, les tribunaux américains appliquent une norme sociale communautaire de tolérance. Ce critère a été promulgué par la Cour

---

[78]Dans le cadre d'une mentalité de responsabilisation des usagers de l'inforoute, l'utilisation de cette technique de *l'entrapment*, dans les circonstances en cause, est-elle justifiée ? Il est clair que l'enquêteur ne faisait pas partie de la communauté des usagers habituels du AABBS. En conséquence, il est loisible de se demander si, sans son intervention, la communauté des usagers habituels du Tennessee aurait jugé à propos de porter une plainte contre les opérateurs Thomas.

[79]The Electronic Frontier Foundation (EFF), *Community Standards in Cyberspace. A Virtual Amicus Brief in the Amateur Action Appeal*, 12 avril 1995.

http://www.eff.org/pub/Alerts/aa_vbrief.html

Suprême des États-Unis en 1973 [80] qui voulait reconnaître et encourager la diversité d'expression qui existe à travers le pays :

> *[O]ur nation is simply too big and diverse for the Court to reasonably expect that [obscenity] standards could be articulated for all 50 States in a single formulation, even assuming the prerequisite consensus exists ... It is neither realistic nor constitutionally sound to read the First Amendment as requiring that people of Maine or Mississipi accept public depiction of conduct found tolerable in Las Vegas, or New York City. [People] in different States vary in their tastes and attitudes, and this diversity is not to be strangles by the absolutism of imposed [uniformity].*

Ce standard fondé sur la perspective de la communauté géographique locale sert à établir un équilibre entre le droit des personnes d'un État d'exercer un contrôle sur le matériel qui pénètre leur communauté et entre le droit des créateurs et distributeurs de matériel d'opérer librement dans les communautés où le matériel ne choque pas les standards prévalents.

Dans l'affaire Thomas, la Cour a donc informé le jury qu'il devait déterminer si le matériel en question était obscène par référence aux points de vue dominants dans la communauté locale du Tennessee. Même si le matériel distribué n'était pas considéré obscène en Californie, les Thomas ont été trouvés coupable au Tennessee, parce que le seuil de tolérance de

---

80 *Miller v. California*, 415 US 15, 33 (1973) .

cette communauté était plus bas que celui de la Californie[81].

Au Canada, vu l'application d'une norme sociale nationale de tolérance, en théorie, un même échantillon de matériel pornographique ne pourrait pas être jugé obscène par le tribunal d'une province et non obscène par le tribunal d'une autre. En fait, une définition régionale ou locale de la “norme de tolérance” ne serait-elle pas plus conforme à la réalité canadienne qui veuille, *inter alia*, que les différentes provinces aient des seuils de tolérance variables ?

Finalement, il pourrait arriver qu'un opérateur de B. É. télécharge du matériel pornographique à partir d'un autre pays où il n'est pas jugé obscène, permettant qu'il soit télédéchargé par un abonné situé au Canada, où on le jugerait obscène. Quelles sont les conséquences, au Canada, d'un tel geste ? Comment distinguer cet exemple de celui d'un résident du Canada qui voyage en Californie pour acheter du matériel pornographique jugé obscène au Canada, qu'il ramène chez lui ? N'avons-nous pas vu déjà que la possession simple de matériel obscène était légale ?[82] L'imposition de sanctions à l'acheteur n'équivaudrait-il pas à limiter son droit à la libre circulation ?

---

[81]Les nouveaux environnements électroniques permettent à des millers de communautés, chacune ayant ses propres standards, de communiquer ensemble et ce, très rapidement. Selon Douglas Barnes, l'impact de cette réalité se fera d'abord ressentir en matière de transmission d'images sexuelles, à l'égard desquelles les normes d'acceptabilité varient. Par exemple, en Arabie Saoudite, la distribution du *Sports Illustrated Online* justifierait probablement l'amputation involontaire du coupable sans anesthésie ; alors qu'à Amsterdam, presque tout est permis, y compris ce que le reste du monde considère être de la pornographie juvénile. Au Japon, la mise à vue d'organes génitaux ne cause pas de problème en soi, mais l'exposition des poils pubiens constitue un motif d'emprisonnement. Aux États-Unis, même les magazines moins osés exposent du poil pubien, avec censure spéciale des organes génitaux, dépendant de la norme communautaire en jeu. Douglas BARNES, *The Coming Jurisdictional Swamp of Global Internetworking, (Or, How I Learned to Stop Worrying and Love Anonymity*), 16 November 1994.

http://www.communities-com/paper/swamp.html

[82]La possession simple de matériel pornographique est également légitime aux États-Unis. Voir *Stanley v. Georgia* 394 US 557 (1969).

Nous suggérons que l'exemple précité soulève les questions supplémentaires suivantes :

- Est-ce que la décision dans *R.* c. *Pecciarich* devrait être maintenue ? En d'autres mots, est-il souhaitable que le fait de télécharger du matériel obscène sur un B. É., permettant qu'il soit télédéchargé par des abonnés intéressés, constitue, en droit, de la distribution au sens de l'article 163 du Code ?

- Si oui, est-ce que le fait de télécharger du matériel obscène sur un B. É. situé dans un autre pays, permettant qu'il soit télédéchargé par un abonné situé au Canada, constitue toujours de la distribution au sens de l'article 163 du Code ? En d'autres mots, est-ce que le fait que le matériel soit téléchargé à partir d'un autre pays change quelque chose à l'application de l'article 163 ?

- Est-il souhaitable qu'une personne qui télécharge du matériel pornographique sur un B. É. à partir d'un pays où il n'est pas jugé obscène puisse faire l'objet d'une poursuite criminelle dans un autre pays où il l'est ?

- Si oui, comment faire appliquer la loi canadienne à cette personne ? Comment l'obliger à comparaître ? Faut-il nécessairement un traité d'extradition entre le Canada et ce pays ? Que faire dans les circonstances où il n'existe pas de traité d'extradition ? Par ailleurs est-il raisonnable d'entamer des procédures d'extradition contre une personne qui a distribué du matériel pornographique obscène ? Si oui, dans quelles circonstances ?

- Aux yeux de la communauté globale et internationale des usagers de réseaux informatiques, la norme nationale de tolérance canadienne ne correspond-elle pas, en fait, à une norme communautaire de tolérance, semblable à celle appliquée aux États-Unis ? Si oui, est-il souhaitable que ce soit le seuil de tolérance des Canadiens qui dicte aux fabricants de pornographie à travers le monde ce que devrait être le contenu

de leur produit ?

- Dans le contexte actuel d'un nombre toujours croissant de personnes qui participent à des communautés “virtuelles”, qui surpassent les frontières physiques, est-il souhaitable que le contenu du matériel qui puisse légitimement pénétrer leur domicile soit dicté par le lieu physique où il se trouve[83] ?

- Comment protéger les intérêts des citoyens canadiens contre ce qu'ils considèrent être les effets néfastes du matériel obscène tout en préservant le droit de groupes ayant des sensibilités différentes de s'associer et de former des communautés qui établissent et appliquent des standards différents ?

- Le problème n'en est-il pas un de définir la communauté à partir de laquelle la norme doit être créée et appliquée, plutôt que de tenter de définir, à une échelle internationale, ce que constitue l'obscénité[84] ?

### 33.1.3 La pornographie juvénile

Au Canada, qu'il soit jugé obscène ou non, le matériel pornographique impliquant des enfants constitue en soi un mode d'expression interdit. Contrairement au matériel obscène, la possession simple de pornographie juvénile est interdite[85]. Sont également réprimées, sa production, son impression, sa publication, ou sa possession en vue de publication[86].

---

[83]Mike GODWIN, *Virtual Community Standards* (30 Jan. 1995).

http://www.eff.org/pub/Publications/Mike_Godwin/obscen_virtcom_stds.article

[84]David LOUNDY, *Whose Standards ? Whose Community ?*, August 1994, Chicago Daily Bulletin 5.

http://www.leepfrog.com/E-Law/CDLB/AABBS.html

[85]Article 163. 1 (4) C. cr.

[86]Article 163. 1 (2) C. cr..

Finalement, sont aussi bannies, son importation, sa distribution, sa vente ou sa possession en vue de distribution ou de vente[87]. Notons que la défense fondée sur la valeur artistique n'est pas admise en matière de pornographie juvénile, alors qu'elle l'est en matière d'obscénité.

En vertu de l'article 163. 1 (a) du Code, la pornographie juvénile s'entend de toute représentation photographique, filmée, vidéo ou autre, réalisée ou non par des moyens mécaniques ou électroniques, 1) soit où figure une personne âgée de moins de dix-huit ans ou présentée comme telle, et se livrant ou présentée comme se livrant à une activité sexuelle explicite, 2) soit dont la caractéristique dominante est la représentation, dans un but sexuel, d'organes sexuels ou de la région anale d'une personne âgée de moins de dix-huit ans. En vertu de l'article 163. 1 (b) du Code, constitue également de la pornographie juvénile, tout écrit ou toute représentation qui préconise ou conseille une activité sexuelle interdite par le Code avec une personne âgée de moins de dix-huit ans.

Dans *R. c. Pecciarich*, l'accusé a démontré que les nouvelles technologies informatiques permettent de fabriquer de la pornographie juvénile sans jamais avoir recours à de vrais enfants. Muni d'un numérisateur, Pecciarich a créé de la pornographie juvénile, en reproduisant des images d'enfants trouvées dans des magazines. Au moyen d'un logiciel informatique, il a altéré ces images de façon à ce qu'elles représentent des personnes de moins de dix-huit ans se livrant à des activités sexuelles explicites.

L'article 163. 1 (1) (a) C. cr. prévoit que la pornographie juvénile se constitue de toute représentation photographique, filmée, vidéo ou autre de personnes de moins de dix-huit ans, réalisée ou non par des moyens mécaniques ou électroniques. Il n'y a donc pas que la pornographie juvénile produite avec la participation d'enfants qui soit bannie. Le législateur a

---

87 Article 163. 1 (3) C. cr.

considéré que la représentation d'enfants se livrant à des activités sexuelles explicites était néfaste en soi, qu'on ait ou non utilisé de vrais enfants[88].

En décembre 1993, l'artiste torontois Eli Langer, a fait l'objet de la première poursuite criminelle en vertu des dispositions canadiennes sur la pornographie juvénile. Bien que les poursuites aient été abandonnées contre sa personne, les oeuvres de Langer ont fait l'objet d'une ordonnance de confiscation en vertu de l'article 164 (4) C. cr[89]. En vertu de l'article 164

---

[88]Aux États-Unis, les rationalités de la répression du matériel pornographique juvénile sont fondées sur un motif de protection des enfants. Grâce aux développement des nouvelles technologies, il est désormais possible de fabriquer de la pornographie juvénile sans utiliser de vrais enfants. Cette réalité suscite présentement de nombreux débats aux États-Unis, puisqu'on se demande si le matériel pornographique juvénile fabriqué sans l'utilisation de vrais enfants est banni. Le juriste Mike Godwin est d'opinion que le matériel fabriqué sans l'utillisation d'enfants ne constitue pas de la pornographie juvénile, mais de la pornographie "simple". En conséquence, cette pornographie "simple" serait soumise au test de l'obscénité (critères de l'arrêt *Miller*) au même titre que n'importe quel autre matériel pornographique. D'autres soutiennent que la pornographie juvénile cause toujours un préjudice aux enfants et ce, même dans les circonstances où elle a été fabriquée sans utiliser de vrais enfants. À leur avis, dans ces circonstances, la simple représentation d'enfants leur cause un préjudice. Le débat reste donc ouvert. D'ailleurs aux États-Unis, des propositions se font présentement en vue de l'adoption d'une loi semblable à la loi canadienne, c'est-à-dire, une loi qui mentionnerait de façon explicite que la pornographie juvénile fabriquée sans utiliser de vrais enfants serait illicite.

[89]Le texte de l'art. 164 se lit ainsi :

> 164 (1) [Mandat de saisie] Le juge émet, sous son seing, un mandat autorisant la saisie des exemplaires d'une publication ou des copies d'une représentation ou d'un écrit s'il est convaincu, par une dénonciation sous serment, qu'il existe des motifs raisonnables de croire :
>
> [...]
>
> *b)* soit que la représentation ou l'écrit, dont les copies sont tenues dans un local du ressort du tribunal, constitue de la pornographie juvénile au sens de l'article 163. 1.

(6)[90] C. cr., il a été interjeté appel de cette ordonnance devant la Cour suprême du Canada, au motif que l'article 163. 1 C. cr. était inconstitutionnel[91]. La Cour Suprême a refusé d'entendre cet appel.

Il est néanmoins loisible de continuer à se demander si 163. 1 C. cr. constitue une limite raisonnable et justifiable au droit à la liberté d'expression. Dans le cadre de la présente étude, cette interrogation est d'autant plus pertinente qu'il est désormais possible de fabriquer de la pornographie juvénile qui puisse circuler dans les environnements électroniques, sans jamais impliquer de vrais enfants.

De façon générale, on soutient que l'interdiction de la production de pornographie impliquant la participation d'enfants se justifie afin de les protéger contre ce genre d'exploitation. Plusieurs arguments s'ajoutent pour justifier la répression d'images d'enfants se livrant à des activités sexuelles explicites, qu'on ait ou non utilisé de vrais enfants pour les produire : 1) il

---

> (4) [Ordonnance de confiscation] Si le tribunal est convaincu que la matière [...] constitue de la pornographie juvénile, il doit rendre une ordonnance la déclarant confisquée au profit de Sa Majesté du chef de la province où les procédures ont lieu, pour qu'il en soit disposé conformément aux instructions du procureur général.

[90]Le par. (6) précise :

> 164 (6) [Appel] Il peut être interjeté appel d'une ordonnance rendue selon les paragraphes (4) [...] par toute personne qui a comparu dans les procédures :
>
> *a)* pour tout motif d'appel comportant une question de droit seulement ;
>
> [...]

[91]Frank ADDARIO ; Paul BURSTEIN ; *Memorandum of Argument*, In The Supreme Court of Canada [On Appeal From The Ontario Court of Justice (General Division)] between Paintings, Drawings, and Photographic Slides of Paintings and Her Masjesty The Queen,

http://insight.mcmaster.ca/org/efc/pages/law/doc/Langer-Appeal-Index.html

existerait un lien causal entre l'utilisation d'images à caractère sexuel explicite impliquant des enfants et la prévalence de l'abus sexuel des enfants ; 2) il existerait un lien causal entre l'existence et l'utilisation d'images à caractère sexuel explicite impliquant des enfants et le phénomène de la pédophilie 3) ces images causeraient un préjudice à la société, et en particulier aux enfants, qui sont présentés comme des objets sexuels.

Ces trois derniers arguments ont été contestés dans la cause des oeuvres de l'artiste Langer. Notamment, des experts en psychologie sociale soutiennent qu'il n'existe pas de preuve tangible à l'effet d'un lien causal entre l'exposition à de la pornographie juvénile et la commission d'abus sexuels sur des enfants. Ils contestent également le fait qu'il existe un lien causal entre les fantaisies sexuelles et les actes commis par les pédophiles. D'autres prétendent que la création d'images d'enfants se livrant à des activités sexuelles explicites par des personnes qui ont été abusées sexuellement lorsqu'elles étaient enfant, peut avoir, pour elles, un effet thérapeutique. Finalement, certains sont d'avis que le fait de permettre que des jeunes soient exposés à de la pornographie juvénile peut constituer une activité bienfaisante, qui se justifie dans un cadre éducationnel.

- Vu qu'il existe déjà des dispositions servant à contrôler le matériel obscène, l'article 163. 1 C. cr. constitue-t-il une limite nécessaire à la liberté d'expression ?

- La répression de la pornographie juvénile, qu'elle ait été fabriquée ou non par des moyens mécaniques ou électroniques, constitue-t-elle une limite raisonnable et justifiable à la liberté d'expression ?

- Est-ce que le fait que la défense fondée sur la valeur artistique ne soit pas admise en matière de pornographie juvénile constitue une limite qui se justifie dans le cadre d'un société libre et démocratique ?

Une des questions majeures qui se posent ici c'est celle de la responsabilité des opérateurs de réseaux face au matériel pornographique

qui circule dans leur système[92]. Les opérateurs de réseaux ont-ils une responsabilité face au matériel pornographique qui quitte, pénètre ou passe par leur site ? Ont-ils l'obligation de surveiller le contenu du courrier électronique qui circule dans leur système ? En droit criminel, ces questions sont pertinentes. Si la réponse est oui, leur responsabilité pourrait en être une de conspirateur, de co-conspirateur, d'accessoire ou de complice[93].

En droit américain, à l'exception des messages transmis au sein de sites publics de discussion, toutes les communications stockées sur un B. É sont protégées par la loi : *Electronic Communications Privacy Act of 1986* (ECPA)[94]. La ECPA permet aux opérateurs de réseaux d'avoir accès aux communications électroniques stockées sur leur système. Par contre, leur pouvoir de disposer de cette information est limité. Par exemple, en matière criminelle, la ECPA leur accorde la discrétion de divulguer aux autorités policières le contenu d'un courrier électronique privé stocké dans leur système, à condition qu'ils en aient pris connaissance par inadvertance et que cette communication paraisse liée à la commission d'un crime.

Selon Mike Riddle, afin de se protéger contre la responsabilité criminelle, les opérateurs de B. É. américains auraient avantage à ne pas faire la surveillance régulière du contenu du courrier électronique qui circule sur leurs réseaux. Par exemple, dans *Cubby* v. *Compuserve*[95], il a été établi que Compuserve n'était responsable que du matériel dont elle avait pris connaissance. D'ailleurs, le fait que le contenu du courrier électronique soit encrypté pourrait servir à réfuter cette connaissance.

---

[92]Mike GODWIN, *Sex and the single sysadmin : The risks of carrying graphic sexual materials*, March/ April 1994, Internet World, accessible à l'adresse suivante : http://www.wff.org/pub/EFF/Frontier_Files/EFF_Files/Legal/obscenity_online.article

[93]D'ailleurs, les autorités policières ont le pouvoir d'obtenir un mandat pour saisir tout matériel considéré comme probablement impliqué dans la commission d'un crime. Selon Mike Riddle, en pratique, ces saisies sont effectuées quand les policiers croient que le propriétaire du matériel est impliqué dans la commission du crime. Voir Mike RIDDLE, *Sysop liability for enroute (and/or encrypted) mail*, November 7 1993.

[94]18 U. S. C.

[95]776 F. Supp. 135 (S. D. N. Y. 1991).

Qu'en est-il au Canada ? Les opérateurs de réseaux ont-ils l'obligation ou même le droit de vérifier le contenu les messages électroniques qui y circulent ?

Il est possible que des images pornographiques circulent dans des sites électroniques à l'insu des personnes qui les opèrent. Par exemple, elles peuvent voyager sous forme de courrier encrypté. Également, le système de stockage et d'envoi de courrier électronique fait en sorte que du matériel pornographique puisse se retrouver dans un lieu électronique, à un certain moment donné, même s'il n'y a pas tiré son origine et même s'il ne finit pas par y aboutir. Il est possible que ce genre de matériel réussisse à s'immiscer dans un site électronique qui n'a pas de vocation sexuelle. Ainsi, les sites électroniques à vocation licite peuvent servir de couverture aux usagers qui veulent faire circuler du matériel illicite.

Qu'en est-il des opérateurs de B. É qui font eux-mêmes la distribution de matériel pornographique jugé licite au Canada mais illicite ailleurs ? Comment pourraient-ils filtrer l'entrée de chacun des usagers qui visitent leur site ? Par exemple, la distribution du matériel peut se passer à l'insu de l'opérateur, si elle s'effectue durant la nuit, au moyen d'un logiciel qui fonctionne de manière automatique ? Cette mise en situation est d'ailleurs bien différente de celle d'un vendeur de revues pornographiques qui prend la décision consciente d'envoyer son produit dans la juridiction qui le poursuit, établissant ainsi l'intention criminelle pour les fins de distribution de matériel obscène. De plus, comment un opérateur B. É. pourrait-il se tenir au courant des lois applicables, à la limite, dans toutes les juridictions du monde ?[96]

Plutôt que de faire reposer la responsabilité sur les épaules des opérateurs de réseaux seuls, n'y aurait-il pas lieu de développer des techniques permettant aux usagers de limiter leur propre accès à certaines informations. Ceci constituerait une certaine censure volontaire de l'information.

---

[96]Mike GODWIN, *Virtual Community Standards*, 30 Jan. 1995.

http://www.eff.org/pub/Publications/Mike_Godwin/obscen_virtcom_stds.article

Notons que certains opérateurs ont décidé de prendre en charge cette responsabilité, qu'ils n'exercent pas toujours de façon démocratique. Par exemple, la compagnie America Online Inc. (AOL), basée à Vienne, a récemment mis fin à l'abonnement de certains usagers suite aux plaintes d'autres usagers à l'effet qu'ils distribuaient de la pornographie juvénile au sein du système. AOL a informé la FBI et a mis fin à leurs abonnements, de façon unilatérale, et ce, sans avis au préalable[97].

### 33.2 Les autres infractions d'ordre sexuel

Le Code criminel reconnaît un certain nombre d'infractions criminelles qui ont trait à la sexualité. Outre la question de l'obscénité et de la pornographie juvénile, on peut noter la nudité, les actions indécentes et l'exhibitionnisme. Dans les circonstances où ces activités se manifestent dans les environnements électroniques, on peut se demander si elles sont couvertes par le Code criminel. Le Législateur ne visait-il pas à réprimer des comportements purement physiques ? En outre, la plupart de ces infractions comportent un aspect relatif au caractère public de la tenue de ces activités. L'article 150, qui précède l'énumération des infractions d'ordre sexuel, définit ainsi "l'endroit public" :

> *Tout lieu auquel le public a accès de droit ou sur invitation, expresse ou implicite.*

---

[97] Benjamin WITTES, *Law in Cyberspace : Witnessing the Birth of a Legal System on the Net*, january 23, 1995, Legal Times S27.

Sans aller plus en profondeur dans l'examen de ces diverses infractions, il semble que ce soit principalement l'interprétation donnée au terme "d'endroit public" et de sa possible transposition en matière d'inforoute qui sera au coeur des développements juridiques futurs. Les listes de discussion ou les babillards électroniques constituent-ils des "endroits publics" ? S'agit-il de "lieux" auxquels le public peut accéder ?[98] L'autre aspect important de toute cette question est le critère de la "norme de tolérance

[98]Sur cette question, il suffit de souligner que l'affaire *R.* c. *Tremblay*, [1993] 2 R. C. S. 932, qui traitait d'une accusation "d'avoir tenu une maison de débauche à des fins de pratique d'actes d'indécence, en contravention au par. 210(1) C. cr.", a discuté de ces deux principes généraux. Bien que la Cour ait été unanime à considérer que *Pussy Cat* constitue un "endroit public", il y a eu divergence sur le fait que les activités reprochées aient eu lieu dans cet "endroit public". Le juge Cory, pour la majorité conclut :

> Ainsi, même si les actes étaient accomplis dans un endroit public au sens du *Code* , ils n'étaient pas accomplis à la vue du public de manière flagrante, mais bien à l'intérieur d'une pièce fermée, dans une relative intimité, et seuls des adultes consentants y participaient.
>
> Toutefois, les juges Gonthier et LaForest, dissidents, concluent plutôt :

sociale", abondamment dégagé dans les pages précédentes.

Enfin, parmi les infractions d'ordre sexuel, on peut noter avec intérêt l'obligation qui est imposée aux responsables de l'accès à un "lieu" où sont commis des actes sexuels interdits de s'assurer que des mineurs ne puissent pas y accéder. La sanction est encore plus importante lorsque le mineur a moins de 14 ans[99]. Cette disposition est particulièrement utile pour les fins qui nous occupent. Toutefois, la principale difficulté demeure le fait que la protection des mineurs est liée en grande partie à la possibilité de les identifier. Ainsi, que l'on soit majeur ou mineur, l'accès à des sites pornographiques ou autres sur les réseaux d'information reste sensiblement le même. Tout au plus, peut-on voir parfois un avertissement à l'effet que ce site est réservé aux 21 ans et plus (âge de majorité fixé aux États-Unis).

---

> Bien que la relative intimité d'une activité soit pertinente, puisqu'elle peut avoir des conséquences sur les attentes des gens, par exemple, elle n'est qu'un des nombreux facteurs à considérer. La distinction entre la nature privée et la nature publique d'un geste ne repose qu'en partie sur le nombre de personnes qui peuvent être témoins des activités en question. Elle repose également sur les *attentes particulières et légitimes du public quant aux activités qui se produiront en privé seulement*, et celles qui peuvent se produire en public. Ces attentes ne se limitent pas à celles qui peuvent être justifiées pour le motif que des personnes ne devraient pas être témoins des activités en question contre leur gré. Elles s'étendent également aux attentes légitimes du public à l'égard de la sphère que tous partagent.

[99]Voir l'article 171 C. cr.

Or, l'effet dissuasif d'un tel avertissement peut certainement être mis en doute.

### 33.2.1 Les jeux, gageures et loteries

Les jeux et loteries constituent en vertu du droit criminel canadien des infractions criminelles. Cette interdiction est cependant assortie d'un certain nombre d'exceptions qui permettent notamment à des gouvernements provinciaux de mettre sur pied ou d'exploiter des loteries[100]. L'article 202 C. cr. prévoit ainsi que commet une infraction de gageure ou bookmaking quiconque :

> i) *volontairement et sciemment envoie, transmet, livre, reçoit quelque message par la radio, le télégraphe, le téléphone, la poste ou les messageries, donnant quelque renseignement sur le bookmaking, la vente d'une mise collective, les paris et gageures, ou destiné à aider au bookmaking, à la vente d'une mise collective, aux paris ou gageures.*

On peut constater avec intérêt que cette disposition ne comporte aucune allusion à la transmission par télécommunication. Cependant, en matière de loteries, la définition semble beaucoup plus large. L'article 206 C. cr. semble interdire toute participation à l'organisation d'une loterie non autorisée. Ainsi commet une infraction quiconque :

> b) *vend, troque, échange ou autrement aliène, ou fait vendre, troquer, échanger ou autrement aliéner, ou amène à vendre, troquer, échanger ou autrement aliéner, ou y aide ou y contribue, ou offre de vendre, de troquer ou d'échanger un lot, une carte, un billet ou autre moyen ou système pour céder par avance, prêter, donner, vendre ou autrement aliéner quelque bien par lots ou billets ou par tout mode de tirage ;*

---

[100] Voir art. 207 C. cr.

> c) *sciemment envoie, transmet, dépose à la poste, expédie, livre ou permet que soit envoyé, transmis, déposé à la poste, expédié ou livré, ou sciemment accepte de porter ou transporter, ou transporte tout article qui est employé ou destiné à être employé dans l'exploitation d'un moyen, projet, système ou plan pour céder par avance, prêter, donner, vendre ou autrement aliéner quelque bien par tout mode de tirage ;*

Pour montrer le potentiel réel du développement de loteries sur le réseau, il suffit de mentionner que le Liechtenstein a été le premier État à lancer une loterie sur l'Internet : "l'Interlotto"[101].

### 33.2.2 La trahison et la sédition

Les crimes de trahison et de sédition remontent à l'époque royale. Il s'agit principalement de crimes qui visent à assurer le maintien des autorités en place. La trahison implique une communication de renseignements à des autorités étrangères qui auraient pour effet de porter atteinte à la sécurité du Canada[102]. Ce crime s'apparente à la *"felony"* du droit américain. Quant à

---

[101]Information reçue par abonnement à la liste cyberia : cyberia-l@warthog.cc.wm. edu ; parue dans la revue *Information Week* du 23 octobre 1995. Pour participer à la loterie du Liechtenstein, il suffit de s'adresser à l'adresse suivante :

http:www.interlotto.li

[102]Voir art. 46(2)*b)* C. cr. :

> 46. (2) [Trahison] Commet une trahison quiconque, au Canada, selon le cas :
>
> [...]

la sédition (art. 59 C. cr.), c'est la communication de renseignements ou d'informations qui visent, sans autorité législative, à préconiser un changement de gouvernement par l'usage de la force.

Ces crimes ont fait l'objet de peu de poursuites et semblent indiquer un respect notable de la démocratie, tant par les gouvernants des dernières décennies que par les citoyens eux-mêmes[103]. Par ailleurs, la possibilité que resurgissent de tels crimes dans les environnements électroniques n'est pas à repousser du revers de la main puisque le terrorisme international constitue l'un des enjeux majeurs de la réalité mondiale actuelle[104]. Or, plusieurs acteurs politiques reconnaissent dans l'inforoute un mode de communication important dans l'organisation des actes terroristes.

## 34. Les atteintes à la dignité et à la sécurité des personnes

Les activités informationnelles violant le droit à la dignité des personnes sont celles qui ne reconnaissent pas la personne humaine comme une fin en soi, c'est-à-dire comme une personne qui mérite respect, sécurité et valeur. La dignité est un concept suffisamment large pour englober l'ensemble des droits fondamentaux reconnus à l'être humain, y inclus le droit à l'égalité.

---

> *b)* sans autorisation légitime, communique à un agent d'un État étranger, ou met à la disposition d'un tel agent, des renseignements d'ordre militaire ou scientifique ou tout croquis, plan, modèle, article, note ou document de nature militaire ou scientifique, alors qu'il sait ou devrait savoir que cet État peut s'en servir à des fins préjudiciables à la sécurité ou à la défense du Canada.

[103]L'une des plus importantes décisions en cette matière est *Boucher v. The King*, [1951] R. C. S. 265.

[104]Notons qu'en France, *les appels téléphoniques malveillants et les agressions sonores (sont) désormais incriminés parmi les atteintes à l'intégralité de la personne* (art. 222-16 du noveau code pénal) et peuvent être considérés comme des actes de terrorisme. Voir à ce sujet Marie Elisabeth CARTIER, *Le terrorisme dans le nouveau code pénal français* (avr. - juin 1995) 2 *Rev. sc. crim*. 225, 229.

En ce sens, les activités énoncées ci-dessous comportent toute une atteinte à cette dignité.

### 34.1 Le harcèlement *("Stalking")*

Le thème du harcèlement est emprunté ici aux seules fins d'illustrer l'infraction de "stalking" bien connue en droit américain. Cette infraction est une innovation californienne qui a été largement suivie dans plusieurs autres États américains[105]. Ces lois visaient essentiellement à prévenir les actes d'agression, en permettant aux policiers d'intervenir dès qu'une personne se sentait "traquée" ou poursuivie[106]. *The motive behind stalking*

---

[105]L'auteur Eileen Ross écrit que depuis deux ans, ce sont 48 États qui ont adopté des lois crimininalisant le "stalking" : Eileen S. ROSS, *E-Mail stalking : is adequate legal protection available ?*, (1995) XIII *Journal of Computer & Information Law*, 405.

[106]La loi du Michigan, Mich. Stat. Ann. § 750. 411h(1)(c), (d) (e) (vi), (2) (WL 1995), distingue les termes de harcèlement et de stalking :

> *(c)* "Harassment" means conduct directed toward a victim that includes, but is not limited to, repeated or continuing unconsented contact, that would cause the victim to suffer emotional distress. Harassment does not include constitutionally protected activity or conduct that serves a legitimate purpose.
>
> *(d)* "Stalking" means a willful course of conduct involving repeated or continuing harassment of another individual that would cause a reasonable person to feel terrorized, frightened, intimidated, threatened, harassed, or molested, and that actually causes the victim to feel terrorized, frightened, intimidated, threatened, harassed, or molested.

Notons que parmi les actions considérées comme des "unconsented contact", on note à l'article 411h. (1)(e), al. (vi) le fait d'envoyer du courrier ou des communications électroniques à une personne. Une personne trouvée coupable de "stalking" peut encourir une peine d'emprisonnement d'au plus un an ou une amende d'au plus 1000$ (§411h. (2)).

*legislation is to eradicate the frustration of being unable to protect the victims of violence before the violence occurs*[107].

On peut penser que cette action de traquer puisse se réaliser dans le contexte de l'Internet. Des exemples américains le confirment : les affaires Archambeau[108] et Powell. Dans ce dernier cas, une femme était constamment assaillie par un auteur de courrier électronique qui menaçait de violer sa fille et qui a fait connaître son adresse à plusieurs millions d'usagers du réseau, les incitant ainsi au harcèlement.

Un équivalent au crime de "stalking" se retrouve dans notre Code criminel à l'art. 372 (3)[109]. Il apparaît sous la section relative aux "*Faux et*

---

[107]David K. McGRAW, *Sexual Harassment in Cyberspace : The Problem of Unwelcome E-Mail*, 1995, 21 Rutgers Computer and Technology Law Journal 491, 509. L'auteur nous renvoie aux articles suivants : Laurie SALAME, *A National Survey of Stalking Laws : A Legislative Trend Comes to the Aid of Domestic Violence Victims and Others*, 1993, 22 Suffolk U. L. Rev. 67 et Robert A. GUY, *The Nature and Constitutionality of Stalking Laws* (1993) 64 *Vand. L. Rev.* 991.

[108]Voir E. S. ROSS, précité, 407. L'affaire Jane et Archambeau du Michigan a été le premier cas de poursuite pour le crime de stalking par courrier électronique. Après avoir entretenu entre eux une "relation de communication par courrier électronique", Jane a demandé à Archambeau qu'il cesse de communiquer avec elle. Il a insisté en lui faisant transmettre une vingtaine d'autres messages. Elle a donc porté plainte sous la loi Anti-stalking : *State v. Archambeau*, No. 2404-4039-SM (47th D. Mich. pending until Spring 1995).

[109]Il semble intéressant de noter que l'objectif poursuivi par les lois anti-stalking de permettre aux policiers d'intervenir avant que n'aient lieu les actes de violence trouve un équivalent à l'art. 810 C. cr. qui permet qu'une ordonnance judiciaire soit émise à l'effet d'engager l'auteur de menaces de voies de fait à ne pas troubler la paix. Une telle dénonciation doit être portée devant le juge de paix. La professeur Hélène Dumont donne quelques exemples ayant donné lieu à de telles ordonnances :

*infractions similaires"*[110]. Notons cependant déjà que d'autres instruments juridiques interdisent le "harcèlement" qui est une composante même du crime de "stalking"[111]. En ce sens, l'interdiction du harcèlement peut permettre, dans une large mesure, de limiter les cas de "stalking". L'article 372 précise ainsi :

> ***372.*** *(1) [Faux messages] Est coupable d'un acte criminel et passible d'un emprisonnement de deux ans quiconque, avec l'intention de nuire à quelqu'un ou de l'alarmer, transmet ou fait en sorte ou obtient que soit*

---

> Un ordre de garder la paix a été émis à l'encontre d'une personne qui faisait un nombre important de coups de téléphone à une plaignante (*McKenzie* c. *Martin*, [1954] R. C. S. 361). Un homme a reçu un ordre de garder la paix alors qu'il poursuivait et harcelait systématiquement une femme sur la rue (*R.* c. *Poffenroth*, [1942] 2 W. W. R. 362, (1942) 78 C. C. C. 181 (Alta. Police Ct.)). La frayeur causée à une personne au point de lui faire croire qu'on endommagerait ses biens peut donner ouverture à l'ordonnance de l'article 810 C. cr. (*Moses* c. *Enns*, [1981] 2 W. W. R. 440 (Man. C. A.)).

Voir Hélène DUMONT, *Pénologie : Le droit canadien relatif aux peines et aux sentences*, Montréal, Éd. Thémis, 1993, p. 533.

[110]Par ailleurs, les infractions de "menace" (art. 264. 1 (1) *a)* du C. cr.) ou d'"intimidation" (art. 423 C. cr.) peuvent avoir des composantes similaires au crime de stalking. Le crime de menace sera abordé au point suivant, alors que le crime d'intimidation ne couvre pas le harcèlement par courrier électronique, ni même par téléphone. Cette infraction peut avoir lieu lorsqu'une personne suit avec persistance une autre personne de place en place ; prive une personne de l'usage de ses biens ou fait obstacle à un tel usage ; cerne ou surveille le lieu où cette personne réside, travaille ou exerce son entreprise, dans le dessein de la forcer à s'abstenir de faire une chose qu'elle a le droit de faire ou de l'obliger à faire ce qu'elle peut légalement s'abstenir de faire.

[111]Voir à ce sujet la *Loi canadienne des droits de la personne*, L. R. C. (1985), c. H-6 En outre, pour plus de détails relativement au harcèlement, dans le contexte d'un recours civil, on peut se reporter à la section sur la responsabilité civile.

> *transmis par lettre, télégramme, téléphone, câble, radio* ou autrement, *des renseignements qu'il sait être faux.*
>
> *(2) [Propos indécents au téléphone] Est coupable d'une infraction punissable sur déclaration sommaire de culpabilité par procédure sommaire quiconque, avec l'intention d'alarmer ou d'ennuyer quelqu'un, lui tient au cours d'un appel téléphonique des propos indécents.*
>
> *(3) [Appels téléphoniques harassants] Est coupable d'une infraction punissable sur déclaration sommaire de culpabilité par procédure sommaire quiconque, sans excuse légitime et avec l'intention d'harasser quelqu'un, lui fait ou fait en sorte qu'il lui soit fait des appels téléphoniques répétés.*

Les principales remarques qui peuvent être formulées à l'égard de ces dispositions sont d'abord le fait que le par. (1) se distingue de l'infraction de la diffusion de fausses nouvelles de l'art. 181 C. cr., déclaré inconstitutionnelle dans l'affaire *Zundel*. La principale distinction semble relever du fait que l'art. 181 C. cr. exigeait qu'il y ait atteinte à "un intérêt public", alors que l'art. 372(1) exige que le message ait été communiqué "avec l'intention de nuire à quelqu'un ou de l'alarmer". Cette disposition, par les termes "*ou autrement*", trouverait sans doute application dans le contexte des environnements électroniques.

Les deux par. suivants, cependant, sont intimement liés au mode de communication téléphonique. On peut certainement penser qu'au moment de la rédaction de cet article, le téléphone constituait le mode de communication le plus intrusif et il le demeure sans doute encore. Toutefois, le courrier électronique s'en rapproche de façon non négligeable. Ainsi, à moins que les termes de ces dispositions soient modifiés pour inclure le courrier électronique, le "stalking" par courrier électronique demeurerait non couvert au Canada.

Le terme "indécent" du par. (2) permet aussi de s'interroger sur la norme à appliquer. S'agit-il encore de la "norme de tolérance sociale" ou plutôt du degré de tolérance de la personne qui reçoit le message ?

Toujours sous la section relative aux *Faux et infractions similaires*, on peut noter l'existence d'une interdiction relative à l'envoi de télégrammes, de câblogramme ou de messages radiophonique sous un faux nom (art. 371 C. cr.) ainsi qu'une interdiction de rédiger un document, toujours avec l'intention de frauder, pour le compte d'une autre personne, peu importe son mode de transmission (art. 374 C. cr.).

Aux État-Unis, quatre États ont élargi la portée de leurs lois anti-stalking pour y inclure le *E-mail Stalking*[112] : il s'agit des lois du Michigan, de l'Alaska, de l'Oklahoma et du Wyoming. En effet, il n'est pas certain que seule une interprétation des dispositions existantes permette de couvrir les cas de harcèlement répétitif par courrier électronique, puisque dans certains cas, un contact physique est exigé.

Toutefois, plusieurs auteurs estiment que ces "stalking laws" ne respectent pas le *due process of law*, garanti au quatorzième amendement du *Bill of Rights* américain qui mentionne que *No State shall (...) deprive any person of life, liberty, or property, without due process of law.* Deux arguments d'inconstitutionnalité sont surtout avancés à l'encontre de la Loi du Michigan. Il y a d'abord le caractère vague du crime[113] ainsi que le fait que la disposition, telle que rédigée, crée une *mandatory rebuttable presumption*, c'est-à-dire que la loi porte atteinte à la présomption d'innocence et à l'exigence, en droit criminel, de faire la preuve hors de tout doute raisonnable pour chacun des éléments du crime et non, une preuve par

---

[112] E. S. ROSS, précité, 407.

[113] Le caractère vague signifie que le comportement réprimé ou interdit n'apparaît pas clairement pour une personne d'intelligence ordinaire et que la loi n'élimine pas une application subjective de celle-ci. Plus précisément, on estime que la loi n'exige pas que l'auteur de stalking ait l'intention spécifique de terroriser, effrayer, intimider, etc. la victime et c'est en cela que la loi serait inconstitutionnelle. C'est le terme "willful" qui permet d'en arriver à cette conclusion, de même que l'importance reconnue aux émotions de la victime ("that would cause" et "emotional distress"), plutôt qu'à l'intention de l'auteur. Aussi, la définition même des contacts non consentis n'exige pas que la victime ait informé l'auteur de son absence de consentement. Voir E. S. ROSS, précité, 415 et suiv., citant l'affaire *Grayned v. City of Rockford*, (1972) 408 U. S. 104.

présomption[114]. Transposé dans notre droit, la création d'une telle infraction devrait respecter les articles 7 et 11 de la *Charte canadienne*, c'est-à-dire surtout, le droit pour tout accusé de "comprendre" le sens de l'infraction qui lui est reprochée et le droit de jouir entièrement de la présomption d'innocence et d'être jugé coupable hors de tout doute raisonnable sur chacun des éléments du crime reproché[115].

Au niveau fédéral américain, les cas de harcèlement ont amené la proposition du congressiste Mfume à l'effet d'amender la *Communications Act of 1934* [116] qui comporte une partie intitulée *Federal Telephone Harassing Statute*. L'adoption de l'*Electronic Anti-Stalking Act*[117] aurait

---

[114]Ainsi, par exemple, dans le cas de la loi du Michigan, l'auteure Ross estime qu'un jury appelé à juger d'une affaire d'*e-mail stalking* serait invité à tenir compte du comportement de la victime plutôt que celui de l'accusé et ainsi à considérer si la victime s'est ou non sentie effrayée du seul fait que la preuve démontre la répétition de contacts non consentis par télécourrier. Une telle présomption a déjà été jugée inconstitutionnelle par la Cour suprême américaine dans *Francis v. Franklin*, 471 U. S. 307 (1985). E. S. ROSS, précité, pp. 422 et suiv.

[115]L'article 7 de la Charte canadienne garantit à chacun *le droit à la vie, à la liberté et à la sécurité de sa personne* et exige qu'il ne soit *porté atteinte à ce droit qu'en conformité avec les principes de justice fondamentale*. Dans la Charte québécoise, ce principe est affirmé avec moins de ferveur. Ce sont les articles 23 et suivants qui précisent les droits judiciaires. À l'article 23 on peut lire que :

> Toute personne a droit, en pleine égalité, à une audition publique et impartiale de sa cause par un tribunal indépendant et qui ne soit pas préjugé, qu'il s'agisse de la détermination de ses droits et obligations ou du bien-fondé de toute accusation portée contre elle.

Toutefois, l'article 24 précise que : *Nul ne peut être privé de sa liberté ou de ses droits, sauf pour les motifs prévus par la loi et suivant la procédure prescrite*. Une telle disposition semble avoir pour effet de placer la loi au-dessus du droit à un processus judiciaire juste et équitable.

[116]47 U. S. C. §223 (1989).

[117]H. R. 5015, 103 d Cong., 2d Sess. §223 (1994) ; devenue H. R. 112, 104d Cong., 1st Sess. §223 (1995).

pour effet d'inclure dans le terme “téléphone” et “appel téléphonique” toute communication par le moyen d'un modem informatique et toute autre communication bidirectionnelle par fil ou radio télécommunications[118]. Cette proposition suscite également des critiques. Ainsi, l’auteure Ross considère que l'assimilation du courrier électronique à de la communication vocale par téléphone n'est pas sans conséquence. Dans le dernier cas, la communication est directe et la voix de l'appelant peut manifester certaines intonations ou doutes, la personne appelée peut raccrocher subitement pour démontrer son refus de communiquer ou manifester sa colère ou tout autre sentiment. Toutefois, dans le cas du télécourrier, la conversation est réalisée en différé, à la manière du courrier régulier et surtout, nul n’est alors tenu de lire le courrier qui lui est transmis.

Enfin, une autre proposition émanant du fédéral a été formulée par les sénateurs Exon et Coats, intitulée *Communications Decency Act of 1995*. Celle-ci est à l'effet d'amender le *Communications Act of 1934*, et particulièrement la section 223 pour édicter le crime suivant[119]:

*(a) Whoever*

---

[118]Le texte de la proposition se lit ainsi :

> SECTION 1. SHORT TITLE.
>
> This Act may be cited as the `Electronic Anti-Stalking Act of 1995'.
>
> SECTION. 2. AMENDMENT.
>
> Section 223(a) of the Communications Act of 1934 (47 U. S. C. 223(a)) is amended by adding at the end thereof the following new sentence : `For purposes of subparagraphs (B), (C), and (D), the terms `telephone' and `telephone call' include communications by means of computer modem or any other two-way wire or radio telecommunications device.

[119]Voir Amendment No 1362, S. 653 :

http://www.eff.org/pub/Alerts/s652|95|a1362|exon|coats.amend

*(1) in the District of Columbia or in interstate or foreign communications*

*(A) by means of telecommunications device knowingly-*

*(i) makes, creates, or solicits, and*

*(ii) initiates the transmission of,*

*any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person ;*

*(B) makes a telephone call or utilizes a telecommunications device, whether or not conversation or communications ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communication ;*

*(C) makes repeated telephone calls or repeatedly initiates communication with a telecommunications device, during which conversation or communication ensues, solely to harass any person at the called number or who receives the communication ;*

*[...]*

*(2) knowingly and willfully permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be so-used for such activity,*

*shall be fined not more than $100,000 or imprisoned not more than two years, or both.*

Pour l'auteur Ross, cette disposition ouvre la voie à des poursuites criminelles fédérales pour les actes de “flaming”, définis comme étant une communication non consentie et anonyme par laquelle on indique à une

personne qu'elle a violé les règles de conduite, dans des termes peu élogieux (*"messages full of personal invective"*[120]). Même le harcèlement, sans nécessité de stalking, serait ici criminalisé. Cela pourrait ouvrir la voie à des poursuites frivoles, estiment certains auteurs. De plus, l'obligation d'identification pourrait donner lieu à une contestation au motif qu'elle viole la liberté de parole[121], mais aussi, la *Communications Decency Act* pourrait porter atteinte au droit à la vie privée[122]. Malgré cela, on estime qu'il demeure possible d'adopter une loi qui répondrait aux véritables enjeux de ce problème tout en étant constitutionnelle[123].

---

[120]E. S. ROSS, précité, 428.

[121]Voir sur cette question Vickie BELL and Denise DE LA RUE, *Gender Harassment on the Internet* :

http://www.gsu.edu/~lawppw/lawand.papers/harass.html

[122]Michael S. EVANS et Rebecca C. STONE, *Communications Decency Act Abridges Constitutional Freedoms : A Recommendation for a Free Internet*, 1995, disponible à l'adresse suivante :

http://www.gsu.edu:80/~lawppw/lawand.papers/cda.html

[123]Voir à ce sujet le "MODEL STATE ANTI-STALKING STATUTE", présenté par E. S. ROSS, précité, reprenant National Criminal Justice Association, *Project to develop a Model Anti-Stalking Code for States* (1993) :

> §1. A person commits the crime of stalking if that person :
>
> A) intends to engage in a course of conduct directed at the victim, or an immediate family member, that would cause a reasonable person to fear death or bodily harm ; and
>
> B) knows or should know that a particular course of conduct would cause a reasonable person to fear death or bodily harm ; and
>
> C) actually causes the victim, or an immediate family member, to fear death or bodily harm.

Rappelons enfin que les articles 10 et suivants de la *Charte des droits et libertés de la personne* garantissent le droit à l'égalité en interdisant le harcèlement et toute autre forme de discrimination.

> *10. Toute personne a droit à la reconnaissance et à l'exercice, en pleine égalité, des droits et libertés de la personne, sans distinction, exclusion ou préférence fondée sur la race, la couleur, le sexe, la grossesse, l'orientation sexuelle, l'état civil, l'âge sauf dans la mesure prévue par la loi, la religion, les convictions politiques, la langue, l'origine ethnique ou nationale, la condition sociale, le handicap ou l'utilisation d'un moyen pour pallier ce handicap.*
>
> *Il y a discrimination lorsqu'une telle distinction, exclusion ou préférence a pour effet de détruire ou de compromettre ce droit.*
>
> *10. 1 Nul ne doit harceler une personne en raison de l'un des motifs visés dans l'article 10.*

---

§2. Definitions :

A) "Course of conduct" means a series of two or more acts that communicate the threats directed at a specific person.

B) "Communicate" means communicating with another through implied conduct or by verbal, written, or electronic means.

C) "Immediate family" members include a spouse, child ans sibling or any individual that has resided in the household for at least one year.

En outre, une personne dont les droits ont été atteints peut porter plainte à la *Commission des droits de la personne* pour obtenir réparation contre l'auteur de l'acte fautif[124]. Par ailleurs, une difficulté propre aux recours civils est le fait que la victime doive s'engager dans un processus judiciaire coûteux et parfois émotivement douloureux. De là, estiment certains, l'avantage de criminaliser de telles pratiques, laissant ainsi au ministère public la charge financière de la poursuite. Une telle solution implique cependant une activité gouvernementale sur les réseaux et la création possible d'une police qui pourrait s'immiscer dans les communications électroniques, ce qui, à notre avis, ne constitue pas nécessairement la meilleure alternative[125].

[124]Voir art. 74 et suiv. de la Charte québécoise.

[125]À l'heure des coupures budgétaires des États on peut imaginer d'autres solutions qui impliqueraient une plus grande participation de la part des usagers. Cette question méritera de plus amples études.

### 34.2 Les menaces

La “menace” est définie, dans le langage courant, comme étant l'*expression du projet de nuire à autrui*[126]. Les cas de menace, dans les environnements électroniques, peuvent sans doute s'accompagner du crime d'extorsion, de l'article 346 C. cr., c'est-à-dire le fait de forcer quelqu'un à faire quelque chose, sans son consentement, sous la force de menaces, d'accusations ou d'actes de violence. Le recours à la menace, dans la résolution des conflits ou même dans leur création, peut être emprunté pour des motifs variés, allant de l'incapacité de faire valoir ses idées au besoin d'argent[127].

Le crime de menace, énoncé à l’article art. 264. 1 (1) *a)* C. cr., est relativement limité. Il exige qu’une personne *sciemment profère, transmet ou fait recevoir par une personne, de quelque façon, une menace* :

> *a)* de causer la mort ou des blessures graves à quelqu’un ;
>
> *b)* de brûler, détruire ou endommager des biens meubles ou immeubles ;
>
> *c)* de tuer, empoisonner ou blesser un animal ou un oiseau qui est la propriété de quelqu’un.

Selon les termes de cette disposition, il semble clair qu’une menace puisse avoir lieu dans le contexte des environnements électroniques et ce qui semble particulièrement intéressant, c’est le fait qu’il n’est pas nécessaire que la menace soit adressée à la personne qui pourrait être victime de la réalisation de la menace. Il n’est pas nécessaire non plus que la personne visée par la menace ait l'impression que sa vie ou sa sécurité soit en danger. En outre, la menace peut, dans certaines circonstances, s'accompagner ou avoir été précédée de harcèlement.

---

[126] Petit Robert 1.

[127] On doit noter que le crime d’extorsion qui interdit à quiconque d’induire une personne à accomplir ou faire accomplir quelque chose en recourant à des menaces, des accusations ou de la violence peut donner ouverture à l’extradition. Voir Annexe I (18) de la *Loi sur l’extradition*, L. R. C. (1985) c. E-23.

Les dommages qui peuvent être encourus par les menaces, c'est d'abord et certainement la réalisation du projet évoqué dans celle-ci. Également, on pourrait trouver tous les autres sentiments de peur, d'angoisse, etc. qui résultent du harcèlement. On peut également ajouter ici le crime de "torture" qui, en raison de son énoncé, pourrait se voir appliquer dans le contexte des environnements électroniques :

> *acte, commis par action ou omission, par lequel une douleur ou des souffrances aiguës, physiques ou mentales, sont intentionnellement infligées à une personne.*

Énoncé à l'article 269. 1 C. cr., on ajoute ensuite qu'on pourra considérer qu'il y a torture pour tout motif fondé sur quelque forme de discrimination que ce soit. En fait, on semble voir ici un parallèle intéressant avec le crime de "stalking" en droit américain, abordé plus haut.

Sur cette question des menaces dans l'environnement électronique, l'affaire Jake Baker est d'un intérêt tout particulier. C'est l'histoire d'un étudiant du Michigan qui a diffusé ses fantasmes sexuels sur le réseau, notamment dans les listes de discussion (*Usenet newsgroups* : alt. sex. stories). Dans une de ses histoires, une étudiante était nommément désignée comme "victime" de ses fantasmes avec violence. Par hasard, une jeune fille russe est tombée sur ce message qu'elle a trouvé effroyable. Elle en a parlé à son père qui en a ensuite parlé à un ami, un ancien de l'Université du Michigan. Ce dernier s'est plaint à l'Université qui a dû entreprendre des procédures pour fouiller l'ordinateur et la chambre de Baker. La police y trouva alors des communications privées entre Baker et un dénommé Gonda (de l'Ontario - Canada) qui avaient comme objet des discussions à caractère sexuel et violent. Mike Godwin, dans un article récent s'interroge à savoir si le fait de transmettre de telles informations constitue ou devrait constituer un crime[128].

L'une des premières questions qu'il faut se poser, c'est d'abord la qualification du message. S'agit-il de récits fantastiques, de menaces, de harcèlement, de corruption des moeurs, de diffamation ou de communications privées bénéficiant d'une pleine protection sous le premier

---

[128]Mike GODWIN, *Artist or Criminal ?*, 1995, Internet World 96.

amendement ?[129] Il semble d'ailleurs que le défaut d'une bonne qualification ait ici contribué à l'échec des procédures[130]. En effet, les policiers fédéraux ont poursuivi Baker sous le Titre 18 U. S. C. §875*c)* qui prévoit que [traduction] *la transmission (interétatique) de message qui contient toute menace d'enlèvement d'une personne ou toute menace de causer des dommages corporels à une personne* est interdite. Dans son plaidoyer, le procureur prétend que [traduction] *la transmission contient une menace si une personne raisonnable perçoit le message comme étant l'expression sérieuse de l'intention d'infliger des blessures à une personne ou de l'enlever*. Or, puisque Baker avait pris la peine d'indiquer dans toutes ses communications qu'elles constituaient des oeuvres de fiction, le juge a conclu que l'enthousiasme des policiers pour une histoire dégoûtante mais fictive devait mener à l'acquittement de Baker.

### 34.3 Les informations dangereuses

Parmi les informations dangereuses qui pourraient circuler sur les réseaux d'information, on peut penser aux directives sur la procédure à

---

[129]En vertu de notre Code criminel, on peut penser que le procureur général aurait pu poursuivre pour violation de l'article 163(1) sur la corruption des moeurs en raison de la mise en circulation de "publication obscène", signifiant une exploitation indue des choses sexuelles ou une exploitation de choses sexuelles et d'un ou des sujets suivants : crime, horreur, cruauté ou violence. Dans ce cas, l'emprisonnement maximal serait de deux ans.

[130]Il était impossible de poursuivre sous le crime de mise en circulation de matériel obscène puisque l'affaire *United States v. Carlein Communications*, 815 F. 2d 1367 (1987) avait exigé que ce terme était *restricted in its terms to the transportation of tangible objects*.

suivre pour se suicider[131], à des informations relatives à la confection de bombes, ou à toute autre information qui aurait la qualité ou le "pouvoir de nuire ou d'exposer à un danger, c'est-à-dire qui menace ou compromet la sûreté, l'existence d'une personne ou d'une chose". Les informations ne sont toutefois pas susceptibles d'être qualifiées de "dangereuses" pour toutes les personnes. Dans certains cas, des informations ne seront dites dangereuses qu'à l'égard des personnes les plus vulnérables, comme les enfants ou les personnes souffrant de problèmes mentaux et de dépression.

Un des éléments qui permet de qualifier certaines informations de dangereuses peut être de les relier à certaines infractions criminelles. Or, dans le cas du suicide, il convient de souligner que l'article 271 C. cr. interdit à quiconque de conseiller à une personne de se donner la mort ou de l'aider ou de l'encourager à se donner la mort.

### 34.4 La diffamation criminelle

La diffamation, dans le langage courant, se définit comme "toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé". En ce

---

[131]En effet, que penser d'un site donnant accès à *des instructions détaillant, étape par étape, la façon de se suicider ?* (le *Death Net*). Ces services menacent-ils la santé des adolescents ou des personnes à tendance suicidaire ? Sans doute que l'accès facile à de telles informations peut pousser une personne, qui en est déjà loin dans son stade dépressif, à passer aux actes, selon la procédure précisée. Toutefois, il existe des livres qui donnent de telles indications et pour lesquels on peut reconnaître le même genre de risque. On doit plutôt s'interroger sur les causes profondes du suicide. Souvent, on peut penser que celui-ci constitue un soulagement pour ceux qui le commettent. Par ailleurs, on doit se demander si l'accès à de tels renseignements peut inciter une personne en bonne santé mentale à se suicider ? Plusieurs, avec nous, en douteront. Voir PC, *Le suicide sur Internet*, Le Devoir, 13 mars 1995, A3. Une solution à envisager dans ces cas particuliers serait de créer ou d'inciter à la création de sites d'informations visant à prévenir le suicide ou encore d'imposer à ceux qui détiennent les sites d'informations à caractère de risque, d'offrir des alternatives, par des liens les rattachant à des services psychologiques ou autres. En fait, sur cet aspect, il semble que ce soit plus une solution sociale que criminelle qui devrait être envisagée.

sens, le mensonge n'est pas nécessaire pour qu'il y ait diffamation[132].

Généralement, la diffamation peut faire l'objet de recours civils en responsabilité délictuelle pour atteinte à la réputation ou à la vie privée. La diffamation criminelle suppose cependant l'existence d'une diffamation très grave. Dans le *Code criminel*, ce sont principalement les articles 296 et suiv. qui criminalisent ce genre d'activités, en posant une présomption de responsabilité sur le propriétaire du journal où est publié cette information (art. 303 C. cr.). Cette présomption appellerait une réflexion supplémentaire sur l'application de celle-ci à un opérateur de réseaux ou de babillards électroniques. On admet ainsi la présomption de responsabilité du propriétaire à moins qu'il ne prouve que la matière diffamatoire a été insérée à son insu et sans négligence de sa part. Le "journal" est défini à l'article 297 C. cr. comme étant :

> *Tout journal, magazine ou périodique contenant des nouvelles, renseignements ou comptes rendus d'événements d'intérêt public, ou des remarques ou observations à leur sujet, imprimé pour la vente et publié périodiquement [...]*

Ainsi, cette définition exige un document imprimé, ce qui pourrait repousser l'application de la présomption aux documents numérisés. En outre, on peut soupçonner qu'une telle présomption puisse aller à l'encontre de l'exigence constitutionnelle de la présomption d'innocence. Notons que d'autres infractions ont dans le Code criminel des composantes semblables au libelle diffamatoire : le libelle séditieux et le libelle blasphématoire[133]. Ces crimes semblent toutefois être tombés en désuétude[134].

---

[132]Le Code criminel crée d'ailleurs une infraction distincte pour le libelle diffamatoire faux : art. 300 C. cr.

[133]Voir Douglas A. ALDERSON, *The constitutionalisation of Defamation : American and Canadian Approaches to the Constitutitional Regulation of Speech*, 1993, 15 Advocates Quarterly 385-424. Il écrit qu'en 1984, la Commission du Canada de Réforme du droit avait proposé l'abolition de ce crime.

[134]Il semble qu'aucune poursuite n'ait été intentée pour diffamation criminelle depuis la deuxième guerre. Une recherche plus approfondie sur le thème du libelle et de la diffamation dans les environnements électroniques pourra être réalisée dans une phase ultérieure.

Ainsi, le libelle diffamatoire se définit comme “une matière publiée sans justification ni excuse légitime (qui est) de nature à nuire à la réputation de quelqu’un en l’exposant à la haine, au mépris ou au ridicule, ou destinée à outrager la personne contre qui elle est publiée”[135]. Il n’est pas nécessaire de recourir à des mots pour qu’il y ait un libelle diffamatoire, un objet qui aurait une telle signification pourrait suffire. En outre, on doit souligner que le mot “publication” signifie ici :

> ***299.*** *Une personne publie un libelle lorsque, selon le cas :*
>
> a) *elle l’exhibe au public ;*
>
> b) *elle le fait lire ou voir ;*
>
> c) *elle le montre ou le délivre, ou le fait montrer ou délivrer, dans l’intention qu’il soit vu par la personne qu’il diffame ou par toute autre personne.*

Ainsi, il est facile d’imaginer des cas de diffamation sur l’Internet et le texte actuel du Code permet de considérer que l’envoi de messages électroniques sur le réseau, que ce soit par courrier électronique ou dans une liste de discussion, suffirait à ce qu’il y ait “publication” du message[136]. Enfin, rappelons que le libelle diffamatoire peut donner lieu à des dommages punitifs en vertu de l’article 728 C. cr. Comme le note la professeure Hélène Dumont, il s’agit ici *pour la victime de libelle diffamatoire de recouvrer, de la partie adverse, un montant raisonnable de frais dont le quantum est laissé à l’appréciation de la Cour*[137].

---

[135]Art. 298 (1) C. cr.

[136]Cette conclusion soulève en outre des questions relatives à l’uniformité de sens de ce terme selon les lois. Par exemple, il semble que le terme "publication" dans la *Loi sur le droit d’auteur*, L. R. C. (1985), c. C-42, ait une toute autre définition.

[137]H. DUMONT, précité, p. 532. Voir également art. 729 C. cr. qui prévoit que cette ordonnance de frais peut être exécutée comme un jugement civil lorsqu’impayée.

### 34.5 La propagande haineuse

La propagande constitue une action exercée sur l'opinion pour l'amener à adopter certaines idées politiques, sociales ou autres. La propagande sera dite haineuse lorsqu'elle vise à créer une aversion profonde contre certaines choses ou personnes. La haine, selon le Petit Robert, est un sentiment violent qui pousse à vouloir du mal à quelqu'un et à se réjouir du mal qui lui arrive. Alphonse Daudet écrira d'ailleurs que *La haine, c'est la colère des faibles*.

Le crime de propagande haineuse constitue, au premier regard, une restriction à la libre expression. Au Canada, l'affaire *La Reine* c. *Keegstra*[138] avait, rappelons-le, maintenu le crime de propagande haineuse, c'est-à-dire le fait d'avoir fomenté la haine contre un groupe identifiable, considérant, à la majorité, qu'une telle limite à la liberté d'expression était justifiée par une règle de droit dans le cadre d'une société libre et démocratique.

Le crime de la propagande haineuse a été inséré au Code criminel suite à la recommandation du Rapport Cohen de 1966 [139]. Aux États-Unis, on parlera indistinctement de *racist speech* ou de *hate speech*. À cet égard, on peut souligner que la propagande haineuse est un discours qui vise à

---

[138][1990] 3 R. C. S. 697. Notons que la Cour d'appel de l'Alberta a considéré que cette disposition constituait une limite non justifiée à la liberté d'expression pour plusieurs raisons. D'abord, selon le juge Kerans, pour la Cour, la disposition en question pénalise les erreurs de faits ou les discours imprudents ; ensuite, il n'est pas certain (absence de preuve) que la haine à l'encontre d'un groupe résulte du discours ; et enfin, le fait que l'accusé soit tenu de démontrer la véracité de son discours lui impute un fardeau de preuve susceptible d'aller à l'encontre de l'article 11*d)* de la *Charte*. Voir Martine VALOIS, *Hate Propaganda, Section 2(b) and Section 1 of the Charter : a Canadiam Constitutional Dilemma*, 1992, 26 *R. J. T*. 373, 389.

[139]Canada, Comité spécial de la propagande haineuse au Canada, *Rapport du Comité spécial de la propagande haineuse au Canada*, Ottawa, Imprimeur de la Reine, 1966. L'auteure Martine Valois, précité, 380-381, note que la réalisation de ce rapport n'a pas été précédée de rencontres avec différents groupes minoritaires ; que l'étude n'a pas non plus porté d'attention sur les conséquences ou les dommages de la propagande haineuse, ayant considéré *a priori* qu'il y en avait. Les conclusions de ce rapport, doit-on enfin souligner, ne faisaient pas l'unanimité au sein de la communauté juridique.

*fomenter la haine contre un groupe identifiable*, alors que le discours raciste pourrait n'inclure aucune fomentation à la haine, mais simplement des expressions fausses, généralisantes ou des préjugés.

Ce crime, prévu à l'article 319(2) C. cr., a été introduit par le projet de loi C-3 en 1970. Il se lit aujourd'hui en ces termes :

> ***319.***
>
> *(2) Quiconque, par la communication de déclarations autrement que dans une conversation privée, fomente volontairement la haine contre un groupe identifiable est coupable :*
>
> a*) soit d'un acte criminel et passible d'un emprisonnement maximal de deux ans ;*
>
> b*) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.*
>
> *(3) Nul ne peut être déclaré coupable d'une infraction prévue au paragraphe (2) dans les cas suivants :*
>
> a*) il établit que les déclarations communiquées étaient vraies ;*
>
> b*) il a, de bonne foi, exprimé une opinion sur un sujet religieux ou tenté d'en établir le bien-fondé par discussion ;*
>
> c*) les déclarations se rapportaient à une question d'intérêt public dont l'examen était fait dans l'intérêt du public et, pour des motifs raisonnables, il les croyait vraies ;*
>
> d*) de bonne foi, il voulait attirer l'attention, afin qu'il y soit remédié, sur des questions provoquant ou de nature à provoquer des sentiments de haine à l'égard d'un groupe identifiable au Canada.*

La majorité, dans l'affaire *Keegstra*[140], rédigée par le juge Dickson, alors juge en chef, a interprété le crime de propagande haineuse comme étant une limite raisonnable à la libre expression. En effet, la criminalisation de ce type de discours poursuit un objectif suffisamment important pour la société canadienne. Le juge reprend ainsi la conclusion du Rapport Cohen selon lequel *the situation of hate propaganda in Canada is critical enough and could cause sufficient harm to justify legislative action*[141]. Le juge définit la propagande haineuse comme étant *l'expression destinée à créer et propager des sentiments extrêmes d'opprobre et d'inimitié envers un groupe racial ou religieux*[142]. Dans son survol historique, il l'apparente à une diffamation contre un groupe. Selon lui, de tels discours peuvent avoir une mauvaise influence sur la croyance populaire des gens en plus de miner le climat social et de pouvoir entraîner des tensions raciales et ethniques importantes. Il précise ainsi que le recours au droit criminel pour limiter ce genre de discours *sert à montrer au public le profond sentiment de réprobation de la société à l'égard de messages haineux*, tout en rappelant à l'ensemble de la collectivité *l'importance de la diversité et du multiculturalisme*[143]. En ce sens, la restriction à la liberté d'expression est proportionnelle puisqu'elle ne s'applique pas dans le cadre de communication privée ; qu'elle exige une *mens rea* ("volontairement") ; que le terme "fomente" (ou "promotion", en anglais) suppose une activité discursive importante et non seulement un simple encouragement ; et enfin que certains moyens de défense sont opposables à cette infraction : la vérité,

---

[140]Notons que cette affaire a été rendue en même temps que deux autres : *La Reine c. Andrews* , [1990] 3 R. C. S. 870 et *Canada (Human Rights Commission) c. Taylor*, [1990] 3 R. C. S. 892. Dans l'affaire Andrews, on a conclu la même chose que dans *Keegstra* avec la même majorité et la même dissidence, puisque la même disposition était en cause. Dans *Taylor*, on invoquait une violation de l'article 13(1) de *Loi canadienne sur les droits de la personne*. Le juge Dickson, pour la majorité, écrira que l'objectif de cette loi est de prévenir les activités discriminatoires et non pas de punir les acteurs de telles pratiques. Pour la juge McLachlin et ses collègues, cette disposition ne rencontre pas les exigences de l'article premier puisqu'elle pourrait interdire même les disours anti-discriminatoires ; qu'aucune défense fondée sur la vérité n'est possible et qu'enfin, cette loi s'applique même dans le cadre de discussions privées.

[141]M. VALOIS, précité, 393.

[142]*Keegstra*, précité, 722.

[143]*Id.*, 769.

la bonne foi, la croyance sincère et l'intérêt public. Le juge a cependant reconnu que le droit criminel n'est pas la seule voie possible pour combattre la propagande haineuse, mais que cette voie était disponible pour le Parlement fédéral[144].

La dissidence, rédigée par la juge McLachlin[145], insiste d'abord sur l'importance d'une interprétation large de l'article 2b) de la Charte. Elle conclura que les arguments du ministère public sont insuffisants pour maintenir la disposition en question. Parmi les arguments évoqués à l'encontre de la proportionnalité de la mesure au regard de l'objectif poursuivi, la dissidence considère que la pénalisation de la propagande haineuse a un "effet paralysant"[146] puisqu'elle peut dissuader le libre échange des idées chez ceux dont le discours pourrait s'apparenter à de la propagande haineuse. En plus, il n'existe aucun *lien fort et évident entre la criminalisation de la propagande haineuse et son élimination*[147]. Enfin, la publicité qui découle du procès criminel peut avoir comme effet de donner plus de crédibilité aux auteurs de tels discours haineux et ainsi amener des membres du public à croire en la vérité des discours avancés. Ainsi, le recours au droit criminel pour condamner de tels discours est considéré comme une voie excessive, surtout que dans l'état actuel les activités discriminantes ne sont pas criminalisées, alors que les discours peuvent l'être. La juge McLachlin écrira enfin que la vérité n'est pas une notion qui puisse être démontrée et qu'en ce sens, la disposition viole également l'article 11 *d)* de la Charte.

Aux États-Unis, dans l'affaire *R. A. V. v. City of Saint Paul*[148], la Cour suprême américaine a déclaré inconstitutionnelle une disposition interdisant une telle forme de discours, au motif qu'il s'agissait d'une disposition basée sur le contenu des discours et non sur la protection des droits individuels ou

---

[144]Parmi les autres voies possibles, il note l'éducation et l'utilisation des lois en matière de droits de la personne.

[145]Elle a été appuyée par les juges Sopinka et La Forest.

[146]*Keegstra*, précité, 850.

[147]*Id.*, 854.

[148]112 S. Ct. 2538 (1992).

collectifs. Cette divergence n'est qu'un faible reflet du débat qui entoure la circulation de matériel haineux sur les réseaux d'information. L'année de la décision *City of Saint Paul* a d'ailleurs été marquée par la publication d'un collectif intitulé *Striking a Balance : Hate Speech, Freedom of Expression and Non-discrimination*[149]. Cet ouvrage démontre notamment la divergence au niveau de la conception des sources et des effets du discours raciste et sur l'opportunité d'une réglementation visant à l'interdire, selon les nations. Les auteurs Stefanic et Delgado recensent ainsi les arguments défavorables à la régulation des discours racistes :

- La suppression des discours racistes n'a que pour effet d'en retarder l'explosion [150] ;
- Le discours raciste n'est pas la source du problème ; réglementer celui-ci est une diversion ; il faut plutôt favoriser l'éducation et les recours civils ;
- La plupart des règles nationales qui visent à supprimer les discours racistes sont utilisées à l'encontre des minorités ou des dissidents politiques ;
- Une réglementation du discours haineux mènera à une érosion de la liberté d'expression (*"slippery slope"*) ;
- Le droit de réponse est un mécanisme qui porte moins atteinte à la liberté d'expression que la répression ;
- Les lois contre le discours haineux vont limiter la discussion, particulièrement dans les campus universitaires ;
- La criminalisation du discours haineux n'est pas efficace,

---

[149] Sandra COLIVER (ed.), *Striking a Balance : Hate Speech, Freedom of Expression and Non-discrimination*, 1992 ; commenté et analysé dans Jean STEFANIC and Richard DELGADO, *A Shifting Balance : Freedom of Expression and Hate-Speech Restriction* (1993) 78 Iowa Law Review, pp. 737-750.

[150] *Suppressing racists speech will cause it to go underground only to surface in more virulent forms later* : cité dans J. STEFANIC and R. DELGADO, précité, p. 741.

d'autres moyens devraient être préalablement exploités[151] ;

- La persécution de ceux qui ont un discours haineux les fait apparaître comme de pauvres martyrs.

Toutefois, les arguments favorables à la suppression des discours racistes par la voie de l'intevention étatique sont également nombreux.

- Le racisme est en croissance dans le monde[152] et il est nécessaire de l'envisager sous l'angle du droit ;
- La suppression des discours racistes amènera une diminution de l'impulsion qui la sous-tend : le racisme ;
- Le discours raciste cause des dommages à ses victimes (dommage psychologique, moral et atteinte à la réputation individuelle ou collective) ;
- Le discours raciste cause des dommages à la société (ordre public, institutions et valeurs morales et sociales) ;
- La suppression du discours raciste envoie un message symbolique aux contrevenants potentiels ;
- Le racisme non contrôlé prend de l'expansion.

Deux types de dommages sont généralement identifiés comme résultant de la circulation de matériel à caractère haineux à l'encontre d'un groupe particulier de personnes. D'abord, un tel discours peut amener des gens à croire en sa véracité et ainsi contribuer à créer ou à perpétuer la discrimination à l'encontre de ce groupe minoritaire. Et ensuite, un tel discours peut causer des dommages moraux ou psychologiques aux

---

[151]Cet argument est l'un des seuls qui soient relativement acceptés par les pays développés : J. STEFANIC and R. DELGADO, précité, 744.

[152]Cet argument est avancé par la totalité des pays développés. Principalement, ce sont les discours antisémites qui sont les plus importants. On note également que les gens sont très racistes : *In Europe, one in three citizens believe that there are too many persons of other races or nationalities living in that citizen's country ; only 19% disapprove completely of racist movements* ; J. STEFANIC and R. DELGADO, précité, 745.

membres des groupes visés par le discours. Ici aussi, la propagande haineuse constitue une atteinte à la dignité et à l'égalité humaine.

Face à de telles divergences, il y aurait lieu de pousser plus loin la réflexion en soulignant l'importance, comme le rappellent d'ailleurs les auteurs Stefanic et Delgado, de l'esprit de communauté. En d'autres termes, une connaissance des valeurs communautaires ou nationales constitue un rempart contre la xénophobie et le racisme, qui sont liés à une crainte de l'étranger. Ces auteurs soulignent d'ailleurs le difficile équilibre entre les exigences de la garantie de la liberté d'expression et de l'égalité entre les humains.

> *The appropriate balance between equality and freedom of expression may be a complex, shifting matrix that includes several different forces : the value placed on community historically and aspirationally ; the value placed on equality among the various national groups ; the perception that minority populations are unfairly exluded or stigmatized ; the degree to which speech is considered an important individual prerogative, rather than a means of achieving community ; and finally, the perception that minority groups lack the means to assert and defend themselves against vilification*[153].

La criminalisation de certaines formes de discours a donc pour effet d'entourer de crainte l'exercice de la liberté d'expression, notamment, peut-on penser, dans le cadre de réseaux comme l'Internet, où la communication ne rencontre pas toujours les critères de la communication privée. D'ailleurs, deux affaires récentes ont abordé la question de la propagande haineuse dans le cadre de communications téléphoniques. Il s'agit des affaires impliquant la Commission canadienne des droits de la personne et le *Canadian Liberty Net*, ainsi que le *Heritage Front*. Les communications privées étant exclues de l'art. 319 C. cr., il demeure possible de porter plainte contre des manifestations racistes ou discriminatoires par le biais de

---

[153] J. STEFANIC and R. DELGADO, précité, 749.

l'art. 13(1) de la *Loi canadienne des droits de la personne*[154].

Outre l'article 319(2) C. cr.[155] et la Loi canadienne, il existe d'autres instruments juridiques qui viennent limiter la propension de discours racistes ou haineux et notamment la *Convention sur la prévention et la punition du crime de génocide* [156], la *Déclaration sur l'élimination de toutes formes de discrimination raciale*[157] qui a donné lieu, quelques années plus tard à la *Convention internationale sur l'élimination de toutes les formes de discrimination raciale*[158]. Ainsi, comme en matière de harcèlement, le point

---

[154]L. R. C. (1985), c. H-6. Sur cette question, on peut lire Eddie TAYLOR, *Hanging Up on Hate : Contempt of Court as a Tool to Shut Down Hatelines*, 1995, 5 *N. J. C. L.* 163. Cet auteur, citant les affaires *Canada (Human Rights Commission) v. Canadian Liberty Net*, [1992] 3 F. C. 504, 56 F. T. R. 42, et *Canada (Human Rights Commission) v. Heritage Front*, [1994] 1 F. C. 203 (T. D.), propose que l'interdiction des messages téléphoniques haineux soit retirée du domaine de la législation sur les droits de la personne pour être insérée dans le domaine du droit criminel.

[155]Notons que le Parlement fédéral a récemment adopté le projet de loi C-41 sur la détermination de la peine, en ce qui concerne l'application de la *Loi sur les crimes haineux*. Il reste à voir si les propos haineux tomberont aussi sous le coup d'une telle Loi.

[156](1951) 1021 R. T. N. U. 27.

[157]Résolution 1904 (XVIII) A. G. N. U. (1963).

[158]Adoptée en 1965 par l'Assemblée Générale des Nations Unies : (1969) 660 R. T. N. U. 213. L'article 4 de la précédente Convention mérite d'être ici cité :

> Les États parties condamnent toute propagande et toutes organisations qui s'inspirent d'idées ou de théories fondées sur la supériorité d'une race ou d'un groupe de personnes d'une certaine couleur ou d'une certaine origine ethnique, ou qui prétendent justifier ou encourager toute forme de haine et de discrimination raciales, ils s'engagent à adopter immédiatement des mesures positives destinées à éliminer toute incitation à une telle discrimination, ou tous actes de discrimination, et, à cette fin, tenant compte des principes formulés dans la Déclaration universelle des droits de l'Homme et des droits expressément énoncés à l'article 5 de la présente Convention, ils s'engagent notamment :

central de la propagande haineuse est le fait qu'il y a “discrimination” à l'encontre de certaines personnes humaines (ou groupes de personnes) et que cette discrimination porte atteinte à leurs droits à la dignité et à l’égalité. Enfin, notons l’existence de l’article 20 du *Pacte international des droits civils et politiques*[159] et l'article 10 de la *Convention européenne de sauvegarde des droits de l’homme et des libertés fondamentales*[160] qui viennent également légitimer l’intervention de l’État pour limiter les dommages pouvant résulter de la circulation de matériel haineux[161].

---

> *a)* À déclarer délits punissables par la loi toute diffusion d'idées fondées sur la supériorité ou la haine raciale, toute incitation à la discrimination raciale, ainsi que tous actes de violence, ou provocation à de tels actes, dirigés contre toute race ou tout groupe de personnes d'une autre couleur ou d'une autre origine ethnique, de même que toute assistance apportée à des activités racistes, y compris leur financement ;
>
> *b)* À déclarer illégales et à interdire les organisations ainsi que les activités de propagande organisées et tout autre type d'activité de propagande qui incitent à la discrimination raciale et qui l'encouragent et à déclarer délit punissable par la loi la participation à ces organisations ou à ces activités ;
>
> *c)* À ne pas permettre aux autorités publiques ni aux institutions publiques, nationales ou locales, d'inciter à la discrimination raciale ou de l'encourager.

[159](1976) 999 R. T. N. U. 187. Cet article prévoit : que "Toute propagande en faveur de la guerre est interdite par la loi" *et que "tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l’hostilité ou à la violence est interdit par la loi*".

[160](1955) 213 R. T. N. U. 221.

[161]On peut se reporter sur cette question à l’étude de Elizabeth F. DEFEIS, *Freedom of Speech and International Norms : A Response to Hate Speech*, 1992, 29 *Stanford Journal of International Law* 57-130, sur lequel nous aurons l’occasion de revenir dans une étape ultérieure.

Par ailleurs, sur la question de la responsabilité des gestionnaires de réseaux à l'égard des contenus de propagande haineuse qui peuvent y circuler, on peut rappeler quelques exemples américains. Prodigy est un réseau commercial de service de courrier électronique qui affiche nettement sa volonté d'être un réseau familial. Or, on y aurait laissé circuler des messages antisémites, ce qui a provoqué, en octobre 1991, un débat important. Un autre réseau, le WELL (Whole Earth 'Lectronic Link) avertit clairement ses usagers à l'effet que : *You own your own words. This means that you are responsible for the words that you post on the WELL*[162]. Enfin, *CompuServe* se qualifie comme une librairie électronique depuis l'affaire *Cubby*[163]. Cela lui permet de n'assumer aucune responsabilité à l'égard des messages qui circulent sur son réseau. Dans une certaine mesure, on peut penser que les gestionnaires de réseaux n'interviennent généralement qu'à des fins correctives, lorsque des plaintes ont été formulées par certains usagers. Ceux qui violent de façon répétée les lignes de conduite fixées par la "télécommunauté" peuvent alors perdre leur abonnement et leur accès.

### 34.6 Les jeux vidéos et autre matériel à caractère violent

Les jeux vidéos et le matériel à caractère violent suscitent beaucoup de controverses, notamment au Québec. D'ailleurs, les dénonciations nombreuses contre la violence de certains films américains et de jeux vidéos a fait du Québec "un leader contre la violence à la télévision"[164]. Cependant, ces manifestations de violence peuvent être nombreuses dans certains jeux informatiques (ludiciels) qui pourraient être rendus aisément accessibles sur les réseaux d'information. En effet, malgré le fait que le meurtre et les actes d'agression constituent des crimes hautement

---

[162]Cité dans A. W. BRANSCOMB, précité, p. 102. Le directeur de WELL soutient l'analogie du réseau qui serait comme un "*saloon*" dont il serait le "*barkeeper*". D'autres auteurs utilisent l'analogie du centre d'achats, souvent considéré par la jurisprudence comme un "*espace public*" (a public forum). Pour l'auteure Branscomb, "*self-policing is the best*".

[163]*Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135, 1991, U. S. Dist., LEXIS 15545 ; 19 *Media L. Rep*. 1525 (1991).

[164]Voir Presse Canadienne, *Le Québec, un leader contre la violence à la télévision*, 21 novembre 1994, *Le Devoir* A3.

répréhensibles dans notre société et que la possession d'armes soit interdite, on semble en général plus permissif à l'égard du matériel violent que du matériel pornographique. Il semble cependant que toute cette question soit liée aux préjudices pouvant découler de la circulation de ce genre de matériel. La circulation de matériel violent entraîne-t-elle la banalisation de la violence chez les jeunes ? Stimule-t-elle les comportements violents ou n'a-t-elle pas plutôt pour effet de les dissuader ? Y a-t-il des effets psychologiques à une exposition à ce genre de matériel ? Cette question pourrait faire l'objet d'une attention particulière dans une étape ultérieure.

En vertu du droit public canadien, il n'existe pas d'interdictions à l'égard des contenus violents. On sait cependant que la violence ne constitue pas une forme d'expression protégée par la Charte canadienne[165]. C'est plutôt au niveau de l'auto-réglementation que les radiodiffuseurs abordent cette question. L'Association canadienne des radiodiffuseurs a d'ailleurs adopté un *Code d'application volontaire concernant la violence à la télévision*[166], dont l'une des exigences est qu'une mise en garde soit formulée lorsque des scènes de violence apparaissent. Si l'on peut parfois douter de l'efficacité d'une telle réglementation - qui n'interdit pas la diffusion de films violents -, il semble que le doute soit encore plus grand à l'égard du matériel informatique, des images, des jeux[167] ou même des

---

[165]Voir à ce sujet l'affaire *Irwin Toy Ltd.* c. *Procureur général du Québec*, [1989] 1 R. C. S. 927, qui a été la première décision à exclure la violence ou les menaces de violence de la sphère protégée par la liberté d'expression. Toutefois, on peut penser que cette exclusion *a priori* soit le reflet d'un emprunt injustifié à la jurisprudence américaine en cette matière. En effet, l'interprétation qui doit être donnée au Premier amendement diffère de celle qui devrait être donnée à l'art. 2*b)* de la *Charte canadienne,* principalement en raison de la clause limitative de l'article premier de la *Charte*, inexistante dans le *Bill of Rights.* Par ailleurs, avec l'affaire *Keegstra*, rappelons que la dissidence a conclu que "*les déclarations fomentant la haine ne s'apparentent pas à la violence ni à des menaces de violences*", puisque le terme "violence" des arrêts *Irwin Toy* et *Dolphin Delivery* "*connote une ingérence ou une menace d'ingérence matérielle réelle dans les activités d'autrui*". R. c. Keegstra, [1990] 3 R. C. S. 697, 829 et suiv.

[166]Voir ASSOCIATION CANADIENNE DES RADIODIFFUSEURS, *Code d'application volontaire concernant la violence à la télévision*, C. R. T. C., Avis public 1993-149, 28 octobre 1993.

[167]Parmi les ludiciels qui comportent des scènes de violence, on peut souligner l'existence des jeux "Blood Bath", "Mortal Kombat", "Wolfenstein 3D", "Doom", etc.

extraits de films, accessibles par le réseau Internet.

## 35. Les atteintes à la vie privée

Le courrier électronique constitue, selon certains, le service de communication le plus personnalisé de l'Internet. Toutefois, aux États-Unis, le caractère confidentiel du courrier électronique n'est pas tout à fait tranché. L'auteure Anne W. Branscomb rappelle d'ailleurs qu'en raison de l'absence de statuts reconnaissant que l'*e-mail* au travail était confidentiel, la poursuite d'Alana Shoars contre son employeur, *Epson America*, fut rejetée[168]. Et ce, malgré que le courrier papier bénéficie de la protection de confidentialité. Cette affaire a par ailleurs donné lieu à la proposition du *Privacy for Consumers and Workers Act*[169] devant être intégré à l'*Electronic Communications Privacy Act of 1986* [170], et appliquant ainsi aux messages transmis par télécommunications la même protection que les messages téléphoniques vocaux.

Le *Code criminel* par ailleurs, énonce de façon non-équivoque ce qui constitue une "communication privée" à l'article 183 :

> *Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en*

---

[168] *Alana Shoars v. Epson America*, No. SWC112749 (L. A. Super. Ct.) ; cité dans A. W. BRANSCOMB, précité, pp. 92 et suiv. au chapitre intitulé : *Who Owns Your Electronic Mail ?* Notons qu'aux États-Unis, plusieurs entreprises procèdent au "monitoring" de leurs employés pour s'assurer de leur efficacité au travail. Cette question est abordée dans la section relative à la protection de la vie privée sur l'inforoute.

[169] Introduit le 19 mai 1993 (103rd Cong. 1sr Sess., U. S. Senate, 1993, S. 984).

[170] 18 U. S. C., §2701 et seq.

> *vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine.*

Cette disposition, à notre avis, peut conférer au courrier électronique le caractère de "communication privée" ouvrant ainsi la voie à la criminalisation de son interception en vertu de l'article 184 C. cr. On y énonce que quiconque intercepte une communication privée est coupable de cette infraction. Cependant, il faut souligner que l'ensemble des dispositions relatives à l'écoute électronique ont surtout comme objet de définir les moyens par lesquels les agents de la paix, ou autres personnes ayant un mandat légal, peuvent procéder à l'écoute électronique.

Également, la divulgation de renseignements qui ont été interceptés lors d'une communication privée fait l'objet de sanctions criminelles en vertu de l'art. 193 C. cr. De plus, cette divulgation illégale de communications privées peut donner lieu à des dommages punitifs à l'encontre de l'auteur de cette divulgation qui ne peuvent toutefois pas excéder les cinq mille dollars (art. 194(1) C. cr.).

## 36. Les atteintes à la saine administration de la justice

Bien que la règle générale veuille que les procédures dirigées contre un prévenu aient lieu en audience publique, le législateur a accordé au juge d'une audience criminelle une discrétion pour limiter, *inter alia*, le droit à la liberté de presse. Le 5 juillet 1993, le Juge Kovacs, présidant sur la notoire affaire Karla Homolka[171], s'est prémuni de ce privilège, en émettant une ordonnance de non publication, en vertu de l'article 486 (1) C. cr[172]. Cette

---

[171] http://www.eff.org/pub/Censorship/Foreign_and_local/Canada/Homolka_Teale_case/homulka_media_ban_canada.ruling

Voir également [1993] O. J. No 2047 ACTION nO. 125/93.

[172] 486. (1) Les procédures dirigées contre un prévenu ont lieu en audience publique, mais lorsque le juge, le magistrat ou le juge de paix qui préside est d'avis qu'il est dans l'intérêt de la moralité publique, du maintien de l'ordre ou de la bonne administration de la justice, d'exclure de la salle d'audience l'ensemble ou l'un quelconque des membres du public, pour toute ou partie de l'audience, il peut en ordonner ainsi.

ordonnance a été accordée, à la demande de la Couronne[173], au motif que toute publication sur l'affaire Homolka risquait de causer préjudice au droit de l'accusé Paul Bernardo à un procès juste et équitable, puisque les faits ayant donné lieu aux poursuites contre Bernardo et Homolka étaient similaires. Dans ces circonstances, selon le juge Kovacs, l'ordonnance de non publication garantissait un procès juste et équitable à Bernardo, assurant, de ce fait, la saine administration de la justice.

Malgré l'émission d'une telle ordonnance, certaines informations concernant le procès de Karla Homolka ont circulé, notamment au sein des environnements électroniques[174]. À titre d'exemples, certains se sont échangé cette information dans le cadre de Groupes de Discussion. Dans le journal étudiant de l'Université de Toronto, le procédé à suivre pour obtenir de l'information à l'aide du réseau Internet a été publié par un étudiant[175]. Un dénommé Jamie Baillie a téléchargé des informations sur un B. É. qui ont pu alors être télédéchargées par des personnes, dont des Canadiens[176].

Puisqu'il est possible d'y faire circuler de l'information à titre anonyme, encryptée, avec une rapidité sans précédent et ce, de façon transfrontalière, les environnements électroniques rendent-ils désormais ineffectif ce type d'ordonnance ? Comment empêcher que de telles informations émanant d'un pays comme les États-Unis atteignent le Canada ? Est-il possible, en pratique, de contrôler la circulation de telles informations ? La saine administration de la justice est-elle réellement garantie par ce type d'ordonnance ? Pensons à l'affaire O. J. Simpson. Croyons-nous vraiment

---

[173]Le droit à un procès juste et équitable appartient à l'individu, mais également à la société : *R. v. Morin* (1992) 71 CCC (3d) 7 (S. C. C.). La Couronne a invoqué le droit de Paul Bernardo à un procès juste et équitable au nom de la société,et ce, en vertu des articles 11 d) et 26 de la Charte canadienne des droits et libertés.

[174]L'information a également circulé par des moyens plus traditionnels, tels la presse. Ainsi, des copies du *Buffalo News* et du *Detroit News* qui contenaient un reportage du *Washington Post* sur l'affaire Homulka ont été confisquées par les douanes canadiennes.

http://www.cs.inidiana.edu/canada/Police

[175]http://www.cs.indiana.edu/canada/BannedInCanada.txt

[176]http://www.cs.indiana.edu/canada/police

qu'il a été possible d'empêcher aux jury de prendre connaissance de l'information sur le procès qui circulait à l'extérieur de la Cour ? Y a-t-il lieu de s'interroger sur la notion de saine administration de la justice ?

## 37. Conclusion

L'avènement de l'inforoute met au premier plan la qualification de certaines infractions relatives à la communication d'information. En effet, puisque l'inforoute transcende les frontières nationales, les informations qui y circulent ne sont pas intimement liées à un État ou n'y sont pas nécessairement situées. Ainsi, ce qui est qualifié de "criminel" au Canada ne l'est pas nécessairement dans tous les pays et ce qui l'est ailleurs, ne l'est pas toujours au Canada. Cela est un constat qui invite à observer les tendances dominantes en cette matière dans les autres pays et à travers les divers instruments internationaux. Tous les États sont, en quelque sorte, appelés à aménager leurs politiques à celles de leurs voisins ou du moins à celles avec qui ils communiquent. Par ailleurs, toutes les collectivités n'ont pas toutes les mêmes valeurs et il semble tout à fait souhaitable d'assurer la présence et l'affirmation de cette diversité.

L'exposé qui précède fait état des principales activités qui, dans le contexte familier actuel, limitent la circulation de certains contenus informationnels. Qu'il s'agisse de matériel à caractère sexuel, ludique ou haineux ; qu'il s'agisse d'atteinte particulière à la vie privée, à la dignité ou à la sécurité des personnes ; ou encore qu'il s'agisse d'informations qui autrement portent atteinte à "l'ordre public", on reconnaît avec évidence qu'il y a là de nombreuses restrictions à la liberté d'expression, qui peuvent entraîner des conséquences criminelles.

Le *Code criminel* est un instrument important d'affirmation des valeurs et d'un certain équilibre entre la "liberté" individuelle et la protection de la collectivité. Toutefois, le Code criminel est adopté par le Parlement fédéral, ce qui rend difficile pour le Québec d'en modifier les textes.

En outre, il semble que le recours à la criminalisation des discours doive être limité aux infractions "les plus graves" qui, par ailleurs, sont ainsi reconnues dans une majorité d'États. L'importante gravité du discours est

exigée en raison du fait que la liberté d'expression est au coeur même de l'éclosion de l'inforoute et de l'émergence des sociétés démocratiques, tout en faisant l'objet d'une constitutionnalisation dans de nombreux États et étant affirmée comme l'une des libertés fondamentales de tout être humain. Aussi, les questions relatives aux justifications profondes de la criminalisation des discours, de ses effets concrets et de l'efficacité de la sanction criminelle devraient mériter une plus ample réflexion[177].

Enfin, il semble essentiel d'insister sur le principe en vertu duquel, en droit criminel, nul n'est censé ignorer la loi[178]. De cette présomption de connaissance imposée à tous les citoyens canadiens semble découler l'obligation pour l'État fédéral de diffuser, voire de rendre disponibles sur les réseaux d'information, les dispositions relatives aux infractions de communication[179].

---

[177]Sur cette question, on pourrait se reporter à l'étude intitulée *La régionalisation du droit pénal international et la protection des droits de l'homme dans les procédures de coopération internationale en matière pénale* (1994) 65 Revue internationale de droit pénal.

[178]Voir art. 19 C. cr. où on indique que l'ignorance de la loi n'est pas une excuse à la perpétration de l'infraction.

[179]Voir à cet égard le site Internet du Centre de recherche en droit public (C. R. D. P.) de l'Université de Montréal à l'adresse suivante :

http://www.droit.umontreal.ca

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

**Karim BENYEKHLEF**[1]

## 38. Introduction

L'avénement 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[2]. 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

---

[1]Professeur, Centre de recherche en droit public, Faculté de droit, Université de Montréal. 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 Me François Themens pour sa contribution au repérage de la doctrine.

[2]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 "Comité consultatif-Vie privée").

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[3]. Il est de coutume maintenant de dire que la mondialisation des échanges n'est pas étrangère à ce phénomène. Toutefois, au-delà du cliché, l'interprète note que l'information n'a plus de port d'attache fixe, qu'elle circule librement et qu'aucune autorité nationale ne peut à elle-seule contrôler ou, à tout le moins, policer les échanges d'informations. Cela explique les efforts déployés par plusieurs organisations internationales dans le domaine des données à caractère personnel. En effet, le droit international n'est pas silencieux en la matière. Il convient donc, dans une première partie, de décrire et d'analyser les efforts normatifs entrepris par ces organisations. Dans une deuxième partie, on se demandera si ces normes internationales sont adaptées aux nouvelles voies électroniques de communication. En d'autres termes, le développement de la technique a-t-il rendu obsolètes, inadaptés ou incomplets les principes fondamentaux en matière de gestion de l'information personnelle que l'interprète peut retrouver dans les instruments internationaux ? Cette question nous amènera également à traiter des voies

---

[3] *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 around 12 million transborder data transactions per day. Gradually the world economy is transforming itself from an industrial-based economy to an information-based economy, in which the free exchange of information has become the life-blood of modern business life.*, A. C. M. NUTGER, Transborder Flow of Personal Data Within the EC, Deventer, Kluwer, 1990, p. 1.

normatives susceptibles d'encadrer l'autoroute de l'information pour ce qui est de la protection de la vie privée. En effet, au-delà de l'applicabilité des normes internationales, se pose la difficile question de leur application pratique. Comment assurer le respect de ces normes dans un environnement électronique tentaculaire qui échappe, par la multiplicité de ses réseaux et de ses acteurs, à toute autorité unique ou centrale ?

## 39. Le droit international de la protection des données personnelles

### 39.1 Les documents internationaux

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

dépourvus de toute législation sur la protection des renseignements nominatifs[4].

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[5].

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[6] adopte en 1980 les *Lignes*

---

[4] *But it is not only the storage of personal data that constitutes a threat to the personal life sphere of the individual. Modern processing facilities as much as the interconnexion of computer systems, due to telematics, 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*, Nutger, *supra* note 2, pp. 3-4.

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

[6] Organisation de Coopération et de Développement Économiques.

*directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* 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*. Les Lignes directrices se présentent sous la forme d'une recommandation aux Etats 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 entraves de l'information personnelle. La création du grand marché intérieur militait également pour une initiative de la Commission[7]. En 1990, la Commission présentait un projet de directive sur le sujet qui s'est rapidement heurté à une forte opposition[8]. 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*[9]. Cette proposition devrait, en principe, être adoptée avec quelques

---

[7]*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 Etats 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.

[8]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 Media & Communications L. R. 149.

[9]COM(92) 422 final-SYN 287, Bruxelles, 15 octobre 1992.

modifications présentées dans la Position commune arrêtée par le Conseil des Ministres[10].

Les Nations-Unies ont également développé un corpus réglementaire en la matière : les *Principes directeurs sur l'utilisation des fichiers personnels informatisés*[11]. Examinons maintenant succinctement ces divers instruments.

### 39.1.1 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 respectifs[12]. 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 :

---

[10]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. Ce texte reprend en le modifiant le projet de directive de 1992.

[11]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, Ed. Thémis, 1992, p. 336 à 342.

[12]Michael D. KIRBY, *Transborder Data Flows and the "Basic Rules" of Data Privacy*, [1980] 16 Stanford Journal of International Law, 42, p. 43.

> *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[13]. 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[14].

---

[13]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.

[14]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.*

Tout comme pour les Lignes directrices, une disposition de la Convention européenne permet aux pays signataires de prévoir une protection plus étendue que celle que l'on retrouve dans cet instrument. L'article 11 autorise alors l'État à accorder à certaines catégories de données une protection spécifique plus importante que celle, par ailleurs, reconnue aux autres types d'informations personnelles. On pense ici encore une fois évidemment aux données sensibles. Là encore, ce régime particulier peut nuire à la circulation de l'information personnelle. Ce régime, dérogeant à la notion de normes minimales, peut entraîner une restriction à la libre circulation de l'information. Mais, à l'instar des Lignes directrices, cette restriction apparaît légitime au regard de l'article 12(3)a) de la Convention.

Pour ce qui est du champ d'application de ces instruments, on remarque qu'ils s'appliquent aussi bien au secteur public qu'au secteur privé. Alors que les Lignes directrices couvrent tant les fichiers automatisés que les fichiers manuels[15], la Convention européenne ne vise que les fichiers automatisés[16]. Dans ce dernier cas, en vertu de l'article 3(2)c), un État peut néanmoins préciser, lors du dépôt de son instrument de ratification ou à tout autre moment ultérieur, qu'il appliquera également la Convention aux fichiers manuels. Les deux instruments ne s'appliquent qu'aux personnes physiques à l'exclusion des personnes morales. La Convention européenne prévoit toutefois explicitement la possibilité d'étendre la protection de son dispositif aux personnes morales[17].

Les deux instruments consacrent l'essentiel des principes fondamentaux en matière de gestion de l'information personnelle. Ces principes sont les suivants : principe de la justification sociale[18], principe de la limitation en matière de collecte[19], principe de la qualité des données[20], principe de la

---

[15] Article 2 des Lignes directrices.

[16] Article 3 (1) de la Convention européenne.

[17] Article 3 (2)b) de la Convention européenne.

[18] Article 6 de la Convention européenne.

[19] Article 5a) de la Convention européenne et Article 7 des Lignes directrices.

[20] Articles 5c) et 5d) de la Convention européenne et Article 8 des Lignes directrices.

spécification des finalités[21], principe de la limitation de l'utilisation[22], principe de sécurité[23], principe de la transparence[24], principe de la détention limitée dans le temps[25], principe de la responsabilité[26] et principe de la participation[27]. 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[28]. 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*)

---

[21] Article 5b) de la Convention européenne et Article 9 des Lignes directrices.

[22] Article 5b) de la Convention européenne et Article 10 des Lignes directrices.

[23] Article 7 de la Convention européenne et Article 11 des Lignes directrices.

[24] Article 8a) de la Convention européenne et Article 12 des Lignes directrices.

[25] Article 5e) de la Convention européenne et interprétation conjuguée des articles 8 et 10 des Lignes directrices.

[26] Articles 8d) et 10 de la Convention européenne et Article 14 des Lignes directrices.

[27] Article 8 de la Convention européenne et Article 13 des Lignes directrices. Pour une analyse des principes fondamentaux en matière de gestion de l'information personnelle, lire Benyekhlef, *supra* note 10, p. 100 et s.

[28] *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 Stanford Journal of International Law, 87, p. 94. Lire également du même auteur : *A Decade of International Data Protection*, [1983] 30 Netherlands International L. R. 103, p. 109-110.

et non pas de chercher à harmoniser les ensembles législatifs eux-mêmes[29]. 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[30].

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 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[31]. Quant aux Lignes directrices, son article 19 traite de cette question. Il ne faut pas perdre de vue le caractère non contraignant, au point

---

[29] *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 "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.*

[30] 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*., H. P. GASSMANN, *Vers un cadre juridique international pour l'informatique et autres nouvelles techniques de l'information*, [1985] Annuaire français de droit international, 747, p. 755.

[31] *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, *supra* note 28, p. 16.

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[32] ou de favoriser et de soutenir des systèmes d'autoréglementation (codes de déontologie ou autres formes)[33]. 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[34].

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 détaillées[35]. Le caractère

---

[32]Article 19a) des Lignes directrices.

[33]Article 19b) des Lignes directrices.

[34]Rapport explicatif, *supra* note 28, p. 16.

[35]Pour en savoir plus, lire Benyekhlef, *supra* note 10, p. 352 à 357.

contraignant de la Convention européenne explique sans doute la complétude du système d'entraide et d'assistance.

Il faut rappeler que les Lignes directrices ne constituent qu'une simple recommandation. Le Canada a adhéré aux Lignes directrices en 1984. Quant à la Convention européenne, il s'agit d'un document juridiquement contraignant. Cette dernière est entrée en vigueur en 1985 suite à sa ratification par cinq pays membres du Conseil de l'Europe[36].

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

> *La Convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel n'a pas permis de limiter cette disparité dans la mesure où, d'une part, elle laisse ouvert un grand nombre d'options pour la mise en oeuvre des principes de base qu'elle définit et, d'autre part, elle n'a été ratifiée que par sept Etats membres (Allemagne, Danemark, Espagne, France, Irlande, Luxembourg, Royaume-Uni)*[37] *dont un (Espagne*[38]*) qui n'a toujours pas de législation interne. La recommandation de la Commission du 29 juillet 1981 invitant les Etats membres de la Communauté à ratifier la convention du Conseil de l'Europe n'a*

---

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

[37]Ce chiffre n'est plus exact aujourd'hui. Voir note 35.

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

*pas modifié cette situation*[39].

La Commission a donc estimé nécessaire d'intervenir afin de corriger cette situation[40]. Nous y reviendrons. Quant aux Lignes directrices, l'interprète remarque que l'autoréglementation, voie de mise en oeuvre du dispositif de la recommandation, n'a pas permis d'amoindrir l'écart normatif existant entre les pays européens et l'Amérique du Nord. Le Canada et les États-Unis ont encouragé le secteur privé à développer des codes de conduite propres à régir le traitement de l'information personnelle. Le secteur privé nord américain a inégalement répondu à l'appel[41]. En fait,

---

[39]Proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Exposé des motifs), COM(90) 314 final-SYN 287, Bruxelles, Septembre 1990, p. 15. Le lecteur notera qu'il s'agit là de l'exposé des motifs de la première version du projet de directive.

[40]Pour un exposé plus complet des motifs d'intervention de la Commission, lire Benyekhlef, *supra* note 7.

[41]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.

l'OCDE elle-même semble reconnaître l'insuffisance de la seule voie autoréglementaire[42].

En terminant, il importe de signaler que le Conseil de l'Europe a également adopté toute une série de recommandations visant à assurer la protection des données personnelles dans divers secteurs, comme la santé, le marketing direct ou la police[43]. Il faut bien comprendre que la Convention européenne est un instrument de nature globale ou générale. C'est-à-dire qu'elle a vocation de s'appliquer tant au secteur public que privé sans que

---

[42]*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*, OCDE, Paris, DSTI/ICCP/88. 5, 1er juin 1988, p. 19.

[43]Recommandation no R(81) 1 relative à la réglementation applicable aux banques de données médicales automatisées (23 janvier 1981) ; Recommandation no 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 no 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 no R(86) 1 relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale (23 janvier 1986) ; Recommandation no R(87) 15 relative à l'utilisation de données à caractère personnel dans le secteur de la police (17 septembre 1987) ; Recommandation no R(89) 2 relative à la protection des données à caractère personnel utilisées à des fins d'emploi (18 janvier 1989) ; Recommandation no 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 no R(91) 10 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics (9 septembre 1991).

des distinctions, de nature fondamentale, n'affectent l'un ou l'autre de ces secteurs. Le Conseil de l'Europe a néanmoins estimé nécessaire d'adapter ces principes généraux ou fondamentaux à certains secteurs de l'activité humaine. Ces recommandations s'avèrent alors complémentaires :

> *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*[44].

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 Etats membres à tenir compte, dans leur droit interne, du dispositif que l'on y retrouve.

### 39.1.2 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 :

---

[44]Rapport de l'OCDE de 1988, *supra* note 41.

> *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[45]. Cet exercice n'est pas inutile puisque, si ce document est adopté, il constituera sans doute la norme internationale de référence en matière de protection des données personnelles.

**- Champ d'application**

Le projet de directive s'applique, en principe, indistinctement au secteur public et au secteur privé[46]. De même, il vise aussi bien le traitement automatisé de l'information personnelle que les fichiers manuels[47]. À ce propos, l'article 3(2) précise que sont exclus du champ de la directive les traitements de données à caractère personnel effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. Le projet de directive ne s'applique qu'aux personnes physiques, à l'exclusion, par conséquent, des personnes morales[48].

**- Collecte et traitement**

---

[45]Voir *supra* note 9.

[46]Le premier projet de directive de 1990 traitait différemment les deux secteurs. Lire notamment R. G. BOEHMER et T. S PALMER, *The 1992 EC Data Protection Proposal : An Examination of Its Implications for U. S. Business and U. S. Privacy Law*, [1993] 31 *American Business Law Journal*, 265, p. 294.

[47]Article 3 de la Position commune de 1995.

[48]Peter MEI, *The EC Proposed Data Protection Law*, [1993] *Law & Policy in International Business* 305, p. 311.

L'article 6 consacre les principes de la limitation en matière de collecte, de spécification des finalités et de la qualité des données. Autrement dit, les données personnelles doivent être collectées loyalement et licitement. Elles doivent être collectées pour des finalités déterminées, explicites et légitimes, et utilisées de manière compatible avec ces finalités[49]. De plus, les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées[50]. Les données doivent également être exactes et, si nécessaire, mises à jour. L'article 6(1)d) précise à ce propos que toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités de collecte, soient effacées ou rectifiées. L'article 6(1)e) consacre, pour sa part, le principe de la détention limitée dans le temps.

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

---

[49] Article 6(1)b) de la Position commune de 1995.

[50] Article 6(1)c) de la Position commune de 1995

particulières de cueillette et de traitement Ces conditions sont évidemment plus strictes.

**- 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[51]. 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 le 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 verouillage 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 verouillage, la notification aux tiers, à qui ont été communiquées les données, de cette rectification, effacement ou verouillage. 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, à 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 de ce 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 instruments internationaux en la matière. Il prévoit que la personne fichée peut s'opposer, à tout moment et dans certains cas, pour des raisons prépondérantes tenant à sa situation particulière à ce que des données la

---

[51] Article 12(1) de la Position commune de 1995.

concernant fassent l'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 inspiré 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 l'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 ...)[52].

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, l'existence d'un droit d'accès et de rectification concernant ces données, 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 l'enregistrement des données ou, si une communication à un tiers est envisagée, au plus tard lors de la première communication des informations relatives à l'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

---

[52]Mais noteons 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 Proposal Amendment to justify positive responses, but every negative response requires that the decision result from personal, as well as computer, analysis*, Mei, *supra* note 47.

circonstances particulières dans lesquelles les données sont collectées, ces informations sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données. Le paragraphe 2 de l'article 11 prévoit une exception à ces obligations d'information dans le cas d'un traitement à finalité statistique, historique ou scientifique ou alors dans la situation où l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou encore si la législation prévoit expressément l'enregistrement ou la communication des données. Dans ces cas, la Directive oblige les Etats membres à prévoir des garanties appropriées.

**- Devoirs du responsable du traitement**

Nous avons déjà présenté quelques obligations du responsable du traitement. Ce dernier doit, de plus, notifier à l'autorité de contrôle la mise en oeuvre d'un traitement automatisé[53]. L'article 19 prévoit le contenu de la notification. Cette notification comprend les nom et adresse du responsable du traitement, la ou les finalités du traitement, la ou les catégories de personnes concernées, la description des données ou des catégories de données sur lesquelles porte le traitement, les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées, les transferts de données envisagés avec des pays tiers, la description des mesures de sécurité. L'article 18 prévoit une procédure de notification simplifiée et, dans certains cas, l'exonération de l'obligation de notification[54].

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

---

[53] Article 18(1) de la Position commune de 1995.

[54] *Some commentators estimate that simplified requirements could excuse eighty percent of a company's processing operations from the notification provision*", Mei, *supra* note 47.

**- Autoréglementation**

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

> *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 de bonne conduite. Le paragraphe 3 de l'article 27 reconnaît également cette possibilité au plan communautaire. On y encourage les milieux professionnels à participer à l'élaboration de codes de conduite communautaires, destinés à contribuer à la bonne application de la directive en fonction de la spécificité des secteurs.

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

**- Institutions**

Au plan institutionnel, le projet de directive prévoit, à son article 28, la mise en place d'une autorité de contrôle chargé de surveiller l'application des dispositions nationales prises en application de la directive. Cette autorité constitue bien évidemment l'agence de protection des données personnelles[55]. Le paragraphe 3 énonce les pouvoirs dont doit disposer cette

---

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

autorité de contrôle : pouvoirs d'investigation, droit d'ester en justice, pouvoir d'ordonner le verouillage ou l'effacement etc.

L'article 29 établit un groupe de protection des personnes à l'égard du traitement des données à caractère personnel à l'échelle communautaire. Ce groupe à caractère consultatif et indépendant est composé des représentants des autorités de contrôle mises en place en vertu de l'article 28, d'un représentant de la Commission et d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires. Il s'agit, en quelque sorte, d'une agence européenne de protection des données personnelles. Ce groupe n'a cependant qu'un caractère consultatif en ce que sa mission se limite, selon l'article 30, à donner des avis sur le niveau de protection dans la Communauté et dans les pays tiers, à conseiller la Commission sur tout projet de modification à la directive, à donner son avis sur les codes de conduite élaborés au niveau communautaire, à contribuer à l'application homogène des 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[56]. Ce projet fut également l'objet d'importantes modifications. La Commission devait présenter en 1994 une version remaniée de ce projet de directive[57]. 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

---

[56]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.

[57]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.

par le Conseil de l'Europe[58]. La Commission estime que le secteur des télécommunications exige l'élaboration d'un instrument spécifique qui tiendra compte de ses particularités ; d'autant qu'il semble que les législations nationales pertinentes en l'espèce instituent des normes de plus en plus divergentes entre elles[59].

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.

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

### 39.2 Le principe de l'équivalence

Nous savons déjà que la plupart des lois européennes de protection des données personnelles contiennent des dispositions soumettant l'exportation d'informations nominatives à des contrôles ou autorisations préalables. Ces

---

[58]Voir *supra* note 42. *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*, *Ibid*., p. 3.

[59]*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*, *Ibid*., p. 3.

dispositifs s'avèrent nécessaires afin d'éviter le contournement des prescriptions nationales par un transfert informationnel vers un pays dépourvu de toute législation ou doté d'une législation beaucoup plus laxiste que celle du pays d'exportation. En général, le transfert sera permis si le pays importateur assure aux données personnelles transferées une protection de même nature que celle ayant cours dans le pays exportateur. C'est là le principe de l'équivalence qu'on peut reformuler ainsi : un pays ne s'opposera pas à la transmission de données personnelles vers un pays tiers pourvu que ce dernier assure, dans son droit interne, une protection aux données personnelles qui équivaut en substance à celle existant dans le pays exportateur.

Le principe de l'équivalence est au coeur du dispositif réglementant les flux transfrontières de données à caractère personnel à l'article 17 des Lignes directrices 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[60].

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 conduite professionnelle. Toutefois ces mesures volontaires ne suffisent pas par elles-mêmes pour donner suite à la Convention[61].*

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[62], 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

---

[60]Voir pourtant *supra* note 41.

[61]Rapport explicatif, *supra* note 28.

[62]Sur l'approche américaine, lire entre autres Benyekhelf, *supra* note 40.

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[63]. 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 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*

---

[63]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*, Boehmer et Palmer, *supra* note 45.

> *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[64]. 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[65]. 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 Etats 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

---

[64]Sur la voie contractuelle comme moyen de pallier l'absence de législation nationale dans le pays importateur, lire Benyekhlef, *supra* note 10.

[65]Article 25(6) de la Position commune de 1995.

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 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*[66].

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

---

[66] Simon CHALTON, *A Privacy Law for Europe : Back to the Data Protection Drawing Board,* [1993] 9 Computer Law & Practice, 4, p. 6-7.

## 40. L'applicabilité des normes internationales aux nouvelles voies électroniques de communication

### 40.1 Les nouvelles voies électroniques de communication

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

À ce propos, le réseau Internet illustre sans doute ces potentialités[67]. Celui-ci préfigure ce que devrait être les futures autoroutes électroniques. Les communications électroniques apparaissent novatrices en ce qu'elles amalgament des techniques jusqu'ici isolées, comme le téléphone, la câblodistribution, la radiodiffusion, l'ordinateur etc. En d'autres termes, les nouvelles voies de communication permettent la transmission de la voix, du son, de l'image et de données (textes, graphiques etc.). La communication n'est plus unidirectionnelle, comme pour la câblodistribution, ou bidirectionnelle, comme pour la téléphone, mais plutôt muldirectionnelle et interactive. L'usager n'est plus un spectateur passif ; il peut devenir un acteur en participant à des échanges ou discussions électroniques, en créant des fichiers accessibles (FTP, WWW[68]), 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

---

[67]On estime qu'il existe entre 8,9 à 17,8 millions d'utilisateurs du réseau Internet, ce qui en fait évidemment le plus grand réseau électronique du monde,. Sur le réseau Internet, lire entre autres : J. J. QUATERMAN et S. Carl MITCHELL, *The Internet Connection. System Connectivity and Configuration*, Reading (Mass.), 1994, p. 5.

[68]FTP : File Transfer Protocol ; WWW : World Wide Web.

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[69]. 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 des 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 ;
- Communicationnelles.

Les trois premières fonctionnalités se passent d'explication. La quatrième se rapporte aux échanges d'informations entre universitaires, à la publication de revues électroniques, à la tenue de séminaires électroniques ou de listes discussions (babillards électroniques) sur des sujets d'intérêt divers. De même, la consultation de banques de données, l'accès à des sites

---

[69]Lire Karim BENYEKHLEF, *Les transactions dématérialisées sur les voies électroniques : panorama des questions juridiques*, dans *Les autoroutes électroniques : usages, droit et promesses*, Cowansville, Ed. Yvon Blais, 1995.

de documentation ou d'informations de type journalistique s'intègrent dans cette catégorie. Quant aux fonctionnalités communicationnelles, nous faisons simplement référence au courrier électronique (E-Mail[70]), c'est-à-dire à la possibilité de correspondre, par le truchement d'un réseau électronique de communication, avec des usagers quel que soit leur lieu de résidence.

Il faut bien comprendre qu'un réseau, comme l'Internet, offre, en général, toutes ces fonctionnalités. Celles-ci coexistent dans le cyberespace. L'usager passe de l'une à l'autre sans difficulté. Évidemment, ces services ne sont pas tous gratuits. Certaines fonctionnalités, comme la commande de films ou de disques, par exemple, supposent un déboursé qui s'additionne aux frais d'abonnement au réseau[71]. Cette classification a un objet juridique. Elle permet de mieux cerner les enjeux afférents, notamment, à la protection du droit à la vie privée. En effet, l'interprète aura deviné que les potentialités d'atteintes au droit à la vie privée sont plus grandes dans le cas des opérations commerciales que dans celui des échanges académiques. De même, la consultation de sites d'informations de type journalistique soulève, en général, moins de risque d'atteinte à la vie privée que la commande de biens et services. Ce n'est pas tant l'achat, dans ce dernier cas de figure, qui constitue un danger pour la vie privée que la possibilité pour le serveur commercial de dresser un profil des habitudes de consommation de l'usager (données transactionnelles[72]). Ce profil devient une précieuse source de

---

[70]Electronic Mail.

[71]Sur les environnements réseaux, lire entre autres : Ruel Torres HERNANDEZ, *ECPA and Online Computer Privacy*, [1988] 41 Federal Communications L. J. 17, p. 19 à 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*, Cowansville, Ed. Yvon Blais, 1995, à paraître, p. 19 à 21 de la version manuscrite.

[72]Lire Benyekhlef, *supra* note 10.

données personnelles qui peut être vendu à d'autres entreprises entraînant par là, bien souvent, un détournement des finalités premières de collecte[73].

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[74] aux nouveaux environnements électroniques de communication.

### 40.2 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[75].

---

[73]*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 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.

[74]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.

[75]Sur ce sujet, lire Benyekhlef, *supra* note 7. Lire également l'arrêt *La Reine* c. *Dyment*, [1988] 2 R. C. S. 417, p. 429-430.

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.

Toutefois, ces organes ne sont pas les seuls acteurs du théâtre télématique. Il y a également les usagers. Or les principes fondamentaux en matière de gestion de l'information personnelle ne s'appliquent pas aux individus dans l'exercice de leurs activités privées[76]. Il est donc clair que ces principes ne sont pas applicables à l'interception par un tiers du courrier électronique d'un utilisateur. Ces principes ne couvrent pas davantage les situations d'accès non autorisé à des sites pouvant contenir des données personnelles et la dissémination de ces données sur le réseau. Certaines lois pourvoient parfois à ce type de situation. Quoi qu'il en soit, ces situations mettent également en cause le droit à la vie privée ou, à tout le moins, un élément de celui-ci que constitue le principe de confidentialité.

Par conséquent, la protection de la vie privée sur les nouvelles voies électroniques de communication ne se limite pas aux simples questions afférentes aux principes fondamentaux en matière de gestion de

---

[76]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.*

l'information personnelle. Ainsi, la possibilité d'échanger des messages électroniques sans faire l'objet d'une interception par un tiers ou même par l'État ou sans faire l'objet d'une surveillance par son employeur[77], par exemple, s'inscrit dans une problématique certes associée au droit à la vie privée, mais tout de même distincte de celle relative à la gestion de l'information personnelle telle qu'envisagée par les normes internationales examinées en première partie. Il ne s'agit pas de déplorer l'inapplicabilité de ces normes à ces situations. Celles-ci n'ont pas été, en effet, élaborées pour répondre à ces interrogations. D'autres normes doivent alors être développées ou adaptées pour corriger ces atteintes au droit à la vie privée. Il faut donc bien comprendre que les principes fondamentaux en matière de gestion de l'information personnelle n'ont pas vocation à régir toutes les situations soulevant le problème du droit à la vie privée dans le cyberespace. Par ailleurs, il nous semble que les atteintes potentielles les plus graves et les plus nombreuses au droit à la vie privée sont couvertes, de prime abord, par ces principes fondamentaux. En effet, les organismes publics et les entreprises commerciales sont, sans aucun doute, les principaux détenteurs de renseignements personnels. Cette formidable accumulation de données constitue, en soi, une menace beaucoup plus importante 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 adéquation avec le nouvel environnement électronique mis en place sur l'autoroute de l'information. En effet, comme le souligne le professeur Poullet, ces réglementations *ont combattu le risque relatif aux traitements d'informations recueillies a priori par les centres de traitement*[78]. Or, poursuit-il, *les risques dénoncés ici concernent des données nées a posteriori par l'utilisation du service lui-même*[79]. Deux concepts fondamentaux sont ici mis en cause : les définitions des expressions “données à caractère pesronnel” 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*

---

[77]Lire, par exemple, Steven WINTERS, *The New Privacy Interest : Electronic Mail in the Workplace*, [1993] 8 High Technology Law Journal 197.

[78]Yves POULLET, *Le marché de l'information. Aspects contractuels : les clauses de confidentialité*, Texte inédit, Namur, p. 42.

[79]*Ibid*., p. 42.

*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[80]. 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*[81].

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[82]. 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[83].

---

[80] 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, p. 34-35 (ci-après "Nouvelles technologies").

[81] Article 2a) de la Position commune de 1995.

[82] 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*.

[83] Jon BING, *Impact of Developing Information Technology on Data Protection Legislation*, Paris, OCDE, DSTI/ICCP(86)5, Février 1986, p. 13-14.

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 données personnelles sont stockées et ordonnancées dans un fichier, localisé en un endroit bien précis, vole en éclat. La notion de fichier n'est pas adaptée. Les données sont aujourd'hui éparpillées et ne s'intégrent donc plus dans un ensemble ordonnancé et unique (fichier)[84]. Or, la notion traditionnelle de fichier répondait aux exigences de transparence et d'accessibilité aisée aux données par la personne concernée. Le Conseil de l'Europe propose alors le concept de “fichier logique” afin de pallier ces difficultés de définition. La délocalisation et l'éparpillement des données ne constitueraient pas des obstacles à la création d'un fichier virtuel. En d'autres mots, il est possible, par le couplage notamment, de réunir des données dispersées en un ensemble unique et ordonnancé. Nous sommes alors en présence d'un fichier potentiel ; celui-ci se matérialisant à la suite de diverses opérations informatiques[85].

Le projet de directive de la Commission européenne, tel qu'amendé par la Position commune de 1995, répond à ces développements technologiques en abandonnant la notion de “fichier automatisé”. L'application de la directive n'est donc pas tributaire de l'existence d'un fichier structuré pour ce qui est du traitement 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*

---

[84] *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, *supra* note 79, p. 35.

[85] *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*, *Ibid.*, p. 36.

> *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.*
>
> *Ainsi, sont concernées les données à caractère personnel structurées soit par leur organisation dans un fichier manuel, soit au moyen d'un traitement automatisé*[86].

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

---

86 Projet de directive de 1992, *supra* note 8, 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 includes 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*, Mei, *supra* note 47, p. 311.

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*[87].

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[88] 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 plus, le caractère résolument international des nouvelles voies électroniques de communication réclame l'élaboration de normes propres à faciliter la circulation de l'information et à assurer une protection uniforme des données personnelles. En dépit des efforts de l'OCDE, du Conseil de l'Europe et de la Commission européenne, le droit de la protection des données à caractère personnel est loin d'être uniforme. L'absence au Canada, par exemple, de tout instrument général visant à protéger les renseignements personnels dans le secteur privé illustre notre propos[89]. La

---

[87]Nouvelles technologies, *supra* note 79, p. 44-45.

[88]Voir *supra* note 42.

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

même remarque peut être formulée pour ce qui est des États-Unis[90]. Le problème de l'équivalence des protections se pose donc avec acuïté.

Ce problème apparaît d'autant plus délicat que l'intangibilité du cyberespace rend difficile l'application des règles de protection des données personnelles. Autrement dit, comment assurer une application effective de ces règles lorsque l'usager est domicilé à Montréal et que le serveur, une entreprise commerciale, a sa place d'affaires à la Nouvelle-Orléans ou à Hong Kong ? Quelle autorité assurera l'application et la sanction de ces règles ? Comment déterminer la violation de ces règles dans un environnement aussi volatil et insaisissable ? Même si, par hypothèse, toutes les nations étaient dotées d'une loi de protection des données personnelles, le problème de l'intangibilité et de la délocalisation continuerait à se poser : quelle loi appliquer ? Quelle autorité est compétente ? comment assurer l'exercice des droits d'accès et de correction de la personne concernée ? Comment cette dernière peut-elle déterminer l'existence d'un traitement automatisé la concernant ? Comment concilier les différences normatives qui ne manqueront pas d'affliger les instruments pertinents[91] ? Ces questions ne constituent que la pointe de l'iceberg.

L'interprète constate alors qu'au-delà de la question de l'applicabilité stricte des normes internationales au champ de l'autoroute de l'information, c'est la question de l'application pratique et opérationnelle de ces normes qui soulève le plus de difficultés. Une coopération internationale apparaît dès lors nécessaire, voire inéluctable, si l'on entend assurer vraiment la protection de la vie privée des usagers de l'autoroute de l'information[92]. En attendant la concrétisation d'une telle coopération, certains mécanismes peuvent, avec plus ou moins de bonheur, atténuer les difficultés inhérentes à l'intangibilité du cyberespace. Ces mécanismes constituent, en plus, une voie complémentaire de protection des données personnelles. En d'autres

---

[90]Lire Joel R. REIDENBERG, *Setting Standards for Fair Information Practice in the U. S. Private Sector*, [1995] 80 *Iowa L. R.*

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

[92]Sur les modalités de coopération internationale, lire les articles 13 à 17 de la Convention européenne et les articles 28 à 30 de la Position commune de 1995.

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[93], elle peut constituer une voie complémentaire, et non pas exclusive[94], 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[95], 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

---

[93]Sur les conditions à respecter pour qu'un code de conduite constitue un véritable instrument de régulation des données personnelles, lire Benyekhlef, *supra* note 40, p. 233 à 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 R. CÔTÉ et R. LAPERRIÈRE, *Vie privée sous surveillance : la protection des renseignements personnels en droit québécois et comparé*, Cowansville, Ed. Yvon Blais, 1994, p. 83.

[94]Lire *supra* note 41.

[95]Lire l'article 27(3) de la Position commune de 1995.

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

Le principe de proximité nous semble une solution concrète susceptible de faciliter la normalisation des inforoutes. Le caractère international de celles-ci s'oppose, en effet, à toute solution normative uniquement globale ou générale. Une telle approche se heurte à d'immenses difficultés pratiques d'application. Le principe de proximité a pour avantage de localiser ou de régionaliser, en quelque sorte, la résolution des problèmes ou des conflits suscités par un environnement électronique transnational. En fait, ce principe est le pendant, d'une certaine manière, du principe de subsidiarité que l'on retrouve en droit européen[96]. Selon le principe de subsidiarité, il convient de laisser aux instances nationales ou locales le soin de règler les difficultés qui ne peuvent être raisonnablement traitées au plan communautaire. Il importe de rappeler que l'action des agents de proximité

---

[96]Voir, entre autres, Commission européenne, *Le principe de subsidiarité*, [1992] 28 *Revue trimestrielle de droit européen*, 731 *: 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*, p. 732 *; Le principe de subisidiarité*, (1992) Bull. CE 10-1992, p. 122.

doit s'inscrire dans le cadre normatif général mis de l'avant par le législateur national ou par un accord international. Autrement dit, les normes conçues et appliquées par les agents de proximité tirent leur légitimité et leur licéité du fait qu'elles complètent ou explicitent le cadre normatif général. Bien évidemment, il s'agit de prévoir des mécanismes garantissant l'indépendance des agents de proximité afin d'éviter leur inféodation à des intérêts clientélaires ou financiers[97]. Par ailleurs, on remarque que le principe de proximité peut s'appliquer à d'autres domaines du droit que celui de la protection des données personnelles (droit d'auteur, transactions dématérialisées, exercice de la liberté d'expression etc.).

L'Association Canadienne des Standards (ACS) est en train d'élaborer un code de conduite standard qui serait applicable, en principe, à l'ensemble du secteur privé. L'ACS travaille en collaboration avec des représentants du secteur privé, d'associations de consommateurs et des autorités publiques. L'originalité de l'approche de l'ACS est qu'elle se propose d'intégrer les normes afférentes à la protection des données personnelles aux standards de gestion que connaissent les entreprises (*Quality Management*). Autrement dit, les normes de protection des données personnelles constitueraient un standard de gestion au même titre que le respect des règles comptables reconnues dans l'élaboration des états financiers. Un audit pourrait donc être effectué et comprendrait l'analyse des modalités de gestion de l'information personnelle au regard du standard pertinent. Cette initiative canadienne pourrait être appliquée au plan international (ISO 9000) et faire de la protection des données personnelles un standard de gestion

[97] 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.

internationalement reconnu et uniforme. Ceci contribuerait, sans aucun doute, à atténuer les problèmes inhérents à l'intangibilité du cyberespace[98].

Finalement, la voie contractuelle peut constituer une voie complémentaire ou de substitution. Toutefois, elle comporte certains inconvénients qui en diminuent sérieusement l'attrait. En 1992, le Conseil de l'Europe, conjointement avec la Commission européenne et la Chambre de Commerce internationale, a entrepris la rédaction d'un contrat-type applicable aux flux transfrontières de données à caractère personnel[99]. L'objet essentiel d'un tel contrat est de faciliter la circulation internationale de données nominatives en assurant un degré de protection aux données, ainsi transmises, équivalent, en principe, à celui du pays exportateur. Cette équivalence est bien entendu la résultante des exigences à cet effet que l'on retrouve dans la plupart des lois européennes et dans les instruments internationaux[100]. Ainsi plutôt que de bloquer l'exportation de données personnelles vers un pays dépourvu de toute législation en la matière, l'agence de protection des données personnelles va permettre cette exportation à condition que les parties à la transmission s'engagent à respecter, par voie contractuelle, les principes fondamentaux édictés dans la loi du pays d'exportation[101].

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*

---

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

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

[100]Voir *supra* point B- Le principe de l'équivalence, p. 24 à 29.

[101]Lire l'article 26 de la Position commune de 1995.

> *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*[102].

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[103]. 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[104].

---

[102]Note, *supra* note 98, p. 13.

[103]Pour une analyse critique du contrat-type, lire Benyekhlef, *supra* note 40, p. 271 à 283.

[104]Lire Reidenberg, *supra* note 89, p. 72 à 75 de la version manuscrite. 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.

Ces voies alternatives ou complémentaires ne sont pas dénuées d'intérêt. Il nous semble qu'elles peuvent constituer, avec d'autres[105], 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[106].

## 41. Conclusion

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

---

[105]Comité-consultatif-Vie privée, *supra* note 1, p. 15 à 18. Lire aussi Marc ROTENBERG, *Electronic Privacy Legislation in the United States*, (1994) Vol. 2 The International Privacy Bulletin, p. 15-16.

[106]Sur cette question, lire Trudel, *supra* note 70.

# Droit et inforoute : vers une lex electronica ?

**Pierre-Luc BOUCHER**[1]

## 42. Introduction

En cette fin de 20e siècle, les environnements électroniques occupent une place de plus en plus importante dans nos vies. Bien que l'inforoute présente des avantages certains, il n'en demeure pas moins qu'elle amène également de nombreuses interrogations. À ce titre, la délocalisation des rapports constitue une source de questionnement importante. Cette dématérialisation des échanges entraîne la remise en question de nombre de perceptions sur les plans juridique, social, politique ou encore philosophique.

La délocalisation des rapports constitue un problème majeur en regard du droit. Du fait de cette délocalisation, se pose la question du droit applicable à ce type de relations. Quelles règles régissent les rapports qui se nouent dans les environnements électroniques ? Quelle est la nature de ces règles ? Quelle est la source de ces règles ?

Évidemment la réponse la plus évidente semble être le recours à la technique de conflit de loi. Cependant, cette méthode, qui ultimement mène à l'application d'un droit national, ne nous apparaît pas appropriée. En effet, considérant la nature des rapports dont il est question, il nous semble difficile de concevoir de quelle façon une loi nationale pourrait appréhender de façon satisfaisante des rapports qui, de par leur nature, transcendent l'espace et les frontières nationales. La nécessité d'un certain degré d'uniformité nous amène à nous interroger sur la place des droits nationaux dans la réglementation de l'espace cybernétique.

---

[1]L'auteur est avocat, LLB, LLM et agit à titre d'agent de recherche au Centre de Recherche en Droit Public de l'Université de Montréal. Il est à noter que ce texte ne constitue qu'une section d'un texte plus général sur les environnements électroniques intitulés *Le cadre juridique et réglementaire des nouveaux environnements électroniques.* Il est également à noter que ce texte n'est pas encore complété il s'agit donc d'une réflexion en cours.

Le recours à des lois modèles ou encore à des conventions internationales peut sembler de prime abord plus attrayant que le recours au système de conflit de loi ; nous en convenons. Il s'agit là sans l'ombre d'un doute d'une avenue à explorer. Toutefois, ces méthodes législatives demandent plus souvent qu'autrement beaucoup de temps et de patience. Or, le rythme auquel les frontières de l'espace cybernétique[2] s'étendent actuellement laisse entrevoir la nécessité d'une réglementation à plus ou moins court terme. Les litiges cybernétiques, si on peut les nommer ainsi, portés à notre attention jusqu'à maintenant, permettent de percevoir toute la difficulté qu'éprouvent les droits nationaux à appréhender ce type de rapports.

Dans cette perspective, il nous apparaît nécessaire, sinon utile, d'explorer des voies de réglementation autres que celles offertes par les droits nationaux. Nous nous proposons donc de jeter un bref regard sur les normativités privées qui semblent émerger de l'espace cybernétique. Bien que cette réglementation n'apporte pas, pour l'instant du moins, de réponse définitive à nos questionnements, elle permet tout de même d'envisager de nouvelles pistes.

À ce titre, l'ensemble des règles du commerce international désigné par le terme *lex mercatoria* nous apparaît comme une voie intéressante. Pour ce motif nous tenterons de dresser un parallèle entre ce phénomène et la normativité privée qui émerge de l'espace cybernétique.

## 43. Espace cybernétique et réglementation nationale

Tel que mentionné précédemment, la dématérialisation des échanges représente, sans l'ombre d'un doute, la caractéristique principale des environnements électroniques. Ces environnements transcendent le concept de distance[3]. En raison de l'apparition de ces nouveaux médiums de communication les frontières nationales apparaissent beaucoup plus

---

[2]Notons le rythme de développement particulièrement rapide de l'Internet.

[3]Dorothy E. DENNING et Herbert S. LIN (dir.), *Rights and Responsabilities of Participants in Networked Communities*, Washington D. C., National Press Academy, 1994, p. 7.

perméables qu'auparavant à la circulation de l'information. Désormais, l'information circule sans égard aux frontières nationales. À tel point qu'il faut aujourd'hui se questionner quant à savoir si le concept classique de souveraineté nationale ne doit pas être remplacé par celui de souveraineté informationnelle[4]. En conséquence, il nous faut envisager le problème de l'application des lois nationales à des rapports qui, de plus en plus, présentent un caractère transnational.

Au-delà des difficultés d'application de lois nationales à des sujets qui se situent hors juridiction au sens traditionnel du terme, se pose également le problème de l'uniformité des règles applicables. Considérant la facilité avec laquelle des liens transfrontières se créent, l'atteinte d'un certain degré d'uniformité quant aux règles applicables apparaît souhaitable. À défaut d'obtenir cette uniformité, il nous semble difficile de concevoir une réglementation qui soit efficace. Cependant, force est de constater que des systèmes de valeurs différents les uns des autres risquent de s'affronter dans

---

[4]Karim BENYEKHLEF, *La souveraineté nationale et le contrôle des échanges internationaux d'informations*, (1991) 25 *R. J. T.* 433. Dans ce texte, le professeur Benyekhlef suggère que les flux transfrontières de données de plus en plus importants s'accordent mal avec la notion traditionnelle des frontières nationales. Il expose notamment que *les réseaux de communication connaissent des frontières qui n'ont rien à voir avec celles qui délimitent la souveraineté d'un État. Ces réseaux font fi de ces dernières et se développent en fonction de critères économiques qui donnent ainsi lieu à la création de zones de communication. Ces zones de communication ont leurs propres frontières*. Selon le professeur Benyekhlef, la technologie transcende la notion classique de souveraineté et amène une réévaluation de celle-ci. Le concept de souveraineté informationnelle comporte deux niveaux de contrôle : un contrôle intérieur, i. e. contrôle de l'exportation des données, et un contrôle extérieur, i. e. contrôle des données stockées à l'étranger concernant un État ou ses nationaux.

l'espace cybernétique[5]. Or, certaines difficultés pourraient se poser en raison de l'organisation décentralisée des réseaux électroniques[6].

### 43.1 Les communautés de réseaux

Ainsi, prenons l'Internet à titre d'exemple. Deux aspects fondamentaux de l'organisation de ce réseau de réseaux présentent une structure décentralisée : sa technologie[7] et sa gestion. En raison de l'absence d'une autorité centrale forte régissant cet espace, divers groupes s'organisent selon leurs intérêts respectifs. Cette structure décentralisée amène donc, si l'on peut dire, la formation de “communautés” de l'espace cybernétique[8]. On

---

[5]Bien que l'Internet demeure encore pour l'instant un phénomène américain, il n'en demeure pas moins que le reste de la planète se fait de plus en plus présent. Michael NEUBARTH, *The Internet : A Global Look*, *Internet World*, Novembre 1995, p. 95 : *Today, about one half of all registered Internet Hosts are located in North America, while the other half of the net's population is distributed around the world*.

[6]Dorothy E. DENNING et Herbert S. LIN (dir.), *Rights and Responsabilities of Participants in Networked Communities*, Washington D. C., National Press Academy, 1994, p. 9 : *The governance of the Internet is also decentralized. That is, each site on the Internet operates under its own locally formulated code of behavior or conduct, though each site communicates with other sites*.

[7]*Id.*, p. 8 : *Two fundamental aspects of the Internet are decentralized : its technology and its governance. The Internet is based on packet-switching technology that transmits a message between two points by breaking the message into packets that travel independently and often through different routes between sender and receiver. As with telephone traffic, the path taken by data sent through the Internet is often not known in advance*. L'information est divisée en segments ("packets") de 200 bits environ (toutefois cela peut varier). Chacun des segments se voit accoller l'adresse du destinataire. Ces segments se promènent d'un ordinateur à l'autre sur l'Internet. Ce sont ces ordinateurs qui déterminent au moment où l'information transite quelle est la connection la plus efficace. Une fois arrivé à destination ces segments sont rassemblés et reconstitués dans leur forme originale. Voir : Dennis FAZIO, *Hang on to your packets : The Information Superhighway heads to Valleyfair or Building a high performance computer system without reading the instructions*, 14 Mars 1995,

ftp://montego.umcc.umich.edu/pub/users/seraphim/doc/nethist94/html

[8]*Id.*, p. 18.

note également que la culture, les valeurs et les standards de comportements de ces diverses communautés ne sont pas homogènes[9] :

> *As with physical communities, network cultures are not homogeneous, and the participants in networked communities often have conflicting values*[10].

Doit-on prévoir que des règles différentes émergeront en fonction de la "communauté" dont il est question ? L'affaire *Thomas*[11] aux États-Unis illustre fort bien l'affrontement entre des cultures différentes qui est, à notre avis, à prévoir.

Les circonstances de cette affaire sont relativement simples. Les Thomas opéraient un BBS[12] sur lequel ils diffusaient du matériel à caractère sexuel. Un inspecteur des postes du Tennessee, en collaboration étroite avec le représentant du Procureur Général, devint membre du BBS des Thomas. Une fois membre du service, cet inspecteur télédéchargea des images à caractère sexuel, commanda une vidéocassette (porno) et envoya une vidéocassette (pornographie infantile) non sollicitée aux Thomas. Ceci mena à des accusations fédérales. En première instance[13], les Thomas furent reconnus coupables des douze accusations relatives à l'obscénité. Cependant, ils furent acquittés de l'accusation relative à la pornographie infantile.

Le critère applicable afin de déterminer si les Thomas ont bel et bien diffusé du matériel obscène constitue l'élément central de cette affaire. On

---

[9] *Id.,* p. 19.

[10] *Id.* p. 19.

[11] Référence non disponible pour l'instant.

[12] BBS est l'abréviation de "bulletin board system". John R. LEVINE et Carol BAROUDI, *The Internet for Dummies*, 2e éd., Foster City-Chicago-Indianapolis-Braintree-Dallas, 1994, p. 19 : *On-line services are services provided to you by a computer or computers interactively. They include but are not limited to computerized banking, shopping, dating, entertainment, and study. [...] Electronic bulletin board systems (abbreviated as BBS or BBSs for plural) provide on-line services generally on a smaller scale and often with a particular focus.*

[13] Cette affaire est présentement en appel.

se rappellera que le BBS en question était situé en Californie alors que l'inspecteur des postes se trouvait à Memphis au Tennessee. Ce qui est obscène pour une communauté ne l'est pas nécessairement pour une autre. Chaque communauté possède sa propre culture et son ensemble de valeurs. Ce principe est reconnu aux États-Unis depuis l'affaire *Miller* v. *California*[14].

À cette occasion, la Cour suprême américaine en arriva à la conclusion que l'obscénité n'était pas protégée par le premier amendement du *Bill of Rights*. Au surplus, la Cour énonça un test afin de déterminer ce qui constitue du matériel obscène. Godwin résume ce test de la façon suivante :

> *In that case, the Court stated that materials is "obscene" [...] if 1) the average person, applying contemporary community standards, would find the materials, taken as a whole, arouse immoral lustful desire (or in the court's language, appeals to the "prurient interest"), 2) the materials depict or describe, in a patently offensive way, sexual conduct specifically prohibited by applicable state law, and 3) the work, taken as a whole, lacks serious literacy, artistic, political or scientific value.*[15]

Godwin ajoute :

> *It has long been held to be constitutionnal to prosecute any porn vendors located in more liberal jurisdictions who have knowingly or intentionally distributed obscenity into conservative juridictions.*[16]

Toutefois, Godwin soumet que la situation des Thomas est différente. Un opérateur de BBS, contrairement à un vendeur de vidéo ou de magazines pour adultes, ne prend pas la décision d'envoyer son matériel

---

[14]Cour Suprême Américaine, 1973.

[15]Mike GODWIN, *Virtual Community Standards,*

http://www.eff.org/pub/legal/cases/aabbs_thomasesmemphis/obscen_virtcom_stds_godwin.article

[16]*Id.*

dans une juridiction dans laquelle il risque d'être poursuivi[17]. La doctrine américaine du "community standard" visait à éviter que le standard d'une communauté ne vienne dicter celui d'une autre communauté située à l'autre bout du continent. L'affaire Thomas remet cette théorie en question et amène une réflexion quant à savoir si le standard de communauté doit être déterminé uniquement sur la base d'un critère géographique[18].

Quant au critère applicable au Canada en matière d'obscénité il s'agit d'un critère national. La Cour suprême du Canada a repris et précisé dans l'arrêt *Butler*[19] le critère de la norme sociale nationale tel que formulé par le juge en chef Dickson dans l'arrêt *Towne Cinema Theatres Ltd* : c. *La Reine*[20] :

> *Puisque la norme est la tolérance, je pense que l'auditoire auquel s'adresse le film prétenduement obscène doit être pris en considération. Les normes qui s'appliquent sont celles de la société canadienne dans son ensemble, mais, puisque ce qui importe c'est ce que d'autres personnes peuvent voir, il est tout à fait concevable que que la société canadienne tolérerait divers degrés de caractère explicite selon l'auditoire et les circonstances.*[21]

À notre avis il y a lieu de s'interroger quant à savoir si les critères canadiens et américains, suite à la décision de première instance dans l'affaire Thomas, demeurent pertinents dans le cadre des environnements électroniques.

---

[17]Néanmoins, considérant la nature des environnements électroniques, on peut s'interroger quant à savoir si le simple fait de rendre de l'information disponible ne constitue pas un geste suffisant en soi pour que l'on puisse considérer qu'il s'agit là d'une intention suffisante de diffuser l'information où qu'elle puisse se retrouver. Voir texte de Mylène Beaupré et Sophir Hein (texte supra) sur cette question.

[18]Voir en ce sens Mike GODWIN, *Loc. cit*, note 14.

[19]*R.* c. *Butler*, [1992] 1 R. C. S. 452.

[20][1985] 1 R. C. S. 477.

[21]*Id.,* pp. 508-509.

Dans un premier temps il importe de s'interroger sur l'existence de ces communautés de réseaux et sur leur organisation. Les règles, tant dans leur formulation que dans leur application, font appel à la culture et aux valeurs d'une communauté donnée. Les environnements électroniques amènent, semble-t-il[22], une multiplication des communautés de même qu'une stratification des systèmes de valeur. Pour cette raison il faut se demander si cela n'entraîne pas une plus grande diversité des règles. Par ailleurs, il y a lieu de se demander si l'uniformité dans la réglementation peut être atteinte en raison de la présence de dénominateurs communs. Par exemple, les problèmes rencontrés par l'ensemble des utilisateurs, peu importe la communauté à laquelle ils appartiennent, ont-ils un effet d'uniformisation des règles ?

Il semble plutôt difficile de recenser l'ensemble des règles qui émanent de ces communautés. Toutefois il apparaît possible de s'arrêter à certaines de ces communautés notamment celle que forment les utilisateurs de USENET. Nous nous attarderons à celle-ci un peu plus loin mais d'abord il apparaît utile de s'arrêter à un autre modèle de normativité privée. À cet égard, les règles élaborées par les opérateurs du commerce international constituent un modèle de réglementation fort intéressant.

Les problèmes de juridiction observables dans l'espace cybernétique ne sont pas réservés à cet environnement puisqu'ils se retrouvent également, dans une moindre mesure, en matière de commerce international. Une étude de ces rapports nous enseigne que des opérateurs privés, insatisfaits des règles offertes par les divers droits nationaux, en sont venus à élaborer leurs propres normes. Ce phénomène désigné par le terme générique de *lex mercatoria* peut à tout le moins nous renseigner sur le mode de formation de règles émanant d'opérateurs privés.

L'étude de ce phénomène nous permettra de démontrer qu'il est possible que des règles d'origine privée puissent constituer une solution viable au problème de juridiction posé par les environnements électroniques de même qu'au problème d'uniformisation des normes.

---

[22]Dorothy E. DENNING et Herbert S. LIN (dir.) *Op. cit.,* note 2, p. 19.

### 43.2 La *lex mercatoria* : Sources et définition

Le terme *lex mercatoria* désigne deux concepts qui sont à la fois distincts[23] et intimement liés l'un à l'autre. Distincts dans le sens où le terme désigne à la fois la loi marchande médiévale et l'ensemble de règles que se donnent la "communauté" des opérateurs du commerce international moderne. Ils se trouvent également intimement liés dans la mesure où la théorie de la *lex mercatoria* moderne s'abreuve à la source de la loi marchande du moyen-âge.

La *lex mercatoria* médiévale[24] consistait en un ensemble de règles d'origine privée régissant les relations entre commerçants. Issues des coutumes des marchands, celles-ci tiraient leur fondement de la pratique commerciale. Présentant un visage résolument cosmopolite, les prescriptions de la *lex mercatoria* du moyen-âge étaient uniformes et généralement acceptées par la communauté des commerçants. A travers leurs voyages, notamment par leur présence lors des grandes foires, Les marchands italiens contribuèrent grandement au développement de ce corpus de règles. Ces dernières gouvernaient entre autres les questions liées à la vente, au transport, à l'assurance et au financement. On note également l'existence de juridictions commerciales spécialisées ayant pour fonction de trancher les différents entre commerçants.

---

[23]Voir sur les distinctions à faire : Luc BOUCHER, *L'uniformisation du droit commercial international par la Cour suprême du Canada : une approche justifiée ?* , mémoire de maîtrise, Montréal, Faculté des études supérieures, Université de Montréal, 1993, pp. 27 et ss.

[24]Voir de façon générale : Francois MOREL, *Les juridictions commerciales au moyen-âge*, Paris, Arthur Rousseau éditeur, 1897 ; Leon A. TRACKMAN, *The Law Merchant : The Evolution of Commercial Law*, Littleton, Fred B. Rothman & co., 1983 ; Francis Marion BURDICK, *Contribution of the Law Merchant to the Common Law* dans *Select Essays in Amglo-American Legal History*, Boston, Little,Brown, and Company, 1909, p. 39 ; K. J. LEVINE et A. M. SQUILLANTE, *Fairs and their impact on the development of commercial law*, (1974) 22 *Chitty's L. J.* 102 ; Antonio PERRAULT, *Traité de droit commercial*, t. 1, Montréal, Édition Albert Lévesque, 1936, 648p., à la p. 50 ; Joseph HAMEL et Gaston LAGARDE, *Traité de Droit Commercial*, t. 1, Paris, Librairie Dalloz, 1954, 1154p., à la p. 26 ; L. BOUCHER, *L'uniformisation du droit commercial international par la Cour suprême du Canada : une approche justifiée ?* , mémoire de maîtrise, Montréal, Faculté des études supérieures, Université de Montréal, 1993, p. 6 à 24.

Plusieurs auteurs[25] réfèrent à la *lex mercatoria* médiévale en tant que modèle régulateur possible pour les environnements électroniques. Ce qui amène Wittes à constater que :

> *The favored analogy among cyberlaw experts for the Net's emerging legal system is the medieval "law merchant.*[26]

Plus près de nous et, pour ce motif, plus intéressante, la loi marchande moderne ne fait pas l'unanimité quant à la qualification qui doit lui être accordée. Toutefois, aussi controversée soit-elle, la théorie de la *lex mercatoria* moderne s'avère de plus en plus difficile à contourner. Il suffit de consulter les recueils des sentences arbitrales de la chambre de commerce internationale pour s'en rendre compte[27]. Bien que cette théorie d'une loi marchande transnationale moderne fasse l'objet d'un vigoureux

---

[25]Notamment : Amelia H. BOSS, *Electronic Data Interchange Agreements : Private Contracting Toward a Global Environment*, (1992) 13 *Northwestern Journal of International Law and Business* ; I. Trotter HARDY, *The Proper Legal Regime For "Cyberspace"*, (1994) 55 *University of Pittsburg Law Review* 993, pp. 1019 à 1022.

[26]Bejamin Wittes, *Law in Cyberspace : Witnessing the Birth of a Legal System on the Net*, *Legal Time*, semaine du 23 janvier 1995, p. S27, à la p. S28.

[27]Sigvard JARVIN, *Recueil des Sentences Arbitrales de la CCI 1974-1985*, Paris-New York-Deventer-Boston, ICC Publishing, *Kluwer Law and Taxation*, 1990 ; Sigvard JARVIN, Yves DERAINS et Jean-Jacques ARNALDEZ, *Recueil des Sentences Arbitrales de la CCI 1986-90,* Paris-New York-Deventer-Boston, ICC Publishing, Kluwer Law and Taxation, 1994 ; Voir également sur le sujet Guy Lefèbvre, *Texte en préparation*.

débat en doctrine[28], il n'en demeure pas moins qu'en pratique force est de constater que les opérateurs du commerce international se donnent eux-mêmes des règles régissant leurs rapports ou à tout le moins certains aspects essentiels de ceux-ci[29].

La définition suivante donne une idée assez exacte de ce qu'est la loi marchande moderne :

> *La* lex mercatoria *est conçue comme un ensemble de règles (ou normes) spécifiques aux relations économiques internationales, d'origine (ou de source) non étatique, formant un droit coutumier transnational permettant à ses bénéficiaires d'échapper à l'emprise de l'ordre juridique*

---

[28]Deux courants s'affrontent en doctrine quant à la nature de ce phénonène. Certains affirment qu'il s'agit bel et bien de règles de droit "anationales" voir même un système de droit : Clive M. SCHMITTHOFF, *International Business Law : A New Law Merchant*, (1961) II C. L. 129 ; Clive M. SCHMITTHOFF, *Commercial Law in Law in a Changing Economic Climate*, Londres, Sweet & Maxwell, 1981 (2e éd.), 78 p. ; Clive M. SCHMITTHOFF, *The Unification of the Law of International Trade*, (1968) J. B. L. 106 ; Berthold GOLDMAN, *Les conflits de Lois dans l'Arbitrage International de Droit Privé*, (1963) Tome 109 vol. 2 Recueils des Cours 347 ; Berthold GOLDMAN, *Frontières du Droit et "lex mercatoria"*, (1964) 9 A. P. D. (NS) 177 ; Berthold GOLDMAN, *La lex mercatoria dans les contrats et l'arbitrage internationaux : réalités et perspectives*, (1979) 106 J. D. I. 475 ; Aleksander GOLDSTAJN, *The New Law Merchant*, (1961) J. B. L. 12 ; Éric LOQUIN, *L'application de règles anationales dans l'arbitrage commercial international* dans *L'apport de la jurisprudence arbitrale*, Paris, ICC Publishing SA, 1986, p. 67. Par ailleurs d'autres soutiennent qu'il n'y a là qu'un phénomène conventionnel lié aux droits nationaux par la théorie des contrats : Antoine KASSIS, *Théorie générale des Usages du commerce*, Paris, L. G. D. J., 602p. ; Jean ROBERT, *Le Phénomène Transnational*, Paris, L. G. DJ., Édition de l'AFA, 1988, 60p. ; Paul LAGARDE, *Approche critique de la Lex Mercatoria* dans Philippe FOUCHARD et Antoine LYON-CAEN, *Le droit des relations économiques internationales : Études offertes à Berthold Goldman*, Paris, Librairies Techniques, 1982, p. 138 ; Georges R. DELAUME, *Comparative Analysis as a basis of Law in State Contract : The Myth of the Lex Mercatoria*, (1988-89) 63 T. L. R. 575 ; Keith HIGHET, *The Enigma of the Lex Mercatoria*, (1988-89) 63 T. L. R. 613.

[29]À titre d'exemple mentionnons le transport de marchandise et le crédit documentaire.

> *international et constituant bien, dès lors, une menace pour ce dernier.*[30]

Bien que cette définition réfère à la notion de coutume il semble qu'il ne s'agisse pas ici de la coutume au sens classique du terme[31] mais plutôt de la notion d'usage. L'usage constitue la pierre angulaire de la théorie de la *lex mercatoria* contemporaine, c'est autour de cette notion que s'articule cette réglementation issue de la pratique du commerce international. Schmitthoff définit l'usage comme suit :

> *A trade usage is a method of dealing or a way of conduct generally observed in a particular line of business with such regularity that it is accepted as binding by those engaged in that line of business.*[32]

L'existence même du phénomène d'une *lex mercatoria* contemporaine est tributaire de l'accession des usages du commerce international au statut de règles de droit[33]. Ce postulat n'est pas sans soulever de nombreuses interrogations. Tout d'abord, quelles sont les conditions de formation de la règle de droit ? À compter de quel moment et dans quelles circonstances y a-t-il apparition ou formation d'un ordre juridique ? Notre propos n'est pas ici de répondre à ces questions[34], aussi nous limiterons-nous à souligner le

---

[30]Jacques BÉGUIN, *Le développement de la lex mercatoria menace-t-il l'ordre juridique international ?* , (1984-1985) 30 *McGill L. J.* 478.

[31]Selon la théorie classique de la coutume, celle-ci se compose de deux éléments : un élément matériel, soit la répétition d'une pratique, un élément psychologique, soit la conviction que cette pratique constitue une règle obligatoire. Voir Francois GÉNY, *Méthode d'interprétation et sources en droit privé positif*, Paris, A. Chevalier-Marescq & Cie, 1899, à la page 278.

[32]Clive M. SCHMITTHOFF, *International Trade Usages*, Paris, ICC Publishing SA, 1984, p. 14.

[33]Sur cette question il suffit pour nos fins de mentionner que la Cour suprême du Canada a reconnu l'importance du rôle des usages dans le commerce international à quelques occasions : *ITO - Intel Terminal Operators* c. *Miida Electronics*, [1986] 1 R. C. S. 752 ; *Q. N. S. Paper* c. *Chartwell Shipping*, [1989] 2 R. C. S. 683 : *Monk Corp.* c. *Island Fertilizers ltd*, [1991] 1 R. C. S. 779.

[34]Sur ces questions voir : Luc BOUCHER, *Op. Cit.*, note 22, p. 41 et ss.

fait que les mêmes interrogations se posent relativement à la réglementation privée qui s'élabore dans les environnements électroniques. Nous reviendrons sur ces questions fondamentales de façon plus spécifique dans les sections subséquentes.

Les usages du commerce international tirent leurs origines de sources diverses. La pratique contractuelle, les codifications professionnelles, les principes généraux du droit de même que les sentences arbitrales apparaissent comme les plus importantes[35]. Parmi ces dernières la pratique contractuelle et les sentences arbitrales jouent un rôle fondamental. La nouvelle loi marchande s'exprime principalement par leur entremise.

La pratique contractuelle du commerce international révèle l'existence de clauses visant à exclure l'application des droits nationaux[36]. Les usages du commerce viennent alors régir ces rapports. Ceux-ci se dégagent

---

[35]D'autres ajoutent à cette liste le droit international public, les lois uniformes, les règles des organisations internationales (résolutions, recommandations, etc ...). Voir à titre d'exemples : Louis KOS-RABIEWICZ, *Le droit du commerce international : une nouvelle tâche pour les législateurs nationaux ou une nouvelle "lex mercatoria" ?* , UNIDROIT, *New Directions in International Trade Law* , Dobbs Ferry, New York, 1977, vol. 2, p. 459 et Ole LANDO, *The law applicable to the merits of the dispute* dans Petra SARCEVIC, *Essays on International Commercial Arbitration* , Londres-Dordrecht-Boston, Graham & Trotman-Martinus Nijhoff, 1989, 247p., p. 129-159. Sur les règles des organisations internationales, c'est-à-dire sur ce qu'il est maintenant convenu d'appeler la *soft law,* voir, de façon générale, Sergei A. Voitovitch, *International Economic Organizations in the International Legal Process*, The Netherlands, Martinus Nijhoff Publishers, 1995, 199 pages.

[36]Certaines clauses vont jusqu'à exclure l'application des lois nationales. Voir par exemple la sentence arbitrale No. 2886 de la chambre d'arbitrage de la Chambre de Commerce Internationale reproduite à (1978) 105 *J. D. I.* 996, à la p. 997. On note également des cas où les parties optent pour un régime mixte à l'intérieur duquel il est fait référence à un droit national et aux usages du commerce, voir à ce sujet Berthold Goldman, *La lex mercatoria dans les contrats et l'arbitrage internationaux : réalité et perspectives*, (1979) *J. D. I.* 474. D'autres clauses sont renvoyées expressément aux usages du commerce et y réfèrent implicitement. Les clauses d'amiable composition et d'équité en sont des exemples. Voir à ce sujet : Éric Loquin, *L'amiable composition en droit comparé et international*, Paris, Librairies Techniques, 1980, 385p.

principalement des sentences arbitrales. Certains affirment même qu'une jurisprudence arbitrale se développe progressivement[37].

Il existe des liens très étroits entre l'arbitrage et les usages du commerce international. L'arbitrage apporte une cohésion aux usages en éliminant, ou à tout le moins en réduisant, les interprétations contradictoires qui autrement risqueraient d'émaner des diverses juridictions nationales[38].

Les codifications professionnelles comptent également parmi les sources de la *lex mercatoria*. Les INCOTERMS[39] de même que les règles et usages du crédit documentaire[40] apparaissent comme les compilations les plus importantes.

Quels enseignements faut-il retenir de ce phénomène ? Tout d'abord, qu'il est possible pour des opérateurs privés de formuler des règles contraignantes et généralement suivies. À cet égard la *lex mercatoria* médiévale représente un précédent historique fort intéressant. Plus intéressant encore, les opérateurs actuels du commerce international se donnent des règles propres à leurs sphères d'activités respectives. Peu importe que l'on reconnaisse ou non à la loi marchande moderne le statut

---

[37]W. Lawrence CRAIG, William W. PARK et Jan PAULSSON, *International Chamber of Commerce Arbitration* , 2e éd., New York-Londres-Rome-Paris, Oceana Publications inc-ICC Publishing S. A., 1990, pp. 621 à 632.

[38]Yves DERAINS, *Le statut des usages du commerce international devant les juridictions arbitrales*, (1973-74) *Rev. Arb.* 122, à la p. 123.

[39]*Incoterms*, Paris, ICC Publishing SA, 1990, 215p. Il s'agit d'une compilation de définition de termes utilisés en matière de transport de marchandises. En plus des définitions, les Incoterms réfèrent également aux droits et obligations des parties à divers types de contrat de transport. On y traite notamment des contrats de types CIF, FOB et FAS.

[40]*Documentary credits*, Paris, ICC Publishing SA, 1984, 87p. Cette compilation porte sur le financement des transactions internationales par crédit documentaire. Cette compilation codifie les solutions retenues pour ce type de financement propre au commerce international.

d'ordre juridique indépendant[41], le fait est que des opérateurs privés se donnent des règles qui gouvernent effectivement leurs rapports.

## 44. *Lex mercatoria* et espace cybernétique

L'intérêt de l'application du modèle de la *lex mercatoria* aux environnements électroniques repose sur la constatation que les divers contrôleurs[42] privés de l'espace cybernétique formulent effectivement des règles. À cet effet Wittes cite Post selon qui :

> *[...] the net community is developing its own custumary practices - and its own means of enforcing them. It has also developed its tribal chieftains - the system operators, or sysops, who administer online services.*[43]

Ces règles d'origine privée, comme les usages du commerce international, pourraient constituer une solution viable aux problèmes de juridiction rencontrés dans cet espace dématérialisé.

De quelle façon faut-il appréhender l'étude de ces règles ? Dans un premier temps, il importe d'inventorier les règles formulées par les opérateurs privés qui évoluent dans cet environnement. Puis, nous nous devons de nous interroger sur certains aspects bien précis de la question. Quelles sont ces règles ? Qui les formule ? Quel est leur contenu ? Quels types de rapports sont régis par ces règles ? D'où provient le pouvoir de sanctionner le non-respect de ces règles ? Bref, il s'agit ici de procéder à l'examen le plus complet possible des sources, de la nature, du contenu et de l'efficacité de ces règles.

---

[41]Cette question est l'une des questions au centre du débat qui perdure en doctrine relativement à ces règles.

[42]L'expression n'est pas de nous mais de David Post. Voir David POST, *Anarchy, State, and the Internet : An Essay on Law-Making in Cyberspace*, (1995) *J. Online L.* article 3.

[43]Bejamin Wittes, *Loc. cit.*, note 25, p. S28.

### 44.1 Lex electronica ?

Les problèmes de juridiction mentionnés précédemment amènent certains commentateurs à s'interroger sur la nature des règles qui vont gouverner les rapports qui s'établissent dans l'espace cybernétique[44]. Parmi ces commentateurs, Post[45] expose qu'il faut notamment se questionner relativement à l'identité des intervenants qui ont le pouvoir de réguler cet environnement. Qui formulera les règles ? Qui veillera à leur application ?

Post insiste sur la difficulté pour les États d'exercer leur monopole juridictionnel dans l'espace cybernétique. À son avis, la réglementation de cet espace dématérialisé ne sera pas uniquement l'apanage de l'État. Une compétition pour la formulation des règles entre les différents contrôleurs s'installe. Bien que conscient de cet aspect de la question, nous ne sommes concernés ici que par les initiatives privées de réglementation. Ce type de réglementation puise à plusieurs sources[46] : l'éthique personnelle, les usages qui se dégagent de la pratique de certaines activités au sein de certains groupes d'usagers, le contrat, les règles formulées par certaines organisations privées. Nous nous proposons donc d'examiner ces diverses composantes.

---

[44]Notamment David POST, *Anarchy, State, and the Internet : An Essay on Law-Making in Cyberspace*, (1995) *Journal of Online Law* article 3 disponible à :

http://www.law.cornell.edu/jol/post.html

I. Trotter HARDY, *The proper legal regime for cyberspace*, (1994) 55 *Pittsburg Law Review* 993 ; David R. JOHNSON et Kevin A. MARKS, *Mapping Electronic Data Communications onto Existing Legal Metaphors : Should we let our Conscience*, (1993) 38 *Villanova Law Review* 487 ; Pierre TRUDEL, *Internet et Commerce Électronique : Réglementation et Autoréglementation*, Conférence donnée à Montréal le 30 Août 1995 dans le cadre du colloque Faire des affaires en toute sécurité sur les autoroutes de l'information..

[45]David POST, *Anarchy, State, and the Internet : An Essay on Law-Making in Cyberspace*, (1995) *Journal of Online Law* article 3, par. 4.

[46]Voir Pierre TRUDEL, *Loc. cit*, note 43.

L'Internet est aujourd'hui le plus important réseau au monde[47]. En fait il ne s'agit pas d'un réseau au sens classique du terme mais plutôt d'un réseau de réseaux[48]. L'importance de l'Internet justifie que l'on s'attarde aux règles développées par les acteurs qui contribuèrent grandement à sa formation et à son développement. Le National Science Foundation (NSF) joua un rôle de premier plan dans le développement de l'Internet. L'ancêtre de ce dernier, ARPAnet, pour diverses raisons, techniques et politiques, s'avéra être un échec[49]. La NSF assura alors la succession de ARPAnet. Le NSF créa donc son propre réseau, beaucoup plus rapide que l'ARPAnet, et par la suite s'employa à connecter les réseaux régionaux les uns aux autres.

Le NSFnet fût jusqu'au 30 avril dernier[50] le réseau le plus important aux États-Unis. Considérant son importance, il nous apparaît essentiel de nous attarder à son code de conduite[51]. En effet, malgré la disparition du NSFnet, son code de conduite demeure un outil de comparaison intéressant, et ce, pour deux motifs. Tout d'abord, il est difficile de concevoir un code qui soit plus restrictif quant aux activités permises. Pour cette raison il constitue une unité de comparaison intéressante. D'ailleurs, certains des éléments essentiels de cette politique ont constitué, à notre avis, un empêchement sérieux au développement du commerce sur l'Internet. Sans aller jusqu'à dire que cette politique empêcha totalement le développement des activités

---

[47]Bien qu'une évaluation exacte du nombre d'utilisateurs de l'Internet s'avèere presqu'impossible, il n'en demeure pas moins que certains indicateurs permettre d'en estimer le nombre de 20 à 40 millions de personnes. S'il est difficile d'estimer le nombre exact d'utilisateurs, il est cependant possible de déterminer le nombre d'ordinateurs branchés sur l'Internet. Ainsi, Mark Lottor a recensé, en juillet 1996, plus de 10 millions d'hotes sur l'Internet.

[48]John R. LEVINE et Carol BAROUDI, *The Internet for Dummies*, 2e éd., Foster City-Chicago-Indianapolis-Braintree-Dallas, 1994, p. 7.

[49]*Id.*, p. 13.

[50]Ce réseau, fort important dans le développement de l'Internet, a été débranché le 30 avril dernier. Ce réseau concu au départ comme une expérience, fut pendant plusieurs années le plus important réseau sur l'Internet.

[51]*The NSFnet Backbone Services Acceptable Use Policy*, disponible à :

gopher://riceinfo.rice.edu:1170/00/more/Acceptable/nets/nsfnet.txt

commerciales, force est de convenir à tout le moins qu'elle compliquait grandement les choses. En agissant de la sorte elle eut également pour effet de ralentir le développement de règles relatives aux transactions commerciales. Il apparaît donc nécessaire de s'attarder à cette politique afin de bien appréhender toute la portée de sa disparition.

La disparition du NSFnet et la nouvelle structure adoptée par les américains nous portent à croire que des changements majeurs sont à prévoir relativement au contenu des politiques applicables sur les réseaux les plus importants. À notre avis, la disparition du NSFnet annonce une ère de libéralisation des activités commerciales sur l'Internet. Nous reviendrons un peu plus loin sur cette question. Au préalable, il importe de s'attarder aux différents codes applicables.

Une étude des codes de conduites en vigueur sur les différents réseaux permet de constater qu'il en existe trois types. Bien que semblables au niveau de leur forme et de leur structure, ils se distinguent les uns des autres par leur caractère plus ou moins restrictif. Le code du NSFnet constituait sans contredit le plus restrictif des codes de conduites. Les politiques des réseaux régionaux pour leur part s'avèrent, en général, plus permissives que celles du NSFnet alors que les réseaux commerciaux accordent généralement une plus grande latitude que les réseaux régionaux[52].

### 44.1.1 Les “Acceptable use policies”

Pour l'essentiel, ces codes, désignés par le terme “Acceptable Use Policies” (ci-après AUP), constituent des règles de conduite que l'usager doit suivre afin de conserver son accès à un réseau donné[53]. Plus de 25 000 réseaux sont actuellement branchés sur l'Internet et la plupart d'entre eux possèdent leur propre AUP. Les usagers sont tenus de respecter non seulement le AUP du réseau sur lequel ils sont branchés mais également les AUP de tous les réseaux par lesquelles leurs communications transitent[54].

---

[52]Voir également en ce sens J. R. LEVINE et C. BAROUDI, *op. cit.,* note 16, pp. 62-63.

[53]Jill H. ELLSWORTH et Matthew V. ELLSWORTH, *The Internet Business Book*, http://www.oak-ridge.com/ibbch4p1.html

[54]*Id.,* par exemple le AUP de l'université Yale reproduit à

Bien qu'à première vue cette exigence puisse paraître difficile à satisfaire, la pratique démontre qu'il ne s'agit pas là d'une condition impossible à rencontrer, et ce pour deux motifs.

Tout d'abord, on remarque que la plupart des AUP présentent un contenu assez similaire[55]. Au surplus, une part importante du trafic de l'Internet transitait par le NSFnet. En conséquence, plus souvent qu'autrement, vu le caractère restrictif de cette politique, il suffisait de se conformer aux règles en vigueur sur ce réseau afin de respecter les règles applicables sur les autres réseaux[56]. D'ailleurs cela demeure encore vrai aujourd'hui. Il est évident qu'en se conformant à ce standard de conduite les risques de violer les règles applicables sur un réseau donné se trouvent réduits de façon significative.

Le NSFnet “acceptable use policy” (AUP) comprenait trois sections : principe général, usages acceptables et usages inacceptables. La principale caractéristique de ce document résidait dans l'interdiction très ferme et très claire de se livrer à des activités de nature commerciale à partir de ce réseau. L'article 10 interdisait expressément toute activité ayant pour objectif la réalisation d'un profit. L'usage excessif du NSFnet à des fins personnelles ou privées était également prohibé. L'article 1 pour sa part indiquait que la fonction principale du réseau consistait à supporter la recherche et l'éducation au sein de la communauté des chercheurs et du système éducatif américain. L'utilisation du réseau pour d'autres fins était considérée comme inacceptable. Cette politique proscrivait également la publicité de produits ou services autres qu'académiques[57].

---

http://www.cis.yale.edu/policy_doc.html

prévoit que : *Users must observe all applicable policies of external data networks when using such networks.*

[55] *Id.*

[56] *Id.*

[57] Article 7.

Le NSFnet autorisait un large éventail d'activités académiques[58]. Toutefois, même en cette matière, certaines activités étaient assorties de conditions d'exercice précises. Ainsi les communications entre chercheurs ou éducateurs américains avec leurs collègues étrangers bien que permises ne l'étaient que dans la mesure où le réseau utilisé par le collègue étranger accordait un accès réciproque aux chercheurs et éducateurs américains.

Les communications non énumérées dans cette politique étaient permises à condition de demeurer accessoires à l'un ou l'autre des usages acceptables énumérés. Finalement, le trafic en provenance de réseaux d'agences membres du Federal Networking Council étaient autorisées à condition de respecter la politique de cette agence.

Les universités américaines jouèrent également un rôle primordial dans le développement de l'Internet[59]. Bien qu'il soit impossible[60] de passer en revue l'ensemble des AUP actuellement en vigueur sur les réseaux de ces institutions, il demeure possible de se faire une idée assez juste de la situation en se référant aux codes des institutions universitaires les plus importantes[61]. Au surplus, considérant les similarités en cette matière la

---

[58]Les activités suivantes sont permises : les communications et échanges professionnels afin de maintenir ses connaissances à jour, demandes de subventions ou de contrats de recherche, communications administratives en relation directe avec la recherche ou l'enseignement, publicité concernant de nouveaux produits pour utilisation en recherche et dans l'enseignement.

[59]Eric C. RICHARDSON, *Internet Cum Laude*, Vol. 6 n. 10 *Internet World* p. 38 (Octobre 1995) : *When the Internet began as the ARPAnet, it was the higher educational institutions- with funding from the U. S. Department of defense- that spearheaded the effort. [...] Universities and the Internet have existed in a symbiotic relationship since the network began. As the Net developed across the world in the 1970s, it was colleges that most of the applications we use today-Archie, Gopher, and the like-were created and implemented.*

[60]Il en existe plus de 25 000.

[61]Pour un échantillon représentatif consulter les sites suivants :

http://musie.phlab.missouri.edu/Policy/copies/

http://musie.phlab.missouri.edu/Policy/copies/rice-rights-collection.html

http://musie.phlab.missouri.edu/Policy/copies/tamu-collection1.html

lecture de quelques unes de ces politiques permet tout de même d'en dégager les règles les plus généralement acceptées[62].

Une lecture de certaines des politiques des institution universitaires américaines et anglaises les plus en vue[63], permet de dégager certains éléments communs. Ainsi de façon générale on peut affirmer que ces codes prohibent les comportements suivants :

- Activités commerciales (y compris interdiction de faire de la publicité) ;
- Harcèlement (sous toutes ses formes) ;
- Intimidation ;
- Diffusion de matériel "inapproprié"[64] ;
- Interférence ou altération du système ;
- Limitation ou négation de l'accès du réseau aux autres usagers ;
- Transmission de matériel représentant une menace ou pouvant représenter une menace pour les autres usagers ;
- Accès aux dossiers des autres usagers sans une autorisation expresse ;
- Interception ou lecture de communications destinées à d'autres usagers. Il est notamment interdit de tenter de déchiffrer un message qui est encrypté ;

---

[62]Jill H. ELLSWORTH et Matthew V. ELLSWORTH, *The Internet Business Book*, http://www.oak-ridge.com/ibbch4p1.html

[63]Voir Notamment les *acceptable use policies* suivantes : aux États-Unis : Princeton, Cornell, Purdue, MIT, Tulane, Rice, Texas, Notre Dame, UC Davis, Yale ; en Angleterre : JANET (Ensembles des réseaux académiques anglais), NERC (National Environment Research Council), Edimbourg, Southampton.

[64]Cependant, aucune des politiques consultées ne précisent ce qui constitue du matériel inapproprié.

- Création de logiciels “shareware” ayant la capacité de collecter secrètement de l'information sur d'autres usagers ;
- Utilisation du courrier électronique pour diffuser un message à l'ensemble de la communauté ;
- Participation à une chaîne de lettre ;
- Tenter d'obtenir ou utiliser le code d'accès d'un autre usager.

Le droit à la vie privée de même que les droits d'auteur font l'objet de mentions spécifiques dans la plupart des AUP. On note également que l'ensemble de ces politiques tiennent l'usager responsable de l'utilisation qui est faite de son compte. Au surplus, le code d'accès de l'usager doit demeurer confidentiel. On note également que la liberté d'expression, sur la base du principe de la liberté académique, apparaît comme une liberté fondamentale[65].

Toutefois, on remarque une plus grande disparité au niveau de la sanction de ces règles. Ainsi, certaines politiques n'en prévoient tout simplement pas. On peut croire, dans ces cas, que les règles générales de discipline de l'institution s'appliquent en y apportant les modifications nécessaires le cas échéant. Certaines stipulent vaguement que le non respect de ces prescriptions peut entraîner l'une des sanctions suivantes : poursuites en vertu de la loi applicable sur le territoire de l'institution, la suspension ou la révocation du privilège d'accès.

L'AUP de l'université Yale constitue une exception notable à cette tendance[66]. Cette politique prévoit spécifiquement que le computer & Information système (CIS) possède le pouvoir d'imposer des pénalités en cas de contravention. Ces pénalités sont : la diminution des privilèges, la suspension ou la révocation des privilèges. Cette entité possède également le pouvoir de suspendre le privilège d'accès lorsque cela se révèle nécessaire afin de préserver l'intégrité du système. La personne visée par la procédure doit cependant être avisée des actes ou comportements reprochés. On doit

---

[65] Dorothy E. DENNING et Herbert S. LIN (dir.), *Op. cit.*, note 2, 1994, p. 20.

[66] AUP Yale,

http://musie.phlab.missouri.edu/policy/copies/yale.txt

également lui accorder l'opportunité de répondre aux accusations portées contre elles. D'ailleurs, “l'accusé” bénéficie d'un droit d'appel auprès du directeur du CIS en cas de décision défavorable.

En plus de la politique de l'université Yale une autre politique se démarque. Il s'agit du AUP de l'université UC Davis. Celle-ci représente sans doute l'une des politiques les plus complètes qui soit. On remarque notamment que l'administrateur de réseau dispose de larges pouvoirs d'enquête afin de veiller au respect de cette politique[67]. Plus spécifique dans sa formulation que le document du NSFnet, la politique de cette institution universitaire prévoit expressément certaines sanctions en cas de non-respect des règles qu'elle énonce. L'accès au réseau n'est pas un droit mais plutôt un privilège et, à ce titre, peut être retiré en cas de non respect des prescriptions de ce code[68]. On note également que cette politique énumère de façon assez détaillée, quoique non exhaustive, les comportements considérés comme inappropriés. Tout comme dans le cas de la politique du NSFnet, les activités de nature commerciale sont interdites[69].

Considérant l'importance du rôle joué par le milieu universitaire et la communauté des chercheurs dans le développement de l'Internet, ces clauses de “non-commercialité” n'ont pas de quoi surprendre. Toutefois, malgré ces clauses on note que des transactions commerciales ont lieu dans les environnements électroniques. D'ailleurs Amelia Boss souligne que :

> *Although neither a national or an international legal framework currently exists to guide the conduct of electronic*

---

[67]Sous la rubrique Rights and Responsabilities il est mentionné que : *... system administrators may access user files as required to protect the integrity of computer systems. [...] system administrators may access or examine files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged.*

[68]Le second paragraphe de la section sur le "Existing Legal Context", précise que : *Misuse of computing, networking or information resources may result in the loss of computing and/or network privileges.*

[69]Il est précisé que : *Using your account for any activity that is in commercial nature, i. e. paid by non-University funds. Commercial activities include, but are not limited to, consulting, typing services, and developing software for sale.*

> *commerce, such commerce nevertheless occurs on a substantial basis.*[70]

Le professeur Boss ajoute qu'il importe de reconnaître l'importance des pratiques du commerce dans le cadre du processus de réforme du droit international[71]. Considérant l'apparition de réseaux commerciaux de plus en plus nombreux et l'habitude des opérateurs du commerce international à développer des règles pour gouverner leurs rapports, il y a fort à parier que le commerce électronique deviendra un élément, sinon l'élément clé, de l'élaboration d'une éventuelle *lex electronica*. Ces règles pourraient notamment provenir des opérateurs privés[72]. De plus, la disparition du NSFnet a pour conséquence une forte croissance pour ne pas dire une explosion des activités commerciales dans les environnements électroniques. Nous reviendrons sur cette question de façon plus détaillée un peu plus loin. De plus, une modification de la réglementation est également à prévoir.

### 44.1.2 Le “Netiquette” et les usages

Lorsque l'on sait l'importance des usages dans le développement de la *lex mercatoria*, nul n'est besoin d'insister sur l'importance du rôle qu'ils pourraient jouer dans l'élaboration d'une éventuelle *lex electronica*. D'entrée de jeu soulignons que déjà certaines pratiques semblent apparaître dans l'espace cybernétique. Notre objectif n'est pas ici de passer en revue l'ensemble de ces pratiques mais plutôt d'en fournir certains exemples.

---

[70] Amelia H. BOSS, *The Emerging Law of International Electronic Commerce*, (1992) 6 *Temple International & Comparative Law Review* 293, p. 303.

[71] *Id.*

[72] Amelia H. BOSS, *Security : It Ain't Just A Matter of Encryption : The Development of Legal Infrastructures to Support the Growth of Electronic Commerce* , Conférence donnée à Montréal dans le cadre du colloque Faire des Affaires en toute sécurité sur l'autoroute de l'information. Encore une fois cette opinion découle du sérieux problème de juridiction qui affecte la réglementation de l'espace cybernétique : "Some people have asserted that there will eventually be a "law of cyberspace" ; a separate legal jurisdiction for all networks. Whether that will evolve or not, the real problem is that given today's apportionment of law making power among national sovereigns, there are serious questions about the applicability of national laws to this new "space".

L'expression Netiquette désigne un ensemble de principes destinés à assurer un certain ordre dans l'espace cybernétique. D'entrée de jeu la question de leur qualification juridique se pose. Cependant, avant toute chose une description de ces principes nous apparaît essentielle.

En ce qui a trait au contenu il nous semble raisonnable de nous en remettre à la description qu'en donne Arlene H. Rinaldi dans son ouvrage sur le sujet[73].

La qualification de l'utilisation de l'Internet ressort comme l'élément le plus fondamental de cet ensemble de règles. Ainsi il semblerait qu'il n'existe pas de droit d'accès aux réseaux. Il s'agirait davantage d'un privilège[74]. Sur ce point, le “netiquette” rejoint la solution retenue par la majorité des AUP.

Certains types de comportements pourraient entraîner la suspension voir la révocation de ce privilège. Ainsi les comportements suivants feraient l'objet de sanctions : l'affichage d'informations illégales, l'emploi d'un langage abusif dans le cadre de communications publiques ou privées, l'envoi de messages entraînant la perte d'informations, l'envoi d'une chaîne de lettres, ou encore la diffusion de messages destinés à des listes ou des individus entraînant la congestion d'un réseau ou interférant avec le travail d'autres individus. Précisons toutefois qu'il ne peut y avoir révocation permanente qu'après révision par un comité habilité à enquêter relativement à de tels abus.

Ces prescriptions couvrent une large variété de sujets tels : l'utilisation du courrier électronique, l'utilisation de telnet, le transfert de fichiers, l'utilisation du world wide web (WWW), etc ...

Il s'agit d'un ensemble de principes fort développés et très précis dans leur formulation. Évidement, reste à savoir si les utilisateurs se sentent liés par ces principes.

---

[73]Arlene H. RINALDI, *The Net : User Guidelines and Netiquette*, 1995 :

http://www.fau.edu/rinaldi/net/index.html

[74]A cet effet soulignons que la plupart des AUP mentionnent expressément que l'accès au réseau constitue un privilège.

Les dix commandements du Computer ethics institute[75] feraient également partie de cet ensemble. Ces commandements, pour l'essentiel, sont des règles générales auxquelles il semble plutôt difficile de s'opposer. Il s'agit en quelques sorte de règles de civisme de l'espace cybernétique. Elles énoncent que :

> *1. - Thou shalt not use a computer to harm other people ;*
>
> *2. - Thou shalt not interfere with other people's computer work ;*
>
> *3. - Thou shalt not snoop around in other people's files ;*
>
> *4. - Thou shalt not use a computer to steal ;*
>
> *5. - Thou shalt not use a computer to bear false witness ;*
>
> *6. - Thou shalt not use or copy software for wich you have not paid ;*
>
> *7. - Thou shalt not use other people's computer ressources authorization ;*
>
> *8. - Thou shalt not appropriate other people,s intellectual output ;*
>
> *9. - Thou shalt think about the social consequences of the program you write ;*
>
> *10. - Thou shalt use a computer in ways that show consideration and respect.*[76].

Là encore, il faut se demander s'il s'agit de règles d'éthique ou encore de règles susceptibles de sanctions. Une étude de certaines communautés d'usagers apparaît donc comme essentielle afin de nous permettre de constater le niveau d'effectivité de ces règles.

---

[75]Nous procéderons à une description plus détaillée du rôle et de l'importance de cet organisme un peu plus loin.

[76]Reproduit à :

http://www.fau.edu. /rinaldi/net/ten.html

Le cas le plus connu de ce type de “communauté” demeure USENET. Cette entité est constitué d'un ensemble de sites qui pour l'essentiel s'échangent de l'information entre eux. Ces sites sont connus sous le nom de “newsgroups” ou “news”. En fait USENET est un ensemble de “newsgroups”. On peut même aller jusqu'à affirmer qu'il est le plus connu des “newsgroups”[77]. L'information est organisée selon les divers sujets traités. Chaque “newsgroups” porte sur un sujet bien déterminé. De façon plus précise on peut en donner la définition suivante :

> *Usenet is a world-wide distributed discussion system. It consists of a set of “newsgroups” with names that are classified hierarchically by subject. “Articles” or “messages” are “posted” to these newsgroups by people on computers with the appropriate software -- these articles are then broadcast to other interconnected computer systems via a wide variety of networks. Some newsgroups are “moderated” ; in these newsgroups, the articles are first sent to a moderator for approval before appearing in the newsgroup. Usenet is available on a wide variety of computer systems and networks, but the bulk of modern Usenet traffic is transported over either the Internet or UUCP.*[78]

Il semble bien que les “membres” de la “communauté” USENET ait développé certaines “coutumes”[79]. On retrouve une compilation de ces règles[80] affichée sur l'un des “newsgroups”[81] de USENET. Il existe par

---

[77]Pour une description plus complète de ce qu'est USENET voir John R. LEVINE et Carol BAROUDI, *Op. cit.,* note 47, p. 129 et ss. voir aussi :

http://skeena.ucs.ubc.ca/o/appropriate-use/usenet_whatis

[78]What is Usenet ? :

http://www.smartpages.com/faqs/usenet/what-is/part1/faq.html

[79]Bejamin Wittes, *Loc. cit.,* note 25, p. S29.

[80]Cette compilation est disponible à news. annonce. newusers. Également reproduit à :

http://skeena.ucs.ubc.ca/O/appropriate-use/usenet-etiquette

exemple un ensemble de règles particulièrement développées relativement à l'affichage sur USENET[82]. Certains comportements, comme le "spamming"[83], semblent être strictement interdits. De la même façon il semble que la publicité ne soit pas tolérée dans cette "communauté"[84]. Un "newsgroup" a été créé spécifiquement afin de traiter des abus de l'Internet[85].

De façon sommaire il semble que les comportements suivants ne soient pas tolérés dans la "communauté" Usenet :

- afficher un message sur un Newsgroups inapproprié ;
- afficher un message sur un trop grand nombre de newsgroups ;
- poser des questions qui se trouvent sur un FAQ[86] ;
- afficher une chaîne de lettre ;

---

[81]Il s'agit de news. admin. net-abuse.

[82]Rules for Posting to USENET :

http://www.cis.ohio-state.edu/hypertext/faq/usenet/posting-rules/part1/faq.html

[83]Le "spamming" consiste à afficher la même information sur un nombre relativement élevé de "newsgroups". Le contenu du message n'est pas pertinent. Le spamming se mesure de façon objective : le message a t-il été affiché x fois ? Voir news. admin. ney-abuse FAQ,

http://www-sc.ucssc.indiana.edu/~scotty/acena.html

[84]Pierre BEYSSAC, *Non à la publicité sur Usenet :*

http://www.freenix.fr/liste-pub/

[85]alt. current-events. net-abuse, " alt. current-events. net-abuse is a forum to discuss the current net abuses, such as "spamming" of Usenet by the law firm Canter & Siegel, and related issues", voir news. admin. net-abuse FAQ :

http://www-sc.ucssc.indiana.edu/~scotty/acena.html

[86]Les FAQ (pour Frequently asked questions) sont des documents relatifs à un sujet bien précis qui sont disponibles très facilement sur Usenet et l'Internet et qui visent à répondre aux questions des non-initiés.

- affichage qui contrevient aux règles des sociétés matérielles ;
- poser des questions non nécessaires ou demander une assistance excessive ;
- Dans les groupes où l'on discute de télévision et de films il est mal vue de révéler l'intrigue ;
- Longues citations d'affichages antérieurs ;
- afficher un message à partir du compte d'un autre usager ;
- afficher une attitude teintée de racisme ;
- "baiting" i. e. afficher un message qui est clairement en contravention des conventions établies ;
- signature trop longue ;
- écrire en lettres majuscules ("shouting") ;
- tenir des conversations privées sur Usenet.

North précise que :

> *New users are all expected to read the informational postings in groups such as news. annonce. newusers, news. answers and news. newusers questions. Questions posted to other newsgroups asking about matters that are clearly dealt with these introductory group are likely to be met either with silence or irritation*[87].

North remarque également qu'il existe des sanctions en cas de contravention à ces règles :

> *Extreme transgressions of the Net's cultural norms will prompt some users to complain to the offending individual's sysadmin's requesting that some action be taken against the*

---

[87]Tim NORTH. *The Internet and Usenet Global Computer Networks : An investigation of their culture and its effects on new users,*

http://foo.curtin.edu.au/thesis/default.html

> *individual. Such action can lead to the user's account being removed, thus denying him or her access to the Net (at least via that account).* [88].

La menace de contacter les autorités extérieures à la communauté Usenet constitue également un mode de sanction de ces règles.

Il semble donc que, dans le cadre limité de cette communauté d'usagers, ces règles soient contraignantes.

### 44.1.3 La pratique contractuelle

Tel que mentionné précédemment, les contrats constituent une source essentielle des usages élaborés par les opérateurs du commerce international. Il semble bien qu'il pourrait en être de même en matière de réglementation de l'espace cybernétique.

Évidemment, il n'est pas tellement difficile d'imaginer que les contrats jouent un rôle dans la gestion des relations entre les usagers et les fournisseurs de service. Ainsi, les usagers désireux d'avoir recours aux services d'un fournisseur doivent consentir à se conformer aux contrats de services de ce dernier. Ces ententes de services ne sont pas négociables, l'usager possède l'option d'y adhérer ou de ne pas y adhérer. Il s'agit là, sans l'ombre d'un doute possible, de contrats d'adhésion. Au surplus, ces ententes sont complétées par les notices affichées par le fournisseur de services[89]. Reste à savoir si une certaine uniformité règne entre les différents fournisseurs de services.

Cependant, une question beaucoup plus complexe émane de l'examen des rapports contractuels qui se créent dans l'espace cybernétique. En effet, cet examen pourrait entraîner, à notre avis, une remise en cause de la théorie classique du contrat.

---

[88] *Id.*

[89] Il s'agit de ce qu'on appelle les "operating rules". Voir à titre d'exemple le contrat de services de Compuserve.

Ainsi, Perrit estime que le rôle du droit sera plutôt limité en ce qui concerne la réglementation de l'espace cybernétique[90]. Toutefois, les contrats seront appelés, à son avis, à jouer un rôle primordial. Il constate que les communautés de réseaux formulent des règles et que celles-ci sont effectivement appliquées par les réseaux[91]. Il ajoute que plus les réseaux seront interconnectés, plus il sera difficile de faire respecter ces règles. Il poursuit dans la même veine en affirmant que plus les réseaux seront interdépendants plus la nécessité d'une autorité centrale se fera sentir[92]. L'auteur laisse toutefois ouverte la question de savoir quelle pourrait être cette autorité.

Afin de bien illustrer l'importance du rôle du contrat, Perrit identifie trois conflits potentiels : un individu désire se brancher à un réseau mais un ou plusieurs usagers de ce réseau s'y opposent, un individu veut empêcher la circulation d'un certain type d'information alors que la personne qui fait circuler cette information désire continuer à le faire, un usagers du réseau estime qu'un autre usager ne remplit pas ses obligations[93].

Ceci étant dit, il soumet trois modèles législatifs possibles[94] :

- Modèle autoritaire : le fournisseur de service établit unilatéralement les règles d'accès et de conduite ;
- Modèle démocratique : une association d'usagers, d'opérateurs de réseaux ou encore une association professionnelle élabore les règles ;
- Modèle légal formel : l'offre et l'acceptation du contrat détermine le droit d'accès et les règles de conduite,

---

[90] William H. PERRIT Jr., *Dispute Resolution in Electronic Network Communities*, (1993) 38 *Villanova Law Review* 349, p. 350.

[91] *Id.*, p. 352.

[92] *Id.*, p. 353.

[93] *Id.*

[94] *Id.*, p. 354.

> les lois et règlements s'appliquent, le droit de la responsabilité civile trouve application, etc ...

L'auteur examine ensuite les avantages et désavantages que présentent chacun de ces modèles. Cependant, il n'est pas utile pour l'instant de s'arrêter sur ces questions. Il apparaît néanmoins essentiel d'examiner les raisons qui amènent Perritt à remettre en question la théorie classique du contrat.

Selon Perritt, la théorie relationnelle du contrat serait plus appropriée à certains des rapports que l'on retrouve dans l'espace cybernétique. Cette théorie du contrat formulée par MacNeil[95] dans les années 70 met l'accent sur la continuité des relations contractuelles. De l'avis de Perritt la réalité des environnements électroniques lie cette théorie aux modèles autoritaire et démocratique mentionnés précédemment. Perritt résume la théorie relationnelle du contrat de la façon suivante :

> *Under the relationnal theory, obligations are not frozen in an initial bargain. They evolve over time as circumstances change, guided by norms of the particular community within wich the relation exist. [...] The object of contracting is to establish and define a cooperative relationship, not merely to allocate risk. [...]*
>
> *Because, under the relational theory, the parties expect the terms of their relationship will evolve, there is no need for formalities to validate new practices in order to make those practices part of the contract.*[96]

Au-delà de la détermination de la théorie du contrat rendant le mieux compte de la réalité cybernétique, il n'en demeure pas moins que le contrat est appelé à jouer un rôle de premier plan. Par exemple, Dunne avance que le contrat pourrait servir d'instrument régulateur en matière de droit criminel.

---

[95]Ian R. MacNeil, *The many futures of contracts*, (1974) 47 *Southern California Law Review* 691.

[96]William H. PERRIT Jr., *Loc. cit.,* p. 369.

Dunne[97] avance que le droit des contrats pourrait se révéler plus approprié que le droit criminel pour régir certains comportements criminels. Il évoque notamment le problème de juridiction en matière criminelle[98]. Il qualifie ce problème d'insurmontable et s'exprime comme suit :

> *In cyberia, distance is irelevant. There is no single nation whose law viably control behavior in cyberspace. The minimal utilisation of federal law is not a reflection of incompetence or indifference, but of reality. Short of new international law and inforcement mechanisms, there is no viable way to impose existing criminal law on general behavior in cyberspace*[99].

À son avis, un modèle contractuel de réglementation en cette matière comporte plusieurs avantages par rapport au modèle traditionnel législatif : le contrat repose sur la volonté des parties ce qui est en harmonie avec la culture de l'espace cybernétique, le contrat permet de localiser les mécanismes de sanction, et, puisqu'il y a entente entre les parties, le problème de juridiction ne se pose pas.

Dunne n'écarte pas totalement l'application des droits criminels nationaux, il va même jusqu'à préciser que ceux-ci continueraient de s'appliquer aux infractions les plus sérieuses. Cependant, ils ne trouveraient plus application relativement aux comportements moins “sérieux” tel que la plupart des accès non autorisés aux ordinateurs[100].

---

[97]Robert L. DUNNE, *Detering unauthorized access to computers : controling behavior in cyberspace through a contract law paradigm*, (1994) 35 *Jurimetrics Law* 1-15.

[98]Bien que conscient du problème de juridiction que pose cette branche du droit Shackelford abonde plutôt dans le sens d'une réforme des droits nationaux par le biais d'une entente international afin d'accroitre la coopération dans la lutte contre les crimes informatisés. Voir Steve SHACKELFORD, *Computer-related crime : an international problem in need of an international solution*, (1992) 2 *Texas International Law Journal* 479-505.

[99]Robert L. DUNNE, *Loc. cit.*, note 97, p. 10.

[100]*Id.*, p. 12.

Il propose la rédaction d'un code de conduite dans lequel des infractions seraient spécifiquement énumérées. Il faudrait ensuite que les hôtes présents sur l'Internet adhèrent à ce code et exigent de leur usagers qu'ils signent une entente à l'effet qu'ils acceptent les termes de ce code. Les usagers désirant utiliser un "alias" devraient s'enregistrer auprès de leur fournisseur de services. Les hôtes qui maintiennent des sites, les opérateurs de réseaux de même que les fournisseurs de services se verraient alors chargés de veiller au respect de ces dispositions contractuelles à titre de cocontractants[101].

Bien que le mécanisme contractuel laisse entrevoir des possibilités fort intéressantes, il n'en demeure pas moins que certaines questions persistent (preuve, écrit, etc ...).

### 44.2 Le commerce électronique et la clause de "non-commercialité"

Considérant, l'interdiction faite par la majorité des AUP, y compris celle du NSFnet, de se livrer à des activités commerciales, il peut sembler difficile de concevoir que le commerce électronique puisse se développer. Toutefois, il n'en est rien car force est de constater que les sites commerciaux ne cessent de se multiplier. Un auteur va même jusqu'à affirmer que l'Internet est maintenant un réseau commercial[102]. On note que les résultats de la dernière étude[103] sur les domaines[104] révèlent que l'on

---

[101] *Id.* p. 13.

[102] Jeff UBOIS, *The Great Facilitator*, (1995) vol. 6 no. 10 *Internet World* 62. *While the Internet today is very much a commercial network, it has many of its roots in the educationnal community ...*

[103] Celle-ci date de juillet 1995. Les résultats de cette étude réalisées par Network Wizards, sont disponibles à :

http://www.nw.com/zone/WWW/report.html

trouve plus de 1,7 millions de sites commerciaux sur l'Internet[105]. Le phénomène ne date pas de la disparition du NSFnet car les sites commerciaux connaissent une croissance exceptionnelle pour ne pas dire renversante depuis deux ans déjà :

> *The Internet's commercial domain (. com) has been the fastest growing segment over the last two years and is now the largest domain. There were roughly 76 000 commercial adresses registered with the InterNIC as of july 1995, compared with 29 000 in december 1994, and 17 002 in july 1994. During June 1995, approximately 8 000 new commercial registrants were added, while in May more than 10 000 new. com addresses were registered according to Internet Info, a domain analysis firm in Falls Church, Va*[106]

D'ailleurs, il suffit de consulter la première édition du *Buyer's guide to electronic commerce*[107] pour se rendre compte de l'ampleur du phénomène. De plus, l'impact des technologies de l'information sur la façon de faire des affaires ne fait aucun doute[108]. Ces technologies ont donné naissance à une

---

[104]Le nom d'un site Internet doit être décodé de gauche à droite. La partie la plus à droite du nom est la désignation de la nature du site. Il existe deux types de désignation soit à trois lettres et à deux lettres. Il existe 7 désignation de zone à trois lettre : com (commercial), edu (institutions d'éducations), gov (gouvernement et agences gouvernementales), int (organisations internationales), mil (sites militaires), net (organisations de réseaux) et org (toute organisations qui ne peut être incluses dans les catégories précédentes). La partie suivante est le nom de la personne ou de l'organisation. Lorsqu'il est question de domaine c'est de cette partie dont il est question. Pour un exposé plus détaillé sur cette question voir : John R. LEVINE et Carol BAROUDI, Op. cit., *note 47*, p. 58 à 62. Voir p. 61 de cet ouvrage pour une liste des désignations ne comportant que deux lettres.

[105]Les sites académiques représentent le deuxième groupe en importance avec plus de 1. 4 millions de sites.

[106]Cynthia BOURNELLIS, *Internet '95*, *Internet World*, Novembre 1995, p. 47.

[107]Electronic Commerce Strategies Inc., *Buyer's Guide to Electronic Commerce*, Marietta, Debbie Shaw, 1995.

[108]Sur cette question voir : Amelia H. BOSS, *Loc. cit.*, note 70, p. 293.

nouvelle industrie avec l'apparition de services tels les fournisseurs d'accès[109] ou encore les réseaux à valeur ajoutée[110].

Dès avant la disparition du NSFnet on assistait déjà au développement du commerce électronique. Ce développement s'explique entre autre par la tendance des réseaux régionaux à permettre une gamme plus large d'activités[111] que le NSFnet. Ainsi, les politiques de réseaux de niveau intermédiaire, tels MICHnet, JvNCnet et MIDNet, n'interdisent pas spécifiquement les activités commerciales. Par exemple, le paragraphe 1.1 du AUP de JvNCnet indique que l'un des objectifs de ce système consiste à promouvoir et faciliter l'innovation ainsi que la compétitivité régionale et nationale. La politique de MIDNet précise expressément que le trafic circulant sur ce réseau n'a pas à se conformer aux AUP du NSFnet. De plus, les activités commerciales n'apparaissent pas sous la rubrique “unacceptable use”.

Malgré l'importance du NSFnet jusqu'au 30 avril 1995, on constate que la communauté de gens d'affaires de l'Internet ne comptait déjà plus uniquement sur ce dernier afin de faire circuler l'information. La mise sur pied du Commercial Internet Exchange (CIX)[112] laissait déjà entrevoir une plus grande liberté de commerce sur l'Internet. Cet organisme permettait au trafic commercial de circuler sur son réseau sans crainte de violer les règles du NSFnet. L'apparition de ce réseau à vocation commerciale laissait entrevoir une mutation au niveau de l'uniformité qui règne parmi les

---

[109] L'apparition de fournisseurs commerciaux d'accès constitue un élément essentiel de la croissance du commerce sur l'Internet. Voir Jill H. ELLSWORTH et Matthew V. ELLSWORTH, *Op. cit.,* note 52.

[110] *Id.*

[111] Voir à titre d'exemples : Michnet (réseau de l'état du michigan) AUP :

gopher://riceinfo.rice.edu:1170/00/More/Acceptable/nets/michnet.txt ;

JvNCnet (The John Neumann Computer Network) :

gopher://riceinfo.rice.edu:1170/00/More/Acceptable/nets/jvncnet.txt

[112] Voir http://www.cix.org/

Cette organisation est composée de fournisseurs d'accès désireux de permettre à tout type de traffic de circuler.

politiques de réseaux. L'une des fonctions de cet organisme consiste à fournir un forum neutre dans l'élaboration de politiques[113]. Il est également précisé qu'il n'existe aucune restriction quant au type de trafic pouvant circuler sur les réseaux membres[114] du CIX[115]. Considérant le territoire couvert[116] par ce réseau de réseaux, on ne peut douter de l'influence que des règles de conduite formulées par le CIX aurait sur la réglementation de l'espace cybernétique. Toutefois, pour l'instant la seule règle distincte des AUP académiques demeure la possibilité d'y faire du commerce.

Néanmoins, il nous semble que cet état de fait risque de se modifier au cours de la prochaine année. D'ailleurs, croyons-nous, la possibilité de faire des affaires en toute sécurité[117] jumelée à la disparition du NSFnet et de la clause de non commercialité de son AUP vont mener à une modification marquée du paysage réglementaire de ce type d'activité et du nombre de

---

[113]http://www.cix.org/about-cix.html

[114]Pour une liste de ces réseaux voir :

http://www.cix.org/members.html

[115]http://www.cix.org/about-cix.html

[116]Ce réseau couvre à peu de chose près la totalité de la planète. Voir la carte de ce réseau :

http://www.cix.org/Maps/CIXmap.html

[117]Un auteur mentionne que 1996 marquera le début de l'ère du commerce électronique en toute sécurité : *Commercial information-delivery services and other Internet sellers will rely on the secure online-transaction technologies that have been under development for the last two years. S-HTTP and SSL, the two secure transaction protocols developed by Terisa Systems and Netscape, respectively, are being adopted by vendors and becoming established as co-standards. Terisa's Secure Mosaic and Netscape's Navigator provide encrypted transaction capabilities within the two most popular browsers. RSA Data Security has spun off a company called VeriSign to handle the authentification of buyers. Netscape's new Navigator 2. 0 browser includes an e-mail program with built-in encrypted message capability, and Netscape is offering a Secure Courier application (with partners Mastercard and VeriSign) to handle transactions between buyers and sellers. Broadvision, Open Market, Tandem, and other venture also are selling secure transaction servers. And Internet EDI (electronic Data Interchange) systems such as Premendos' s Templar are making business-to-business transactions possible. E-cash systems are also appearing. With all these types of systems im place in 1996, the era of secure Internet commerce will be upon us..*

transactions commerciales effectuées dans les environnements électroniques.

À ce stade ci, une brève description de la nouvelle infrastructure américaine s'impose. Celle-ci peut être décrite comme suit :

> *In the United States, the backbones are fiber optic cables provided by long distance phone companies such as MCI and Sprint. There are four main Network Access Points (NAPs), in San Francisco, Chicago, New York, and the Washgington DC area, maintained by regional or long distance telephone companies. Also connecting at these NAPs are services to Europe (Ebone and EuropaNET), Asia and the rest of the world, the US government via the Federal Internet Exchange (FIX), and the experimental gigabit per second vBNS (very high speed Backbone Network Service). The government's NSFnet, once the main road of the Internet, has been shut down since April.*
>
> *The companies providing the network backbone form the lowest level of food chain of service providers. As network service providers (NSPs), they provide network capacity to regional network providers (RNPs) who in turn service the many Internet Service Providers (ISP) or Internet Access Providers (IAP) who provide connections for end users directly. RNPs may also directly service end users. CIX, the Commercial Internet Exchange, is a consortium of ISPS and private networks whose equipment also taps directly into the network access point.*[118]

Un bref historique de cette transformation s'impose[119]. Le coeur de l'Internet aux USA tire son origine de l'attribution de la gestion d'une

---

[118]Netsurfer Focus On Online Commerce : Part 1 The Business of The Net,

http://panoptic.csustan.edu/netsurf/nsoncom.htm

[119]Voir sur cette question : Herb BRODY, Internet@crossroads. $$$,

http://web.mit.edu/afs/athena/org/t/techreview/www/articles/may95/brody.html

entente de coopération en 1987 à Merit (Michigan) et ses partenaires : MCI et IBM. Cette entente avait pour objectif de fournir un “national backbone network service” ayant une capacité (“bandwidth”) de 1. 5 Mbit/sec. et plusieurs points d'accès[120]. Originellement ce système ne devait servir qu'à la recherche et l'enseignement. Toutefois, avec la popularité grandissante du système, certains virent là une excellente opportunité d'affaire. Des entrepreneurs, ayant acquis de l'expérience sur les réseaux régionaux, mirent sur pied de nouvelles entreprises à vocation commerciale. Les pionniers en la matière furent : Performance Systems International (PSI) et Alternet.

En 1991, le consortium Merit/IBM/MCI créa une corporation à but non lucratif appelé Advanced Networks Services (ANS). Cette entité devint alors responsable des opérations du NSFnet. Par la suite, ANS fonda ANS CO+RE (Commercial + Research & Education) afin d'offrir un service complet au trafic commercial. Dès le départ, la création de cette entité est apparue comme controversés en raison de l'importance du rôle du National Science Foundation (NSF) qui versait alors 10 millions[121] de dollars par année à ANS pour opérer le NSFnet. Toutefois, le rôle du NSF devint rapidement controversé :

> *The concept of NSF-sponsored research/educational-only traffic and commercial traffic running on the same wires was a difficult concept for many to accept and ANS was considered to have an unfair competitive advantage*

---

Dennis FAZIO*, Hang on to your packets : The Information Superhighway heads to Valleyfair or Building a high performance computer system without reading the instructions*,

ftp://montego.umcc.umich.edu/pub/users/seraphim/doc/nethist94.html

[120]Merit apportait son expertise en matière de gestion de réseau et de routing, IBM fournissait l'équipement nécessaire au "routing" alors que MCI fournissait l'infrastructure (trunk lines).

[121]Au moment de son retrait la contribution du NSF était de 20 millions de dollars US. Herb BRODY, Internet@crossroads. $$$,

http://web.mit.edu/afs/athena/org/t/techreview/www/articles/may95/brody.html

*over PSI, Alternet and now Sprint (who was also entering into the commercial backbone service).*[122]

Alors que l'entente de coopération tirait à sa fin le NSF ne pouvait que constater que sa commandite du NSFnet, autrefois considéré comme un instrument de développement de haute technologie et de recherche, était devenu un subside à un service aux réseaux commerciaux qui avec le temps s'étaient formés. Le NSF décida alors de passer à d'autres projets de recherche (Advanced network technology project) et de céder sa place à l'entreprise privée relativement au national backbone. Toutefois, le NSF avait des obligations envers la communauté des chercheurs et des enseignants. Il fut alors procédé à l'élaboration d'un plan de transition qui mena à la structure suivante :

**1. -** NAPs (Network Access Points)[123] : Le NSF proposa de commanditer un certain nombre de points d'échange où les "Network Service Providers" (NSPs) pourraient aiguiller le trafic et le faire transiter d'un réseau à un autre En Février 1994, le NSF désigna donc trois NAPs prioritaires :

New York NAP (Sprint)

Chicago NAP (Ameritech et Bellcore)

California NAP (Pacbell et Bellcore)

---

[122]Herb BRODY, Internet@crossroads. $$$,

http://web.mit.edu/afs/athena/org/t/techreview/www/articles/may95/brody.html

123Un NAP est système informatique haute performance. Selon Fazio (qui a déjà été impiqué dans le développement de tels systèmes), deux règles fondamentales doivent être suivies pour réussir à faire fonctionner efficacement de tels systèmes : 1. - Ne pas changer de technologie et d'architechture et 2. - Construire un prototype qui sera écarté plus tard. La moitié des opérateurs de NAPs violent ces règles. Des problèmes sont donc à prévoir. Des interruptions de services sont à prévoir soit au niveau régional ou au niveau national. Voir Dennis FAZIO, *Hang on to your packets : The Information Superhighway heads to Valleyfair or Building a high performance computer system without reading the instructions,*

ftp://montego.umcc.umich.edu/pub/users/seraphim/doc/nethist94.html

DC NAP (semi-officiel n'est pas considéré comme un NAP) (Metropolitan Fiber System)

**2. -** Routing arbiter

Équipe composée de Merit, Information Science Institute (ISI) et USC. ISI s'occupe de la gestion du "routing management" et Merit aide à mettre en place les "route servers" et les "route servers database".

**3. -** vBNS (very high speed Backbone Network service)

Collaboration entre MCI et NSF. Les cinq "Supercomputer centers" commandités par le NSF seront connectés entre eux et avec les NAPs grâce à ce réseau. Celui fonctionnera en 1995 à une capacité de 155 Mbit\sec, et à compter de 1996 à 622 Mbit/sec.[124]

4. - Inter-regional connectivity.

Plusieurs réseaux régionaux[125] ont été retenus afin d'assurer la relève du NSFnet et en retour ceux-ci ont sélectionné des NSPs afin de diriger leur trafic vers les NAPs et autres "backbones"[126].

Il n'y a donc plus un seul "national backbone". Le succès de cette nouvelle structure repose sur l'efficacité de la coopération entre les nombreuses compagnies de téléphone (régionales et de longues distances), les institutions de recherches académiques et commerciales, les fournisseurs d'équipements et les fournisseurs régionaux d'accès (regional network providers). La nouvelle infrastructure américaine ressemble donc à ceci :

---

[124]Originalement le NSFnet fonctionnait à une capacuté de 1. 5Mbit/sec.

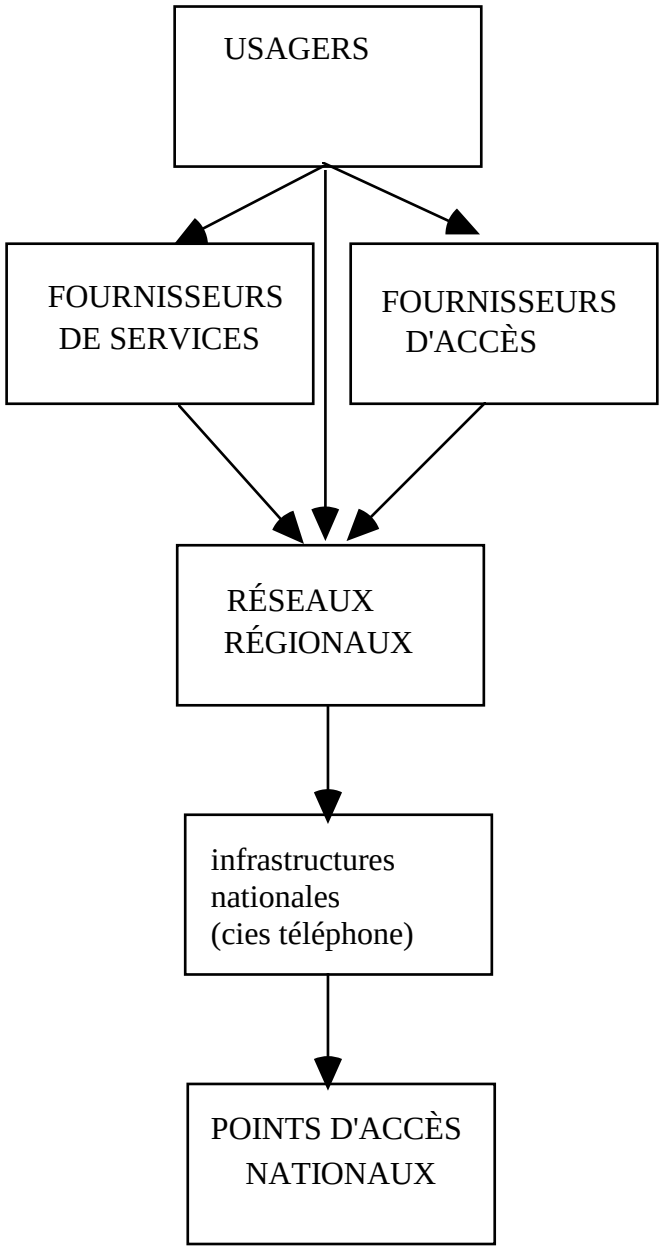
[125]Il s'agit de : BARRnet (maintenant BBN Planet), CERFNet, CICNet, IRC, JVNC, MICHNet, MIDNet, MORENet, MORENet 1, NC-REN, NevadaNet, NYSERNet, NYSERNet 2, PREPNet, SURANet, THENet, WestNet. Voir *Status of Regional/Midlevel Service Providers*,

http://www.ra.net/routing.arbiter/nsfnet/plans/regional.plans.html

[126]La plupart ont retenu les services de MCI (8) alors que d'autres ont opté pour Sprintlink et ANS. Voir Dennis FAZIO, *Hang on to your packets : The Information Superhighway heads to Valleyfair or Building a high performance computer system without reading the instructions.*

ftp://montego.umcc.umich.edu/pub/users/seraphim/doc/nethist94.html

*planet.be*


USAGERS
FOURNISSEURS DE SERVICES
FOURNISSEURS D'ACCÈS
RÉSEAUX RÉGIONAUX
infrastructures nationales (cies téléphone)
POINTS D'ACCÈS NATIONAUX

La disparition du NSFnet combinée à la nouvelle structure mise en place aura, à notre avis, un impact direct sur le commerce électronique. En effet, tel que mentionné précédemment, le AUP du NSFnet constituait la politique la plus restrictive qui soit. On y notait entre autres la présence d'une clause de non-commercialité très stricte. Or, vu l'importance de ce réseau, une part important du trafic devait transiter par lui, ce qui ne favorisait guère le développement des transactions commerciales entre parties se situant à chaque bout du continent. Comme chacun le sait, l'un des avantages de commercer dans les environnements électroniques réside notamment dans l'économie de temps et d'argent due à la disparition des barrières géographiques. Le fait que le trafic commercial ne puisse transiter par le NSFnet représentait, à notre avis, une entrave majeure au développement du commerce électronique. Or la disparition du NSFnet élimine cette contrainte. De plus, les AUP des réseaux régionaux n'imposent pas de restrictions relativement aux activités commerciales. Le CIX est également appelé à jouer un rôle de plus en plus important. Avec la mise en place de la nouvelle structure on remarque que le CIX est branché directement sur les NAPs[127]. Or, tel que mentionné précédemment ce réseau est à vocation commerciale.

## 45. Conclusion

Bien que les lignes qui précèdent ne représentent que le fruit d'une réfexion partielle et inachevée, force est de constater que la voie ouverte par une normativité, d'origine privée, mérite d'être explorée. Évidemment reste à s'interroger quant au rôle et à la place qu'occuperont les droits nationaux et les conventions internationales ou encore les lois modèles.

Néanmoins une chose semble claire : les droits nationaux ne peuvent appréhender à eux seuls l'ensemble des rapports qui se nouent dans l'espace cybernétique.

En terminant soulignons que nous avons dû passer sous silence, pour l'instant, l'influence que pourraient avoir les organisations privées sur la

---

[127] Netsurfer Focus On Online Commerce : Part 1 The Business of The Net : http://panoptic.csustan.edu/netsurf/nsoncom.htm

réglementation de l'espace cybernétique. Lorsque l'on sait l'importance du rôle joué par la Chambre de commerce internationale dans la compilation des usages du commerce international, on imagine bien le rôle que pourraient jouer ce type d'organisation dans la réglementation de l'espace cybernétique.

# La protection de la vie privée et des renseignements personnels dans l'espace cybernétique

**Martin MICHAUD**[1]

## 46. Introduction

La protection de la vie privée et des renseignements personnels est un sujet qui préoccupe de plus en plus les citoyens, en cette fin de siècle voyant l'Homme s'engager plus avant dans le développement d'outils technologiques de communication. L'espace cybernétique, terme générique qui réfère au concept *d'environnement électronique*, a notamment comme effet de favoriser un rapprochement entre les différents acteurs mondiaux, organisations politiques, gouvernements ou entreprises et, plus globalement, entre les peuples. Cette formidable capacité de transcender les frontières nationales des États amène les observateurs à constater que la planète rétrécit et que, bientôt, cette sphère habitable que nos ancêtres croyaient infinie, deviendra trop étroite pour la race humaine et sa soif de progrès. Surgit alors la question de savoir si l'on doit envisager pareil rétrécissement de l'espace vital de chaque être humain ? Dans une perspective plus pragmatique, il convient de se demander si l'émergence d'autoroutes électroniques présente certains dangers à l'égard de l'espace vital qui protège chaque personne à des degrés divers, en d'autres termes la vie privée ?

Le présent texte a précisément pour but de répondre à cette interrogation. Dans cette optique, la première partie présente les principales préoccupations que l'on peut observer à cet égard alors que la deuxième identifie les différentes situations risquant de donner lieu à une intrusion du

---

1 L'auteur est avocat et agent de recherche au Centre de recherche en droit public de l'Université de Montréal où il travaille au sein du Groupe de recherche sur le cadre juridique des environnements électroniques. Titulaire d'une maîtrise en droit de l'information et des communications, il est notamment l'auteur d'un livre à paraître prochainement aux Éditions Wilson & Lafleur intitulé : *Le droit au respect de la vie privée dans le contexte médiatique : de Warren et Brandeis à l'inforoute.*

cyberespace dans la vie privée. Avant d'entrer au coeur du sujet, le lecteur voudra bien noter que ce texte n'a pas la prétention d'apporter des réponses mais plutôt, au contraire, de poser des questions. En effet, il constitue simplement un état des problématiques relatives à la protection de la vie privée et des renseignements personnels dans les environnements électroniques. À ce titre, cet article s'inscrit dans la première phase d'un ensemble de travaux réalisés pour le gouvernement du Québec par un groupe de recherche du Centre de recherche en droit public de l'Université de Montréal sur l'adéquation du cadre juridique et réglementaire québécois aux environnements électroniques. Cette première étape avait pour but la description du cadre juridique et para-juridique du cyberespace tel qu'il se présente actuellement. Aussi, le lecteur voudra bien pardonner à l'auteur la lourdeur du style qui caractérise parfois certains paragraphes en tenant compte du fait que ce qu'il a sous les yeux n'est qu'un texte préliminaire qui fait partie d'une réflexion en cours et qui n'était pas destiné, initialement, à une publication.

## 47. Les préoccupations et menaces

Comme nous venons de le souligner, au plan de la protection de la vie privée, l'émergence des environnements électroniques ne se fait pas sans heurts. Aussi, nous allons tenter, dans les paragraphes suivants, d'identifier les principales sources de préoccupations et de menaces à la vie privée qui découlent de ces environnements.

### 47.1 Les préoccupations

Nous avons relevé deux préoccupations majeures qui semblent vouloir s'imposer comme ayant un impact important sur l'ensemble de la question relative à la protection du droit à la vie privée dans les environnements électroniques. Fait à noter, bien qu'elles semblent en voie de devenir incontournables, il n'en demeure pas moins que ces préoccupations ne sont pas réservées au phénomène électronique. En effet, ces préoccupations étaient déjà présentes, dans l'univers physique, au coeur des questions relatives à la protection de la vie privée. Peut-être, tout au plus, l'étaient-elles à un degré différent.

### 47.1.1 Le droit à la vie privée informationnelle

L'une des grandes préoccupations reliée à la protection de la vie privée dans les environnements électroniques a trait à la vie privée informationnelle, c'est-à-dire à l'intérêt des personnes à l'égard des informations qui les concernent ou qui sont divulguées[2]. Comme l'a fait ressortir Karim Benyekhlef, l'information relative à un individu ne constitue qu'une tranche de la sphère de la vie privée protégeant ce même individu[3]. Cette tranche touche plus directement la conservation et la dissémination de données personnelles informatisées[4]. La grande question à cet égard est sans doute celle de savoir si l'utilisateur de l'environnement électronique devrait se voir reconnaître, pour protéger adéquatement sa vie privée, un droit de contrôle sur l'information qui le concerne ?

#### *47.1.1.1 La revendication d'un droit de contrôle sur l'information*

La nécessité de protéger la vie privée dans les environnements électroniques paraît faire consensus. Qui pourrait, de toute façon, prétendre être fondamentalement contre la vie privée ? Là où les opinions risquent de diverger cependant, c'est sur le degré de protection qui doit être offert. Doit-on protéger la vie privée mur à mur ou y aller d'une approche plus circonspecte ? C'est précisément la question que l'on doit se poser à l'égard du droit de contrôle sur l'information.

---

2 Sur ce sujet, lire Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'information*, Montréal, Éditions Thémis, 1992, p. 49.

3 Ainsi, par exemple, l'écoute électronique, la surveillance par des moyens technologiques, les tests de dépistage de drogues touchent également à la vie privée. Voir BENYEKHLEF, *op. cit.*, note 1, p. 49.

4 *Id*.

Nous savons qu'à l'heure actuelle, un certain droit de contrôle sur l'information nous concernant est reconnu dans toutes les lois de protection des renseignements personnels[5], sous la forme du principe de la participation individuelle, en d'autres termes le droit d'accès. Comme le faisait remarquer Benyekhlef, *le droit du citoyen d'avoir accès aux informations le concernant constitue un des éléments les plus fondamentaux du dispositif général instauré par les lois de protection des données*[6] *[...] Ce droit d'accès n'est cependant pas absolu. De même, il obéit à une procédure et peut faire l'objet, la plupart du temps, de recours judiciaires*[7]. Ce droit d'accès répond à deux préoccupations :

> *La reconnaissance de ce droit présente un double intérêt : elle permet à l'individu de contrôler l'exactitude des données stockées sur son compte et, naturellement en cas de besoin, de les faire rectifier ; elle permet également, de faire participer l'ensemble des personnes fichées au contrôle du respect des règles posées par le législateur en matière d'informations nominatives*[8].

Anne Branscomb pose clairement la problématique en se demandant s'il existe, dans les environnements électroniques, un droit d'empêcher l'accès à notre information personnelle et de contrôler les termes des divulgations d'information nous concernant :

> *Autonomy means the right to exert some modicum of control over one's electronic environment. Efforts to devise some rules to preserve autonomiy must include consideration of several challenging questions. First, is there a right to prevent access to, or control the timing and terms of disclosure of information about oneself, one's corporation, or one's institutional entity ? Second, may certain cyberspaces be maintained as private spaces in wich the users themselves determine the governing rules ? Third,*

---

5 Voir à cet effet BENYEKHLEF, *op. cit.,* note 1, 140.

6 *Id*.

7 *Id*.

8 Cet extrait tiré du Bilan de la CNIL est cité dans BENYEKHLEF, *id.*

> *how can one ensure the confidentiality of messages posted to trusted colleagues ? Such issues of autonomy over communications present difficult challenges in cyberspaces.*
>
> *These questions are often clustered within the area of law called privacy. Privacy law is a fairly recent arrival on the horizon, but it too, derives at least some of its virtues from First Amendment principles. At a minimum, privacy can be translated into some sanctuary to which one may retreat -a personnal space and the ability to screen out unwanted or offensive messages. Although there may be a First Amendment right to speak, there is no comparable right to be heard. Furthermore, privacy must mean some degree of autonomy over personal information and how it is obtained and deployed by others, including governmental entities that may have a compelling interest in obtaining the information.*
>
> *Control over personal information may appear to be the flip side of freedom of speech, that is, the freedom not to speak. This freedom not to speak simply protects the right not to have information disclosed without consent or in a manner that may be contrary to one's interests*[9].

Plus loin, Branscomb conclut qu'il existe clairement une attente croissante du public à l'égard du degré de contrôle sur l'information personnelle et la confidentialité des transmissions :

> *There is a great deal of confusion about what privacy means, what information can be protected from disclosure, and whether unwanted messages may be prevented from intruding into private spaces. It is clear, however, that there is growing public demand for assurances that personal autonomy over private information will be respected and that personal transmissions will be modicum of sanctity of personal space should be guaranteed. What this space constitutes in a legal sense and how much control over it the*

---

[9]Voir Anne Wells BRANSCOMB, *Anonymity, Autonomy and Accountability : Challenges to the First Amendment in Cyberspace,* (1995) 104 *Yale L. J.* 1639, 1644.

*individual may exert has not yet been determined*[10].

Aussi, la question n'est pas tant de savoir si un droit de contrôle sur l'information personnelle doit exister dans les environnements électroniques. Cela semble en effet une nécessité. La vraie question sera de savoir, d'une part, quelle forme il devra prendre et, d'autre part, quelle importance devra-t-on y accorder ? Ainsi, il faudra considérer que garantir un droit de contrôle sur l'information personnelle par le biais du principe de participation individuelle pourra s'avérer problématique, certains pays, dont le Canada anglais, ne possédant pas de loi sur la protection des renseignements personnels dans le secteur privé. Il faudra également se demander si l'on veut accorder un contrôle plus grand que celui du droit d'accès. Dans l'affirmative il faudra se demander pourquoi, et surtout comment ?

Plusieurs de ces questions resteront probablement sans réponse à cette étape, ce qui semble normal puisque nous en sommes précisément à dresser un état des questions. Cependant, nous avons relevé certaines pistes qui méritent d'être mentionnées. Comme nous le verrons plus en détail au paragraphe I du chapitre I de la deuxième partie, un sondage récemment mené au États-Unis semble démontrer que les consommateurs désirent être informés à l'avance sur les profils de consommation, en particulier sur la manière dont ils seront utilisés. Également, les consommateurs estiment important qu'on permette à l'usager de réviser l'information contenue dans son profil et d'indiquer lui-même quel profil peut être utilisé pour la publicité. Commentant les résultats du sondage, les auteurs de celui-ci, dont Westin, émettent l'opinion que les fournisseurs de services devront adopter des règles répondant à ces préoccupations, s'ils désirent rallier une majorité d'usagers. Il leur apparaît évident que les consommateurs veulent connaître les règles du jeu et exercer un contrôle sur la façon de traiter l'information qui circule à leur sujet. Il deviendrait donc primordial de permettre au consommateur un “opting-out”, un contrôle sélectif, sur l'information qui le concerne.

---

[10] *Id.,* 1673.

Un autre type de solution, à caractère technologique, pourrait également être envisagé[11]. Il s'agirait de laisser au consommateur, par le biais d'un programme informatique de gestion, appelé agent mobile, le soin de révéler les informations qu'il juge à propos. Il n'est donc plus ici question de collecter des informations à tous vents et de bâtir un profil de consommation. C'est plutôt le consommateur qui exprime un besoin à son agent mobile, via un réseau électronique. L'avantage d'un tel système résiderait dans le fait que le consommateur détiendrait le contrôle de l'information, contrairement aux programmes conventionnels où le consommateur ne sait pas que des renseignements le touchant ont été collectés et, à plus forte raison, n'y a pas accès non plus que le contrôle. Plutôt que de voir leurs intérêts identifiés par d'autres, les consommateurs pourraient eux-mêmes exprimer positivement ceux-ci.

Anne Branscomb, dans un texte portant sur le premier amendement dans les environnements électroniques, soutient que l'anonymat, l'autonomie (le droit de contrôle d'une personne sur l'information qui la concerne) et l'imputabilité sont des valeurs inter-reliées qui entrent en conflit. La prédominance d'une de ces valeurs aurait donc des implications importantes pour les deux autres. Par exemple, un droit d'anonymat absolu pourrait empêcher l'imputabilité des usagers, tandis qu'une pleine responsabilité des usagers pourrait signifier la négation de leur droit à l'anonymat. Pareillement un droit de contrôle absolu sur l'information pourrait nier, en contrepartie, l'accès d'autres usagers à l'information[12]. Nous abordons justement la question de l'anonymat dans le prochain paragraphe.

### 47.1.2 L'anonymat

La deuxième préoccupation majeure se manifestant au sujet de la protection de la vie privée dans les environnements électroniques a trait à l'anonymat[13]. En termes clairs, la notion d'anonymat concerne l'intérêt des

---

[11]Voir le paragraphe A du chapitre I de la deuxième partie pour plus de précisions.

[12]Voir BRANSCOMB, *loc. cit.,* note 8, 1641.

[13]Voir de façon générale L. DETWEILER*, Identity, Privacy, and Anonymity on the Internet*,

http://www.cis.ohio-state.edu/hypertext/faq/usenet/net-privacy/part1/faq.html

personnes à communiquer sans être identifiées ou reliées au message en dehors de leur volonté. H. Patrick Glenn a déjà abordé cette notion d'anonymat en posant *que la prohibition de l'acte de diffusion de renseignements personnels protège l'anonymat de la personne, soit une situation où elle n'est pas identifiable*[14]. Alan Westin, pour sa part, avait apprécié le concept de “privacy” en fonction de quatre éléments personnels, dont l'anonymat[15]. Comme le souligne Anne Wells Branscomb, l'anonymat n'est pas une problématique inhérente aux environnements électroniques[16]. Cependant, dans les environnements électroniques, l'engouement pour l'anonymat semble exacerbé par l'émergence de moyens techniques permettant une protection de cette valeur, protection probablement supérieure à celle de l'univers physique. Il ne faut cependant pas oublier dans notre analyse du problème que l'émergence des nouvelles technologies de l'information laisse présager une activité plus intrusive pour la vie privée.

Par conséquent, dans les environnements électroniques, il convient principalement de se demander s'il faut admettre que la protection de la vie privée d'un individu comporte également la possibilité pour ce dernier de conserver un certain anonymat dans les gestes qu'il pose quotidiennement. Pourrait-on alors parler d'un droit à l'anonymat ? Serait-il sous-tendu dans le droit à la vie privée informationnelle ? Pour y voir plus clair, il faudra tenter de dégager l'étendue de cette notion. En effet, il n'est pas suffisant de dire que l'anonymat doit être protégé. Il faut savoir pourquoi et jusqu'où on entend le protéger. Cela implique donc que l'on doive se pencher sur les conflits qui pourraient opposer cette notion à des valeurs fondamentales comme le maintien de la loi et de l'ordre, la sécurité nationale, la liberté d'expression[17] et l'intégrité transactionnelle. Avant d'aller plus loin, il convient cependant de noter qu'il existe présentement, comme nous le verrons ci-après, deux principales façons de protéger l'anonymat dans les environnements électroniques, soit par le biais de serveurs anonymes ou de

---

[14]Voir H. Patrick GLENN, *Le secret de la vie privée en droit québécois*, (1974) 5 *R. G. D.* 24, 33 ; H. Patrick GLENN, *Le droit au respect de la vie privée*, (1979) 39 *R. du B.* 879, 881.

[15]Alan F. WESTIN, *Home Information Systems : The Privacy Debate*, *Datamation*, Juillet 1982, p. 106.

[16]Voir BRANSCOMB, *loc. cit.*, note 8, 1646.

[17]*Id.*, 1639.

l'encryptage.

#### *47.1.2.1 L'articulation technique de l'anonymat*

L'apparition d'échanges d'informations anonymes à grande échelle est un phénomène technologique relativement récent dans le réseau Internet. Lorsqu'un usager poste un message à un groupe de discussion, Usenet par exemple, cette opération est précédée d'un en-tête. Celui-ci contient l'information nécessaire à l'acheminement du message. Cet en-tête contient généralement le nom de l'usager, auteur du message, une indication relative à l'endroit d'où part le message ainsi que l'heure, la date et la nature de l'envoi[18]. En théorie donc, il est possible de relier un message à son auteur à l'aide de cet en-tête. En pratique cependant, le désir d'anonymat des usagers augmentant au même rythme que la croissance des groupes de discussion, les percées technologiques permettent maintenant à un usager de poster aisément des messages anonymes ou l'en-tête usuel sera remplacé par un numéro[19].

En contrepartie au développement de mécanismes technologiques permettant le postage anonyme, certains logiciels permettant d'éliminer les messages anonymes sont mis au point[20]. Pour l'instant, ces logiciels ne sont pas en mesure de distinguer les messages abusifs des messages légitimes, éliminant systématiquement tous les messages anonymes circulant sur le réseau. On peut facilement imaginer les conséquences de l'usage de tels logiciels par rapport à une valeur fondamentale comme la liberté d'expression. Aussi, pour Long, lorsque qu'un camp possède la capacité potentielle d'assurer un anonymat complet et qu'un autre est en mesure

---

[18]George P. LONG, *Who are You : Identity and Anonymity in Cyberspace* (1994) 55 *University of Pittsburgh Law Review* 1177, 1183.

[19]Pour des explications techniques plus poussées sur les mécanismes de postage de messages anonymes voir *id*., 1183, 1184 et 1185 et L. DETWEILER, *Identity, Privacy, and Anonymity on the Internet*,

http://www.cis.ohio-state.edu/hypertext/faq/usenet/net-privacy/part1/faq.html

[20]L'ARMM (Automatic Retroactive Minimal Moderation) en est un exemple. Voir *id*., 1186. Voir également Jonathan GILBERT, ity *Associated with Maintaining a Computer Bulletin Board* (Oct. 1990) 4 *Software Law Journal* 147, 148 ; Jonathan GILBERT, *Computer Bulletin Board Operator Liability for User Misuse*, (1985) 54 *Fordham Law Review* 439, 449.

d'éliminer totalement cet anonymat, le juriste doit tenter de trouver un équilibre entre le droit à la vie privée et la prolifération des activités criminelles[21].

Pour Frookmin, la facilité d'accès aux communications anonymes est l'un des premiers effets de la révolution des technologies de l'information. En effet, examinant les questions reliées à l'anonymat sous l'angle du droit américain, Frookmin note qu'il est aisé de communiquer anonymement sur le réseau Internet, pour tout ce qui a trait aux transactions interpersonnelles. Cette facilité d'accès à l'anonymat permettrait notamment aux usagers d'exprimer leurs vues politiques sans crainte de représailles, à certains autres, agissant à titre d'informateurs d'éviter d'être découverts et, enfin, à d'autres encore, de discuter de problèmes personnels embarrassants sans peur d'être identifiés[22]**.** Aussi, Froomkin identifie quatre types de communications qui garantissent, à des degrés différents, l'anonymat des utilisateurs d'Internet, soit l'anonymat identifiable, l'anonymat non-identifiable, le pseudo-anonymat non-identifiable et le pseudo-anonymat identifiable. Il analyse chacune de ces quatre composante séparément[23].

Un serveur anonyme ne donnant au destinataire d'un message aucun indice quant à l'identité de son auteur, mais qui laisse cette information entre les mains d'un tiers unique, peut être considéré comme un système de postage anonyme identifiable. En effet, le destinataire du message pourrait identifier l'auteur de celui-ci en convainquant le tiers ayant anonymisé le message de l'auteur de lui révéler l'identité de ce dernier. Cette information, si elle n'a pas été effacée, pourrait également être obtenue par le destinataire du message, via un subpoena délivré par un juge possédant les pouvoirs de le faire. Comme le souligne Froomkin, cette façon d'anonymiser les messages, qui offre une plus faible protection de l'anonymat que les trois autres, est souvent largement suffisante, quoiqu'elle implique une certaine

---

21 *Id.,* 1187.

22 A. Michael FROOMKIN, *Anonymity and its Enmities*, (1995) *J. Online L.,* art. 4, par. 2 et 7, disponible à :

http://www.law.cornell.edu/jol/froomkin.htm

23 *Id.,* par. 11. Voir également, sur l'anonymat et le pseudo-anonymat comme moyen de garantir l'intégrité transactionnelle, le paragraphe B du chapitre I de la deuxième partie.

dose de confiance envers l'opérateur du système anonymisant qui pourrait copier, lire ou révéler le message aux autorités compétentes[24].

Lorsque Frookmin parle d'anonymat non-identifiable, il fait référence à une communication dont l'auteur ne peut être, en principe, d'aucune façon identifié. La technologie présentement utilisée sur le réseau Internet permet, via l'envoi du message à travers une chaîne de serveurs anonymes, ce type de communications[25]. Sommairement, cette technique consiste à encrypter le message en différentes couches à l'aide de la clé publique du destinataire, chacune contenant l'adresse du destinataire suivant et ne pouvant être déchiffré par lui qu' à l'aide de sa clé privée. Le message est ensuite expédié à un premier serveur anonyme. Celui-ci anonymise la communication, décode la partie du message qui lui est destiné, c'est-à-dire l'adresse du prochain destinataire, et lui expédie. Cet autre serveur, lorsqu'il reçoit la communication, efface également l'en-tête permettant l'identification et décode la partie de la communication qui lui est destinée, c'est-à-dire l'adresse du prochain destinataire. Il réexpédie ensuite le message et la chaîne se poursuit. Aucun des intermédiaires de la chaîne ne pouvant décoder plus que la partie du message qui a été encrypté à son attention, le corps du message parvient finalement à son véritable destinataire qui peut le décoder à l'aide de sa clé privée. Frookmin constate que cette technologie ouvre la porte à des comportements illicites tels la conspiration, la diffamation et la propagande haineuse en ce qu'elle diminue considérablement les risques d'être pris. Cela lui fait affirmer que les gouvernements qui voudront permettre à leurs citoyens de prendre part aux échanges sur le réseau mondial seront forcés de vivre avec une liberté d'expression encore plus grande[26].

Froomkin aborde ensuite la question du pseudo-anonymat, qu'il définit comme le fait, pour un usager, d'utiliser un pseudonyme dans ses relations et ses transactions avec les autres usagers. La pseudo-anonymité permettrait notamment aux personnes désirant participer à un débat avec d'autres usagers d'une liste de le faire sous une identité constante, sans pour autant dévoiler leur véritable identité. De la même façon que l'anonymat, cette

---

[24]Voir FROOMKIN, *loc. cit.,* note 21, par. 14 et suiv.

[25]Voir aussi BRANSCOMB, *loc. cit.,* note 8, 1643.

[26]Voir FROOMKIN, *loc. cit.,* note 21, par. 19 et suiv.

pseudo-anonymité peut être soit non-identifiable, ou identifiable[27]. Une personne utilisant un pseudonyme non-identifiable sur l'Internet pourrait fort bien en arriver à créer une personnalité électronique distincte de sa personne[28], avec une réputation et une image. L'encodage et l'utilisation de la signature électronique peuvent même servir à assurer l'intégrité de cette pseudo-personne en ce qu'ils permettent de s'assurer que personne d'autre n'enverra de messages au nom de cette dernière. Dans le cas d'un pseudonyme identifiable, il est possible d'en arriver ultimement à connaître la véritable identité de l'auteur d'une communication. Cette option a cependant l'avantage de permettre au récepteur de la communication d'y donner suite directement, en postant sa réponse dans le courrier électronique de la pseudo-personne. Cela n'implique pas pour autant qu'il connaisse la véritable identité de l'auteur. En effet, les messages continueront de transiter par un serveur qui les anonymisera, en effaçant l'en-tête. Ce serveur, qui conserve un relevé de la véritable identité de chaque usager pourrait cependant être obligé de la divulguer, suivant un ordre de cour par exemple. D'où le caractère identifiable de ce type de pseudo-anonymat[29].

Froomkin fait également état de l'émergence, l'encryptage aidant, d'argent électronique, aussi appelé “ecash”. Cet argent électronique permettrait aux utilisateurs du réseau Internet d'acheter ou de vendre des biens ou des services sans qu'un relevé de leurs transactions ne puisse être tenu par un commerçant ou une banque. En vertu de cette technique, un utilisateur pourrait acquérir d'une banque de l'argent électronique qui lui permette d'effectuer des transactions sans avoir à révéler son identité aux personnes avec qui il effectuera ces transactions. Un mécanisme de protection technologique ferait en sorte que l'utilisateur ne puisse copier son argent et ainsi le dépenser plusieurs fois. En vertu d'une autre application, quiconque tenterait de dépenser cet argent plus d'une fois pourrait même risquer de voir son identité révélée[30]. Selon Froomkin, l'utilisation d'argent

---

[27]*Id.,* par. 31 et 32.

[28]Voir au même effet KARNOW, C. A., *The Encrypted Self : Fleshing Out the Rights of Electronic Personnalities*, (1994) 8 *Journal of Computer & Information Law* 1 et suiv.

[29]Voir FROOMKIN, *loc. cit.,* note 21, par. 33 et suiv.

[30]Pour un texte détaillé sur la notion de "ecash" voir David CHAUM*, Achieving Electronic Privacy*, SCIAM., (Aug. 1992), disponible sur Internet à l'adresse suivante :

électronique permettrait d'éviter la multiplication de fichiers établissant des profils de consommation. Il prétend, en outre, que si un utilisateur pouvait payer par le biais de sa personnalité électronique, avec de l'argent électronique, ce dernier pourrait être en meilleure position pour marchander, du fait que ses habitudes de consommation demeurent inconnues[31].

Pour sa part, Curtis Karnow a poussé son raisonnement sur l'anonymat jusqu'aux confins de la réalité virtuelle. Posant que la communauté électronique est aux prises avec un conflit entre un besoin de libre circulation de l'information et un désir de protection de la vie privée, en d'autres termes avec le libre accès d'une part et le droit de contrôle sur l'information d'autre part, il estime que les développements extraordinaires des technologies de l'information ont donné naissance à une nouvelle entité juridique dans la communauté électronique, soit la personnalité électronique, plus communément appelée “eper”, diminutif de “electronic person”. En prenant part directement aux échanges dans la réalité virtuelle, on noue, involontairement ou indirectement, des relations électroniques avec des banques, des vendeurs, des compagnies d'assurances, des agences gouvernementales, par le biais d'une participation incorporelle. Pour Karnow, il n'existe aucune contrainte dans la réalité virtuelle, pas de temps, pas d'espace, pas de lois physiques. Il y a donc risque d'attaques émotionnelles à la sensibilité des humains. Pour cette raison, il y aurait lieu de limiter notre

---

http://www.digicash.com/publish/sciam.html

Voir également David CHAUM, *Electronic Cash : What it is and What it Means ?*, présenté dans le cadre du *Fifth Conference on Computers, Freedom and Privacy*, June-July 1994, disponible à l'adresse :

http://www-techlaw.stanford.edu/CFP95.Program.html

Par ailleurs, nous avons appris, par le biais d'un liste de discussion sur Internet, qu'une entreprise offrant un service d'argent électronique fait présentement face à des poursuites légales. En effet, il semble que la compagnie Mondex, qui a lancé en décembre une carte électronique "aussi facile à utiliser et aussi anonyme que de l'argent comptant", soit accusée de faire de fausses représentations au public en promettant un service anonyme qu'elle n'est pas en mesure d'assurer. Pour sa part, Mondex soutient n'avoir jamais promis l'anonymat à ses utilisateurs. Voir à cet égard la liste de discussion Data-Protection du 25 octobre 1995, sur le serveur data-protection@mailbase. ac. uk.

[31] Voir FROOMKIN, *loc. cit.*, note 21, par. 41 et suiv.

exposition et notre responsabilité à ces phénomènes. Pour Karnow, ce qui porte véritablement atteinte à la vie privée d'une personne, c'est la mise en commun de l'information la concernant[32]. En soi, le fait qu'un bibliothécaire puisse avoir accès à mon numéro de téléphone importe peu, mais il y a une marge à ce que ce même bibliothécaire connaisse aussi l'état de mes finances[33].

Aussi, l'information circulant à la vitesse de la lumière et pouvant être facilement mise en commun, il y a lieu d'adopter, nous dit Karnow, une théorie cohérente permettant de limiter l'accès à l'information. Pour ce faire, plutôt que d'éliminer l'information ou les interactions disponibles, il suggère l'idée d'un compartimentage de l'intimité d'une personne physique en plusieurs personnalités électroniques. Ces personnalités électroniques seraient munies de responsabilités ainsi que droits exécutoires, dont un droit à la vie privée, qui permettraient de protéger la personnalité humaine. Ainsi, plusieurs personnalités électroniques reliées à une personne humaine et conduisant ses affaires dans le cyberespace pourraient lui fournir l'anonymat nécessaire. Pour assurer un degré de sécurité maximal, le lien entre la personne humaine et sa personnalité électronique n'aurait qu'à être encrypté[34]. En bref, il y aurait un réel besoin de se dissimuler, selon le temps, les lieux ou certains contextes. Voilà donc précisément, nous dit Karnow, la véritable fonction d'une personnalité. Il ne saurait y avoir de vie privée sans un bouclier ou un masque. Dans le monde réel, les personnes ont le choix entre des communications privées ou publiques. Il y a lieu d'établir les mêmes limites dans le cyberespace.

---

[32]Reidenberg écrit à ce sujet : *Digital communications leave traces and portraits of every interaction with the network, and these traces may be put to a variety of unwanted secondary uses. [...] Because of easy access to multiple sources of data and because there are few existing legal restrictions on the use of information, secondary use of collected information is significant. Personal information is often collected in one context for a particular purpose and used in another context for a different purpose.* Lire Joel REIDENBERG and Françoise GAMET-POL, *The Fundamental Role of Privacy and Confidence in the Network*, (1995) 30 *Wake Forest Law Review* 105, 106 et 112.

[33]VOIR KARNOW, *loc. cit.*, note 27.

[34]*Id.*

#### *47.1.2.2 L'étendue du droit à l'anonymat*

Dans une perspective plus pragmatique, après avoir abordé brièvement la question de l'articulation, au plan technique, de la notion d'anonymat, il convient maintenant de tenter de cerner son étendue. Historiquement, nous dit Long, la loi a reconnu un besoin d'anonymat dans plusieurs domaines. Récemment, la protection de l'identité d'un individu a servi de justification, aux États-Unis, à la remise en question du service d'affichage automatique du nom de l'appelant. Également, cette protection s'est traduite, dans plusieurs cas, par la reconnaissance d'un droit à la vie privée informationnelle. La Cour suprême des États-Unis a, en outre, confirmé l'existence d'un droit à l'anonymat, dans certaines situations où la divulgation de l'identité pourrait embarrasser ou stigmatiser une personne. Enfin, Long précise que l'anonymat a été maintenu dans certains cas où des immunités étaient en cause, notamment celles protégeant les sources journalistiques et les informateurs du gouvernement[35].

Aussi, Long tente de solutionner, à l'aide de ces précédents, la question de l'anonymat dans les environnements électroniques. Il examine d'abord le contentieux relié au service d'affichage automatique[36]. Dans un premier temps, il identifie les arguments des protagonistes en présence. D'une part, certains prétendent que l'afficheur est un mécanisme permettant d'assurer aux usagers des services téléphoniques une plus grande sécurité en ce qu'il permet d'identifier les appels obscènes ou harcelants. D'autre part, leurs opposants objectent que cette technologie porte atteinte à la vie privée et aurait comme effet de décourager les personnes qui veulent utiliser un service anonyme, tel les lignes de prévention du suicide, les lignes d'information sur la toxicomanie, etc. [37]. Un tribunal administratif

---

[35]George P. LONG, *loc. cit.*, note 17, 1183.

[36]Voir également sur cette question , Matthew J. RINALDO, *Caller ID and Fair Credit Reporting : Technology and Traditional Notions of Privacy Clash (includes Draft Amendments to the Fair Credit Reporting Act) (Reflections from the House & Senate)* (Juillet 1992) *16 Seton Hall Legislative Journal* 403-453 et Consuelo Lauda KERTZ, and Lisa Boardman BURNETTE, *Telemarketing tug-of-war : Balancing Telephone Information Technology and the First Amendment with Consumer Protection and Privacy* (1992) 43 *Syracuse Law review* 1029-1072 ; Laurie Lee THOMAS, *U. S. Telecommunications Privacy policy and Caller ID*, (Fall 1993) 30 *California Western Law Review* 1-60.

[37] Voir LONG, *loc. cit.*, note 17, 1188.

américain, saisi d'une contestation du service d'afficheur, a statué qu'un tel service n'est pas dans l'intérêt public, à moins qu'une commande de blocage gratuite ne soit mise à la disposition des consommateurs[38].

Pour Long, il est possible de tracer un parallèle entre le cas du service d'afficheur et le débat entourant l'anonymat sur l'Internet. Ainsi, comme dans le cas de l'afficheur, divulguer l'identité d'un utilisateur d'un groupe de discussion menace l'intimité de la personne voulant demeurer anonyme pour différentes raisons. En effet, de la même façon que dans les environnements physiques, une personne peut vouloir contacter anonymement un service de prévention du suicide par le biais d'un tel groupe, sans vouloir pour autant être identifiée. Il en va de même dans le cas des divers informateurs. Si l'anonymat est prohibé, la divulgation d'informations importantes pourrait être compromise. En effet, pour certaines personnes, l'utilisation d'Internet en milieu de travail constituera peut-être le seul moyen sécuritaire de dénoncer certaines activités illégales de leur employeur. Dans ces cas, prohiber l'anonymat aurait assurément un effet négatif sur les dénonciations potentielles[39].

L'on se penche ensuite sur l'étude de la reconnaissance, par les tribunaux américains, d'un droit à la vie privée informationnelle, en d'autres termes l'intérêt d'un individu à éviter la divulgation d'informations personnelles. Il fait d'abord état du test d'équilibrage dégagé par la Cour suprême américaine dans les affaires *Whalen* et *Nixon*, soulignant que ce sont les cours inférieures qui en ont fixé les limites. Il présente ainsi les critères retenus par ces tribunaux pour ce faire. Premièrement, dans quelle mesure risque-t-on, par la divulgation de l'information en cause, d'embarrasser la personne ou de porter atteinte à sa réputation ? Deuxièmement, la divulgation mènera-t-elle à une intrusion ou au harcèlement ? Troisièmement, l'individu avait-il une attente de vie privée raisonnable ?

---

[38] *Id.*

[39] *Id.*, 1189.

À partir de ces critères, il trace un parallèle avec la protection de l'anonymat sur l'Internet. Reprenant les exemples des personnes désirant discuter des agression sexuelles dont elles ont été victimes ou de l'état de la progression du virus du SIDA chez elles, il démontre que, dans les environnements électroniques, la divulgation de l'identité de ces personnes risquerait grandement de mener à une intrusion ou à du harcèlement. Il démontre également qu'il est probable que cette divulgation embarrasse fortement la personne en cause et même entache sa réputation. Enfin, il prétend que les utilisateurs de services de discussion ont une attente légitime de vie privée, les services anonymes étant en très grande demande et la technologie étant suffisamment développée pour permettre la sauvegarde de l'identité des utilisateurs. Il en conclut donc que, quelle que soit l'approche retenue par les tribunaux, il y a de fortes chances que l'anonymat des participants aux groupes de discussion soit reconnu comme étant protégé par la vie privée informationnelle[40].

Qui plus est, les tribunaux ayant reconnu à différentes reprises, dans l'univers physique, une protection constitutionnelle à l'anonymat ainsi que la nécessité d'assurer cette protection, Long soutient que l'on devrait protéger cette valeur dans les groupes de discussion, quoique sur une base limitée. Pour ce faire, il suggère l'adoption de contrats garantissant 'anonymat[41]. Constatant que ce sont les gestionnaires de réseaux désirant offrir l'anonymat à leurs usagers qui seront touchés par la légalité d'une telle démarche, il suggère que la meilleure façon de procéder serait d'encourager la formation d'accords contractuels entre eux. De cette façon, le gestionnaire de réseau pourrait proposer à l'usager certaines règles et politiques de fonctionnement à l'intérieur d'un site. L'usager s'engagerait alors à suivre ces directives, sous peine de perdre son droit à l'anonymat. Un gestionnaire de réseau pourrait également choisir de permettre ou non l'utilisation des messages anonymes dans son site. De plus, même si un gestionnaire de réseau décidait de permettre les messages anonymes, il pourrait créer autant

---

[40] *Id.*, 1192 et 1193.

[41] Comme nous le verrons au fur et à mesure de nos développements, l'approche contractuelle est une des solutions prônée en doctrine par les auteurs afin de résoudre les conflits émergeant dans le cyberespace. Dans le présent texte, nous ferons état, notamment au paragraphe II du chapitre II de la deuxième partie, des principaux textes de doctrine contribuant à cerner l'état des questions relatives à la protection de la vie privée, par le biais des contrats, dans les environnements électroniques.

de restrictions à leur usage qu'il l'entend. Ainsi, un serveur pourrait restreindre l'utilisation de l'anonymat à certains groupes présélectionnés par l'administrateur du site. Les utilisateurs prendraient connaissance et accepteraient ces restrictions lors de la formation du contrat avec l'administrateur[42].

Cette solution aurait au moins deux avantages majeurs, nous dit Long. D'une part, cela empêcherait l'administrateur du site, qui n'est pas nécessairement un juriste, d'avoir à déterminer si tel envoi est légal ou non. D'autre part, le statut de l'anonymat serait fonction de la loi du marché. En effet, les contrats refléteront la perception du public à l'égard de l'importance à attacher à l'anonymat. Par exemple, si les usagers des services “Usenet” croient que l'anonymat devrait être fortement réglementé ou même restreint à certains groupes, les serveurs offrant des standards plus relâchés seront appelés à disparaître. Lorsqu'un groupe de discussion serait créé, les utilisateurs pourraient très bien décider eux-mêmes de bannir l'anonymat. Il existe d'ailleurs des groupes “modérés”, où une personne reçoit tous les messages et décide lesquels poster. Le fait de bannir l'anonymat d'un groupe de discussion pourrait alors être assimilé, selon Long, à une extension de cette activité modératrice[43]. Aussi, même si un groupe décidait de ne pas se doter d'une instance de modération organisée, il est d'avis que la structure des groupes de discussion favoriserait une régulation démocratique.

En effet, Long identifie deux types de mécanismes auto-régulatoires déjà existants dans les groupes de discussion : le “flaming” et le “killing”. Ainsi, certains usagers en désaccord avec les idées d'autres usagers ou avec certains sujets, peuvent tout simplement placer ces items dans un fichier “kill”. Ce fichier, dès lors qu'il recevra un message sur tel sujet ou de tel auteur indésiré, le détruira sans que l'usager en reçoive jamais copie. La technique du “flaming” est aussi utilisée par les usagers des réseaux. Elle consiste à inonder le courrier électronique de l'auteur d'une opinion impopulaire de virulentes critiques. Plus une opinion est impopulaire et minoritaire, moins elle recevra de support. Cette technique est d'ailleurs devenu un art sur l'Internet, certains groupes s'y appliquant exclusivement.

---

[42]Voir LONG, *loc. cit.,* note 17, 1200 et 1201.

[43]*Id.,* 1201 et 1202.

Pour Long, cette technique est efficace dans plusieurs cas[44].

Selon lui, l'existence de ces deux instruments milite assurément en faveur d'une forte protection de l'anonymat. En effet, si un serveur offre une réglementation et des restrictions minimales favorisant l'anonymat et que cette position est contraire à celle de la majorité, l'administrateur du réseau risque de se voir “flamer” allègrement. Plus fondamentalement encore, plusieurs utilisateurs légitimes pourraient être dissuadés d'utiliser un tel serveur, par peur de contribuer à un abus d'anonymat qui pourrait mettre en péril la préservation de l'anonymat en général. De plus, des logiciels tels l'ARMM pourraient être utilisés contre un tel serveur, éliminant tous les messages anonymes ou encore plusieurs usagers pourraient tout simplement “tuer” certains messages. En contrepartie, si la majorité des utilisateurs des groupes de discussion désirent peu de restrictions à l'anonymat, un tel serveur sera supporté et les utilisateurs de logiciels tels l'ARMM, qui oseront l'utiliser, deviendront alors l'objet d'un “flaming” intensif. Dans les deux cas, le groupe continuera de fonctionner de façon démocratique, les usagers décidant des meilleurs choix à faire pour la sauvegarde de leurs droits. En ce sens, l'anonymat sera disponible pour les groupes de discussion tant qu'il existera un besoin à cet égard[45].

Branscomb, pour sa part, pose que le défi consiste à distinguer les formes désirables d'anonymat des formes indésirables et d'étendre la prohibition le plus précisément possible. Pour elle, il est possible que des pédophiles tentent d'utiliser l'anonymat pour solliciter la compagnie de jeunes usagers du réseau. Elle croit cependant que, plutôt que d'interdire l'utilisation de pseudonymes, une meilleure façon d'aborder le problème serait de poster des messages mettant les enfants en garde contre les dangers de rencontrer un ami électronique dans la réalité. Pour elle, il est essentiel de déterminer à quel endroit sur le continuum de l'anonymat, la censure doit tomber. Pour ce faire, il est plus facile d'évaluer les usages que font les utilisateurs de l'anonymat à leurs extrêmes. Les usages destructifs et dangereux de l'anonymat sont relativement faciles à identifier. La question devient plus difficile lorsqu'on approche du centre du continuum, où l'anonymat peut constituer un problème sans être totalement inacceptable.

---

[44] *Id.*

[45] *Id.*, 1202, 1203 et 1204.

Ces questions constituent un défi pour chaque communauté cybernétique, qui devra imaginer des règles et des standards pour appréhender l'anonymat dans son voisinage électronique[46]. Cependant, l'anonymat ne doit pas être perçu comme un absolu. En effet, bien que l'anonymat soit justifiable à certains degrés, il ne devrait pas pour autant remettre en cause l'existence d'un équilibre entre cette valeur et l'imputabilité des usagers à l'égard des actes répréhensibles qu'ils posent. Selon Branscomb, il ne saurait y avoir de solution générale. On devra mesurer l'utilité de l'anonymat en fonction des circonstances, tout en faisant confiance au potentiel auto-régulatoire déjà présent dans les réseaux. Aussi, elle souligne que, peu importe l'approche primée, il sera toutefois très difficile de faire accepter aux usagers de l'Internet l'idée d'abandonner le droit de contrôle sur l'information qu'ils ont gagné en utilisant l'anonymat[47].

Pour Froomkin, l'anonymat dans les réseaux électroniques est une réponse rationnelle à un monde où la quantité d'information personnelle prélevée sur chacun de nous augmente sans cesse tout en étant plus accessible pour les autres. Il reconnaît cependant que tous ne partagent pas son avis. En effet, le juge Scalia, dans la récente décision de la Cour suprême des États-Unis sur l'anonymat dans le cadre du discours politique écrivait à propos de cette notion : *It facilitates wrong by eliminating accountability, which is ordinarly the very purpose of the anonymity[48]". Cependant, l'inhabileté d'assurer un remède approprié aux gens ayant des motifs légitimes de demander réparation, suite à une utilisation inappropriée des secrets gardés, demeure, pour Froomkin, l'objection morale la plus forte à l'encontre de l'anonymat*[49].

Aussi, il nous semble cerner un peu plus cette notion lorsqu'il pose que,

---

46 BRANSCOMB, *loc. cit.*, note 8, 1665.

47 *Id.*, 1675. En 1985, Johnathan Gilbert estimait qu'un des moyens les plus efficaces, pour l'opérateur de babillard électronique, d'éviter toute responsabilité, passait par le contrôle systématique de l'identité de chaque usager. Voir à cet effet GILBERT, *loc. cit.*, note 19, 446. Force est de constater que les usages ont depuis évolué de façon telle qu'il serait illusoire, aujourd'hui, d'envisager l'application d'une telle solution.

48 *McIntyre* v. *Ohio Elections Commission*, 63 U. S. L. W. 4279 (U. S. April 18, 1995), cité dans le texte de Froomkin.

49 A. Michael FROOMKIN, *loc. cit.*, note 21, par. 50 et suiv.

si la Constitution des États-Unis ne garantit pas comme tel un droit à l'anonymat, le premier amendement a été considéré en plusieurs cas comme lui offrant une protection constitutionnelle. Par exemple, dans l'arrêt *McIntyre*, la Cour suprême a jugé que la décision d'un auteur de demeurer anonyme, comme certaines omissions ou additions au corps du texte, est un aspect de la liberté d'expression protégé par le premier amendement et que l'anonymat de l'auteur n'est pas en soi un motif suffisant pour exclure son travail de la protection constitutionnelle[50]. Frookmin ajoute cependant que si de larges prohibitions de l'expression anonyme ont été jugées contraires au premier amendement, le droit à la vie privée d'une personne à l'égard de ses opinions politiques peut être contourné lorsque l'État possède un intérêt suffisant. Dans l'arrêt *McIntyre*, l'intérêt de l'État à prévenir les propos diffamatoires et frauduleux ainsi que son intérêt à fournir à l'électorat une information éclairée, ont été jugés comme étant des motifs insuffisants pour justifier une interdiction du discours anonyme.

Il est toutefois important de noter, comme le souligne Froomkin, que cette décision concerne le discours politique. Il faudrait donc se garder de tirer de trop grandes conclusions à l'égard du discours anonyme qui n'est pas relié au discours politique. Tout au plus, l'affaire *McIntyre* peut-elle donner une idée de ce qui pourrait survenir. Froomkin insiste également sur le fait que cet arrêt implique une loi d'application générale interdisant l'anonymat. Une loi mieux ciblée pourrait peut-être être considérée comme ne portant pas atteinte à l'anonymat. En effet, il semble logique de croire que la Cour suprême, à la lumière de ses décisions antérieures, maintiendrait une loi rédigée avec rigueur et interdisant l'anonymat, même dans le contexte du discours politique pourtant considéré comme une chasse gardée[51]. Aussi, Froomkin considère qu'il serait trop facile de croire, à la lumière de l'arrêt *McIntyre*, que l'anonymat triomphera assurément dans le cyberespace. En effet, si on considère que même le discours politique anonyme, qui semble le mieux protégé, n'est pas à l'abri d'une loi bien ciblée, les autres types de discours anonymes risquent d'être soumis à d'encore plus grands contrôles[52].

---

[50] *Id.,* par. 56.

[51] *Id.,* par. 57 et suiv.

[52] *Id.,* par. 68 et 69.

#### *47.1.2.3 La double facette de la notion d'anonymat*

On ne peut tenter de cerner l'étendue du droit à l'anonymat sans aborder la question des conflits qui existent, dans les environnements électroniques entre cette notion et d'autres valeurs considérées comme fondamentales par notre société. Aussi, il faut bien comprendre que la notion d'anonymat recèle deux facettes. En effet, d'un côté elle peut être envisagée comme un instrument permettant de mieux protéger la vie privée des utilisateurs du réseau. Il ne faut cependant pas oublier que cette même notion peut également permettre à certains individus de commettre des gestes illicites, sans crainte d'être pris. De cette seconde hypothèse découlent des conflits potentiels, principalement entre l'anonymat et le maintien de la loi et de l'ordre, entre l'anonymat et la liberté d'expression ainsi qu'entre l'anonymat et l'intégrité transactionnelle.

La meilleure preuve de la véracité de cette affirmation réside dans les vigoureux débats qui opposent les usagers des différents groupes de discussion sur Internet[53]. Comme le fait remarquer Long, certains prétendent que le droit à l'anonymat est essentiel dans les cas où la divulgation de l'identité d'une personne pourrait être embarrassante ou lorsque qu'elle exposerait un utilisateur au ridicule ou au harcèlement. D'autres rétorquent que l'anonymat permettra à certains utilisateurs de se cacher derrière un code ce qui aura pour effet de les déresponsabiliser[54]. L'anonymat risquerait donc d'encourager la circulation de messages illégaux ou abusifs sur le réseau[55].

Il n'est certes pas facile d'arbitrer un tel conflit. Comme le soulignent Long et Branscomb, il y a autant de raisons valables de protéger l'anonymat qu'il en existe d'autres, en contrepartie, pour ne pas le protéger. Pour Branscomb, la possibilité d'un anonymat véritable implique tant une valeur positive, celle de permettre la protection des sources de certaines informations, qu'une valeur négative comportant un danger inhérent, celle de permettre aux individus de s'exprimer sans peur d'être détectés ou tenus

---

[53]Voir à cet effet BRANSCOMB, *loc. cit.,* note 8, 1659 et suiv. où elle relate les débats enflammés opposant deux personnes ayant mis au point un serveur anonyme, Johan Helsingius et Karl Kleinpaste.

[54]Voir au même effet BRANSCOMB, *loc. cit.,* note 8, 1645.

[55]Voir LONG, *loc. cit.,* note 21, 1183.

responsables de leurs propos. Par exemple, il peut s'avérer opportun de protéger l'anonymat dans les cas où les journalistes désirent taire leurs sources ou encore qu'un auteur à succès désire écrire un roman sous un pseudonyme[56]. Il y a certes, en contrepartie, des risques d'abus et la possibilité qu'une personne utilise l'anonymat pour poser des actes illégaux ou contraires à l'éthique. Cependant, il faut reconnaître les bénéfices qui peuvent découler de l'utilisation d'un service de discussion anonyme. Par exemple, il semble souhaitable qu'une personne abusée sexuellement puisse partager son expérience avec un groupe de discussion sur le sujet. De même, il paraît important qu'une personne atteinte du virus du SIDA et désirant discuter de ses sentiments avec d'autres personnes atteintes du même virus, que des employés soucieux de dénoncer certaines pratiques illégales de leur employeur, ou encore que des dissidents politiques désirant exprimer des idées impopulaires, puissent le faire sans crainte de représailles, de harcèlement ou d'embarras[57].

Pourtant, même en privilégiant la solution contractuelle qu'il propose, il demeure, nous dit Long, certains problèmes insolubles, notamment celui de savoir ce que doit faire un administrateur de serveur anonyme lorsqu'un message illégal est posté sur le réseau. Doit-il en dénoncer l'auteur ? Pour les administrateurs de réseau qui avaient prévu contractuellement divulguer le nom des utilisateurs si les autorités leur en font la demande, le problème ne se pose pas, selon Long. Cependant, pour les gestionnaires de réseau qui se sont dotés d'un service anonyme plus sécuritaire, un conflit survient. Si ces derniers divulguent arbitrairement l'identité de certains usagers, le serveur deviendra inutile et les utilisateurs perdront confiance en la possibilité d'un service anonyme. En l'absence de lignes directrices, il y a risque que les autorités demandent au gestionnaire du site de révéler l'identité véritable d'utilisateurs innocents, sous prétexte d'un “postage” de matériel illégal. En contrepartie, si les autorités ne peuvent obtenir l'identité des utilisateurs, les activités criminelles risquent de proliférer. Comme le fait remarquer Long, accorder à un usager anonyme l'immunité complète face à la justice encouragerait assurément plus de contrevenants à se cacher derrière un numéro. Les serveurs anonymes deviendraient alors un paradis pour l'activité criminelle, ce qui amènerait des effets contraires à ceux

---

[56]Voir BRANSCOMB, *loc. cit.*, note 8, 1642.

[57]Voir LONG, *loc. cit.*, note 21, 1183.

recherchés[58].

Pour remédier à ce problème, Long suggère de donner aux autorités le pouvoir de demander la divulgation du nom d'un usager en vertu de la loi américaine sur l'écoute électronique, le Title III Wiretap Standard. Sous ce standard, pour obtenir que l'identité d'un utilisateur soit révélée, les autorités devront, en substance, prouver au tribunal avoir des motifs raisonnables de croire que l'individu a commis une infraction, que le matériel obtenu via cette procédure est relatif au délit et qu'une procédure d'enquête normale a été menée sans succès. Les autorités devront également rencontrer une obligation de mitigation, c'est-à-dire qu'ils devront procéder le plus tôt possible et de manière à minimaliser l'interception des communications. Cela impliquerait que l'administrateur du serveur n'aurait pas à divulguer entièrement sa liste d'usagers mais seulement le nom de l'usager fautif. Long ajoute que la possibilité de conserver, d'imprimer ou de retrouver aisément un message anonyme facilite grandement la preuve qu'aura à faire le Gouvernement. Contrairement aux cas d'écoute électronique, il sera déjà en possession de la preuve du délit. Il ne lui restera qu'à en identifier l'auteur. Ainsi, dans plusieurs cas, les motifs raisonnables qu'il devra invoquer devant le juge découleront directement du contenu du message[59].

Long pose qu'un tel compromis servirait autant les gens soucieux de préserver l'anonymat que ceux désirant prévenir les violations de la loi. Il estime qu'à tout le moins, cette solution risquerait de mieux servir la résolution du conflit anonymat-ordre public que le projet de l'administration Clinton visant plutôt à introduire une nouvelle loi[60] qui aurait pour effet d'obliger les télécommunicateurs à reconfigurer leurs réseaux de façon à permettre à une agence gouvernementale d'avoir accès, moyennant un mandat de perquisition, au contenu de toutes les communications. Pour Long, comme Internet repose sur les réseaux des compagnies de téléphone, il serait probablement assujetti à cette loi. À son avis, le libellé de la loi permettrait au FBI de demander la divulgation de l'identité d'un utilisateur

---

[58] *Id.,* 1204 et 1205.

[59] *Id.,* 1206 et 1207.

[60] Digital Telephony and Communications Privacy Improvement Act of 1994. Devant la ferme opposition des géants de l'industrie des télécommunications, dont AT&T, cette disposition originant de demandes du FBI a été retirée.

anonyme sans avoir à obtenir une autorisation judiciaire. C'est notamment pourquoi il juge cette loi inacceptable car, contrairement au standard tiré de la loi sur l'écoute électronique, cette proposition viendrait rendre l'existence de l'anonymat arbitraire[61].

Parallèlement, pour tenter de régler le conflit entre la protection de la vie privée et le respect de la loi, l'administration Clinton voulait inclure, dans les appareils de télécommunication, un mécanisme permettant à ceux qui traitent avec le gouvernement d'encrypter leurs messages. Ce mécanisme, nommé “clipper chip[62]”, aurait permis au gouvernement, en contrepartie, de décoder les messages encryptés après avoir obtenu un ordre de Cour[63]. Ce projet, on s'en doute, a suscité de violents tollés de protestations. Ses principaux critiques opposent notamment que l'utilisation de ce mécanisme ne sera pas utile pour prévenir les crimes tant que d'autres types de logiciels

---

[61]Voir LONG, *loc. cit.*, note 21, 1208 et 1209.

[62]*The Clipper Chip was developed to strike a balance between the need for privacy and the governement's ability to intercept communications. It was designed to help companies protect proprietary information by preventing criminals, terrorists and industrial spies from decoding communications made over telephones, fax machines and computers while ensuring the governement's ability to eavesdrop". Voir Charlene L. LU, "Seeking Privacy in Wireless Communications : Balancing the Right of Individual Privacy with the Need for Effective Law Enforcement*, (1995) 17 Hastings Communication & Entertainment Law Journal 529, 545.

[63]Pour une analyse plus complète de cette question voir notamment Charles R. MERRILL, *Cryptography for Attorneys - Beyond Clipper*,

http://www.law.vill.edu/chron/articles/merrill.html

Voir aussi Dorothy E. DENNING, *Resolving the Encryption Dilemna : The Case for Clipper*,

http://web.mit.edu/afs/athena/org/t/techreview/www/articles/july95/Denning.html

KOFFSKY, M. I., *Choppy Waters in the Surveillance Data Stream : The Clipper Scheme and the Particularity Clause*, (1994) 9 *High Technology Law Journal* 131.

d'encryptage seront disponibles ou autorisés sur le territoire américain[64], essentiellement parce que les criminels utiliseront des mécanismes de

[64]Il y a lieu de noter qu'il existe présentement, aux États-Unis, des restrictions à l'exportation de logiciels d'encryptage. La Electronic Frontier Foundation (EFF) a d'ailleurs institué un recours devant les tribunaux pour faire déclarer inconstitutionnelle la disposition législative en cause. À titre informatif, nous reproduisons un extrait d'un texte traitant de cette question et diffusé par la EFF dans une liste de discussion : "On October 20th in San Francisco, we'll have the first public hearing in the EFF/Bernstein lawsuit, which seeks to have the export laws on cryptography declared unconstitutional. [...] In this case, Dan Bernstein, ex-grad-student from UC Berkeley, is suing the State Department, NSA, and other agencies, with help from EFF. Our main argument is that the export controls on crypto software are a "prior restraint on publication" which is unconstitutional under the First Amendment unless handled very delicately by a court (not just by an agency acting on its own). These agencies restrained Dan's ability to publish a paper, as well as source code, for the crypto algorithm that he invented. There are additional arguments along the lines that the State Department and NSA take a lot more liberties during the export process than their own regulations and laws really permit. Like Phil Karn's case, this lawsuit really has the potential to outlaw the whole NSA crypto export scam. We could make your right to publish and export crypto software as well-protected by the courts as your right to publish and export books. Of course, the government would appeal any such decision, and it will take years and probably an eventual Supreme Court decision to make it stick. But you can be there at the very beginning. [...] The particular issue in front of Judge Patel on the 20th is whether the case should be thrown out. The government is arguing that it should. It's a mess of legal details about whether the Judicial Branch has the right to decide questions like this, and over whether we have really properly claimed a Constitutional rights violation. It will teach most observers something about how the courts work, and how the NSA and State Dept use bureaucratic tricks to avoid facing the real issues. We have managed to drag in some of these issues, like whether there is sufficient "expression" in software that the First Amendment should protect publishers of software. It's possible, but unlikely, that the judge will decide then-and-there. We will get some clues to how she is leaning, based on her questions and comments. Her written decision will come out some days or weeks later". La version intégrale de ce texte peut être consultée dans les archives de la EFF à l'adresse

ftp.eff.org,/pub/Privacy/ITAR_export/Bernstein_case/

chiffrement que le gouvernement ne pourra pas décoder[65]. Également, plusieurs objectent qu'il y a un risque que l'État n'abuse de son pouvoir pour s'introduire dans l'intimité et surveiller la vie privée des gens par le biais d'une telle technologie[66].

Pour Hardy la problématique des conflits résultant de l'anonymat semble

---

[65]Le gouvernement Clinton, pour rassurer l'opinion publique, a longtemps prétendu que la conversion au système clipper se ferait sur une base volontaire. Ses opposants ont rétorqué en faisant valoir que pour remplir ses objectifs, le projet clipper devrait absolument être obligatoire. Des documents obtenus par le Electronic Privacy Information Center en vertu de la loi sur l'accès à l'information semblent leur donner raison. Voici un extrait du texte publié sur cette question par le EPIC, disponible en version intégrale sur le serveur de la EFF à

ftp.eff.org,/pub/Activism/FOIA/Clipper_FOIA/

*Newly-released government documents show that key federal agencies concluded more than two years ago that the "Clipper Chip" encryption initiative will only succeed if alternative security techniques are outlawed. The Electronic Privacy Information Center (EPIC) obtained the documents from the Federal Bureau of Investigation under the Freedom of Information Act. EPIC, a non-profit research group, received hundreds of pages of material from FBI files concerning Clipper and cryptography. The conclusions contained in the documents appear to conflict with frequent Administration claims that use of Clipper technology will remain "voluntary". Critics of the government's initiative, including EPIC and EFF, have long maintained that the Clipper "key-escrow encryption" technique would only serve its stated purpose if made mandatory. According to the FBI documents, that view is shared by the Bureau, the National Security Agency (NSA) and the Department of Justice (DOJ) as a whole. In a "briefing document" titled "Encryption : The Threat, Applications and Potential Solutions," and sent to the National Security Council in February 1993, the FBI, NSA and DOJ concluded that : Technical solutions, such as they are, will only work if they are incorporated into *all* encryption products. To ensure that this occurs, legislation mandating the use of Government-approved encryption products or adherence to Government encryption criteria is required. Likewise, an undated FBI report titled "Impact of Emerging Telecommunications Technologies on Law Enforcement" observes that "[a]lthough the export of encryption products by the United States is controlled, domestic use is not regulated" The report concludes that "a national policy embodied in legislation is needed.". Such a policy, according to the FBI, must ensure "real-time decryption by law enforcement" and "prohibit cryptography that cannot meet the Government standard". The FBI conclusions stand in stark contrast to public assurances that the government does not intend to prohibit the use of non-escrowed encryption. EPIC has recently also filed a brief in support of CPSR's FOIA lawsuit against NSA, seeking allegedly improperly classified NSA documents on Clipper.*

[66]Voir Charlene L. LU, *loc. cit.*, note 61. Voir également REIDENBERG et GAMET-POL, *loc. cit.*, note 31, 109.

se poser légèrement différemment. Pour lui, il faut se demander que faire lorsqu'un message anonyme portant atteinte à la réputation, violant les règles du droit d'auteur ou révélant des secrets commerciaux est posté ? Pour lui, les messages anonymes mettent deux valeurs en conflit. D'une part la volonté du droit de consentir réparation à une personne ayant subi une atteinte à la réputation ou dont le travail a été distribué en contravention des règles du droit d'auteur. D'autre part, la volonté des individus d'être capable d'exprimer leurs vues sans peur d'être punis, une politique appliquée essentiellement aux propos diffamatoires et certes renforcée par l'anonymat[67].

Soutenant que le premier amendement garantit déjà aux citoyens le droit d'exprimer leurs critiques à l'égard du Gouvernement sans crainte de représailles, Hardy pose que le besoin de mettre à la disposition des usagers un service de messages anonymes pour permettre de tels commentaires est moins grand en droit américain qu'il peut l'être ailleurs[68]. Aussi, il émet l'opinion qu'un commentaire diffamatoire non-anonyme à propos d'un citoyen ordinaire amène un certain équilibre à l'ensemble des conséquences qui en découle. En effet, si la peur d'être victime de représailles gouvernementales n'existe pas lorsqu'on diffame un simple citoyen, la peur d'être l'objet d'une poursuite civile a cependant un effet dissuasif sur le diffamant. Lorsqu'on anonymise les messages, cet effet dissuasif disparaît. Le diffamant n'a pas à craindre de représailles.

---

[67]Trotter HARDY, *The Proper Legal Regime for Cyberspace,* (1994) 55 *University of Pittsburgh Law Review* 993, 1011 et 1048.

[68]*Id.*

Comment le droit doit-il résoudre cette problématique ? Hardy prétend que la clé est dans la compréhension du fait que la diffamation perdra son impact à l'égard de la réputation de la personne visée en devenant à la portée de tous, en toute impunité. En effet, la valeur des attaques aura beaucoup moins de poids si le diffamant n'ose pas s'identifier. Aussi, le poids des remarques anonymes faiblira précisément parce qu'elles sont de cette nature, la diffamation perdra toute sa signification. Par conséquent, considérant que le cyberespace procure au diffamé le forum nécessaire pour répliquer, Hardy estime que la réponse adéquate pour le système juridique est de laisser les usagers régler eux-mêmes leurs différends (self-help)[69]. Anne Branscomb tend à appuyer cette idée lorsqu'elle constate, à la lumière des débats entre les serveurs anonymes, que les usagers du cyberespace semblent capables de régler leurs problèmes entre eux, sans interventions extérieures :

> *As the tortured history of anonymus remailers indicates, net users have their own methodology for determining what is considered appropriate behavior, and they tend to favor tolerance rather than strict accountability. Furthemore, they often take enforcement of their standards into their own hands and seem quite capable of doing so without the help or intrusion of lawyers or judges from the real world*[70].

Pour Froomkin, l'anonymat, le pseudo-anonymat et l'argent électronique protègent à la fois des intérêts valables et répréhensibles. En effet, la personne éprouvant une gêne maladive ou le pamphlétaire électronique en bénéficieront autant que les criminels ou les auteurs de propagande haineuse. L'introduction d'argent électronique anonyme et non-identifiable augmentera assurément le nombre de transactions interpersonnelles anonymes[71].

---

[69] *Id.,* 1049 et 1050.

[70] Voir BRANSCOMB, *loc. cit.,* note 8, 1661.

[71] Voir FROOMKIN, *loc. cit.,* note 21, par. 48.

### 47.2 Les principales sources de menaces à la vie privée

Il convient, avant d'entrer directement dans l'analyse des situations particulières portant atteinte à la vie privée des usagers des environnements électroniques, de cerner brièvement les principales sources de menaces à cet égard. Pour l'heure, nous avons relevé cinq pôles où il y a risque d'atteintes à la vie privée des usagers, soit l'activité gouvernementale, les parties avec lesquelles on réalise une transaction[72], les abus des partenaires autorisés[73]

[72]On peut facilement imaginer que, dans les environnements électroniques, les parties avec lesquelles un usager réalise une transaction pourraient porter atteinte à sa vie privée. C'est notamment les cas lorsqu'une entreprise utilise ou vend de l'information qu'elle accumule aux fins de dresser un profil de consommation, ou encore lorsqu'une entreprise utilise des renseignements personnels obtenus lors d'une transaction pour des fins autres que celles rendues nécessaires pour la complétion de cette transaction.

[73]En effet, il est logique de penser que, dans les environnements électroniques, l'intrusion dans la vie privée d'un usager puisse survenir à l'occasion d'un abus d'un partenaire autorisé. Que doit-on entendre par là ? Cela nous semble englober les cas où une personne a normalement un droit de regard sur certaines informations en concernant une autre, mais qu'elle en fait un usage abusif ou que, plus simplement, elle abuse de son pouvoir pour avoir accès à de l'information qui ne la concerne pas. Par exemple, on peut penser que l'employeur qui posséderait un droit de regard sur le courrier électronique de ses employés, limité au contrôle nécessaire pour le maintien du système, abuserait de son pouvoir s'il se servait du contenu de ces communications pour des motifs disciplinaires.

ou des intrus[74], la conception déficiente des environnements électroniques et les erreurs humaines. Comme l'activité gouvernementale est fréquemment perçue comme étant la plus grande source de menace potentielle, nous y consacrerons, pour les fins du présent texte, la totalité de nos développements.

### 47.2.1 L'activité gouvernementale

L'activité gouvernementale est certes perçue comme étant la principale source de menaces à la vie privée des citoyens dans le cyberespace. Aussi, nous n'entendons pas nous attarder longuement sur la question du pourquoi, le projet “clipper chip[75]” nous semblant donner une indication claire des raisons pouvant pousser les usagers des environnements électroniques à craindre une intrusion de l'État dans leur vie privée via les nouveaux canaux de transmission d'informations. Qu'il nous suffise de souligner que l'écart entre la vie privée des personnes et le besoin de la société en matière d'information est certes perceptible dans le conflit entre la protection des données personnelles et le devoir du gouvernement d'assurer le maintien de la loi et de l'ordre[76]. Par conséquent, ce que nous croyons important de cerner, à ce stade, c'est la problématique entourant le comment. En d'autres

---

[74]On parle ici d'accès illégal de hackers ou de crackers aux communications électroniques des usagers des environnements électroniques. Postulant que l'accès aux ordinateurs et autres sources d'informations devrait être illimité et total, les hackers peuvent en effet entrer en conflit de plusieurs façons, dans les environnements électroniques, avec le droit et ses valeurs fondamentales, dont celle de la protection de la vie privée. Par exemple, un hacker pourrait s'introduire dans le courrier électronique d'une personne en réussissant à décoder son mot de passe. Pareillement, on peut imaginer le cas où un hacker s'introduirait dans une banque de données contenant des renseignements personnels. Sur le phénomène du "hacking" dans les environnements électroniques voir en général S. L. NORMAN, *Unauthorized Access to Electronic Fund Transfert Information : Who Should be Responsible ?* , 6 *Computer Law Journal* 171 ; Deidre BLACK, *The Computer Hacker - Electronic Vandal or Scout of the Networks ?* (Été 1993) 4 *Journal of Law and Information Science* 65-79 ; Robert L. DUNNE, *Deterring Unauthorized Access to Computers : Controlling Behavior in Cyberspace Through a Contract Law Paradigm* (Fall 1994) 35 *Jurimetrics Journal* 1.

[75]Voir à cet égard *supra,* note 61 et le texte correspondant.

[76]Voir à cet égard Randolph S. SERGENT, *A Fourth Amendment Model For Computer Networks and Data Privacy*, (1995) 81 Virginia Law Review 1181.

termes, de quelle façon l'État peut-il porter atteinte à la vie privée des citoyens[77] et, partant, quelle protection leur est offerte à cet égard ?

On peut facilement imaginer qu'une atteinte à la vie privée puisse être portée par l'État, dans les environnements électroniques, lors de deux circonstances particulières. Soit que l'État intercepte illégalement une communication électronique[78], soit que l'État accède illégalement à une banque de données contenant de l'information personnelle. Dans le premier cas, l'État devra outrepasser les dispositions législatives garantissant une protection contre ce type d'intrusions, notamment les lois sur l'écoute électronique, pour autant qu'elles s'appliquent à des communications électroniques. Dans le deuxième cas, l'État devra soit violer les droit d'un citoyen en regard d'une loi sur la protection des renseignements personnels[79], pour autant qu'il en existe une dans cette juridiction, soit outrepasser les dispositions garantissant aux citoyens une protection contre les fouilles, les saisies ou les perquisitions[80].

Aussi, rappelons d'entrée de jeu que si, aux États-Unis, puisque nous analyserons principalement des textes de doctrine américaine, la vie privée ne fait pas l'objet d'une protection constitutionnelle, elle est néanmoins protégée par le biais du quatrième amendement[81], disposition garantissant au citoyen une protection contre les fouilles, les saisies ou les perquisitions abusives de l'État. Cette protection ne s'étend qu'au gouvernement fédéral, laissant les intrusions commises par des parties privées être solutionnées par des dispositions statutaires. Fait à noter, la Cour suprême, dans l'arrêt *Katz*

---

[77]Voir, de façon générale, sur les problématiques traditionnellement reliées à la collecte, par l'État, de données personnelles informatisées Mark FALL, *Privacy Protections of Computerized Information*, (1993) 165 *Southern California Interdisciplinary Law Journal* 165.

[78]Voir à cet effet le chapitre II de la deuxième partie.

[79]Voir le chapitre I de la deuxième partie.

[80]Voir le chapitre II de la deuxième partie.

[81]Pour une argumentation faisant valoir que la "Clipper Chip" viole la "particularity clause" du Quatrième Amendement voir KOFFSKY, *loc. cit.*, note 62.

v. *United States*, a déclaré que cette disposition s'attache aux personnes et ne protège pas les lieux [82].

Comment s'est opérée, lors des quelques cas rapportés, l'intervention intrusive de l'État dans les environnements électroniques ? Dans certains cas, les services secrets sont allés jusqu'à saisir l'ordinateur de toute personne listée sur le “mailing list” d'un opérateur de babillard électronique suspecté d'avoir enfreint la loi[83]. Pour Cutrera, ce genre de méthodes d'investigation risque de porter atteinte tant à la vie privée de la personne suspectée qu'à celle d'usagers innocents[84]. Ainsi, en février 1995, l'Église de Scientologie, avec l'aide de la police finlandaise et d'Interpol, a demandé à l'opérateur d'un serveur anonyme de lui révéler l'identité d'une personne soupçonnée de lui avoir volé des fichiers informatiques. Mal préparé et croyant que la seule autre alternative s'offrant à lui aurait été la saisie complète de la banque de données, l'opérateur du serveur a révélé l'identité de l'usager en cause[85]. Bien que dans cette affaire on pourrait difficilement conclure que l'État est l'auteur de l'atteinte, l'opérateur du serveur ayant consenti à révéler l'identité du fautif, il y a lieu de se demander à quelles conditions l'État peut effectuer ce genre d'opérations ?

Cette question s'est soulevée à une occasion, dans l'affaire *Steve Jackson Games*[86], où les Services Secrets américains ont perquisitionné les bureaux d'un marchand de jeux vidéos et saisi plusieurs logiciels et ordinateurs. Dans cette poursuite, fondée sur le Electronic Communications Privacy Act of 1986 (ci-après ECPA), la Cour a jugé que le FBI ne pouvait pas se contenter d'invoquer sa bonne foi quant à une saisie faite “par inadvertance”. Soulignant que le gouvernement savait que le serveur abritait

---

[82]Nan LEVINSON, *Electrifying Speech : New Communications Technologies and Traditional Civil Liberties*.

http://www.eff.org/pub/Legal/electrifying_speech.paper

[83]Terri A. CUTRERA, *The Constitution in Cyberspace : The Fundamental Rights of Computer Users*, (1991) 60 UMKC L. Rev. 165.

[84]*Id.,* 144.

[85]A. Michael FROOMKIN, *loc. cit.,* note 21.

[86]*Steve Jackson Games, Inc.* v. *United States Secret Service* 816 F. Supp. 432 (W. D. TEX. 1993), affd, 36 F. #d 457 (5th Cir. 1994)

des communications privées, elle juge qu'il aurait dû, par conséquent, respecter les dispositions du ECPA et obtenir une autorisation judiciaire valable avant de saisir[87].

Cutrera précise que, hormis cette disposition expresse du ECPA prévoyant l'obligation pour le gouvernement d'obtenir un mandat pour accéder aux communications électroniques entreposées, l'information conservée par un tiers ne serait pas protégée, pas même par le quatrième amendement. En effet, les fichiers étant hors de la possession de leur auteur, les tribunaux américains ont traditionnellement jugé que ce dernier n'avait pas d'expectative légitime de vie privée à l'égard de cette communication. Cela donne à penser, selon Cutrera, que le contenu des babillards électroniques n'est pas protégé constitutionnellement. La protection contre les fouilles ne faisant l'objet que d'une disposition statutaire, en l'occurrence le ECPA, Cutrera estime que le droit à la protection de la vie privée des utilisateurs d'ordinateurs est donc en position précaire, étant sujet à un changement de volonté du Congrès[88].

Tout cela montre, nous dit Cutrera, les limites d'une approche définitionnelle de la vie privée, même lorsque le libellé est général. Les progrès de la science produisent les ambiguïtés du droit. Les personnes qui détestent l'incertitude ont tendance à tenter de définir ces ambiguïtés. De tels efforts ont mené à une loi comme le ECPA qui, bien qu'efficace présentement et bien rédigée, risque d'être modifiée ultérieurement. Cette pratique, consistant à permettre au législateur d'offrir une protection statutaire de la vie privée, ne semble pas respecter les intentions des rédacteurs de la Constitution. Il faut donc, pour Cutrera, explorer les limites de l'expectative légitime de vie privée en balançant les critères subjectifs avec les critères objectifs. Le quatrième amendement devrait protéger la personne, indépendamment du lieu ou des choses. Une personne devrait donc se voir garantir une protection de la vie privée, peu importe le lieux ou les instruments qu'elle utilise, en l'occurrence un réseau électronique. Cette

---

[87]Dilworth, pour sa part, estime que cette affaire soulève la question de la préservation du droit des citoyens d'encoder de l'information électronique sensible sans empêcher les autorités de faire la lutte aux criminels et aux terroristes. Voir Donald DILWORTH, *Federal Privacy Law Protects Electronic Mail* (Juil. 1993) *29 Trial 104(3).*

[88]Terri A. CUTRERA, *loc. cit.,* note 82, 144 et suiv.

approche apparaît évidemment moins sécurisante qu'une approche définitionnelle, mais également plus satisfaisante[89] :

> *Our Constitution guarantees all citizens the right to be secure in their persons and effects against unreasonable searches and seizures. It also provides that individuals will be accorded due process of law before punishment ensues. These concepts have survived two hundred years of changing technology and social conditions. The challenges posed by the proliferation of computer technology cannot change the ideas behind these guarantees. Cyberspace, after all, is the medium of ideas - the ideal place for the Constitution to prosper and glow*[90].

Dans un article récent de droit américain, Sergent pose que l'interprétation du quatrième amendement par les tribunaux rend excessivement difficile la transposition de ses implications dans les environnements électroniques. En effet, Sergent soutient que le cadre d'analyse développé par les tribunaux, qui implique notamment un processus d'équilibrage entre les demandes des individus en matière de vie privée et le maintien de l'ordre et de la sécurité publique, laisse place à l'arbitraire[91]. Selon lui, un standard qui repose sur une notion comme celle de l'expectative légitime de vie privée devrait être suffisamment souple pour appréhender les changements technologiques[92], car une société ne devrait pas voir ses valeurs fondamentales moins bien protégées en raison de tels changements[93]. C'est en fait les valeurs en vigueur dans la société qui doivent primer[94]. À l'heure actuelle, il serait logique de penser que les usagers des environnements électroniques assument simplement qu'il possèdent les mêmes attentes de vie privée qu'à l'égard du courrier postal.

---

[89] *Id.*, 165.

[90] *Id.*

[91] Voir l'analyse de Sergent, *loc. cit.*, note 75, 1193 et suiv.

[92] *Id.*, 1225.

[93] *Id.*, 1228.

[94] *Id.*

D'un point de vue normatif, il semble en effet raisonnable de croire, nous dit Sergent, qu'il devrait y avoir une mesure équivalente. Dans une analyse des risques cependant, force est d'admettre qu'il n'est pas raisonnable de penser que la vie privée est protégée lorsque certaines personnes ont la capacité physique d'intercepter les communications[95].

Sans reprendre l'argumentation étoffée de Sergent à l'égard de l'approche qui devrait être utilisée par les tribunaux américains, il y a lieu de s'intéresser à un aspect particulier de son texte. Ainsi, l'étape déterminante d'une analyse sous le quatrième amendement étant l'identification des attentes de vie privée de la personne subissant la fouille ou la perquisition, il y a lieu de relever les facteurs clés qu'a dégagés Sergent à l'égard de la détermination des attentes lors de situations impliquant de l'information électronique.

Pour qu'il y ait attente de vie privée dans un réseau à utilisateurs multiples, nous dit Sergent, deux conditions doivent être rencontrées : les données ne doivent pas être à la portée des autres utilisateurs et la capacité de l'administrateur du réseau d'avoir accès à l'information ne doit pas donner lieu à une divulgation. Ainsi, lorsque l'information est placée dans un endroit accessible à plusieurs usagers où aucune zone de sauvegarde personnelle n'a été prévue, les chances qu'il existe une attente lÈgitime de vie privée à son égard sont minces[96]. La question demeure ambiguë s'il existe de telles zones, mais pas de mécanismes permettant d'en restreindre l'accès aux tiers. Selon Sergent, il pourrait exister une attente légitime de vie privée dans ce contexte si elle résulte d'une pression sociale[97]. Une utilisation de techniques de sécurité comme l'encryptage ou des codes secrets devrait cependant suffire à créer chez l'utilisateur une attente légitime[98]. Quant aux divulgations résultant de l'administrateur du système, Sergent soutient que l'utilisateur n'a pas d'attente de vie privée à l'égard de l'information nécessaire à ce dernier pour assurer le service. L'administrateur du service ne devrait cependant pas avoir accès à d'autres

---

[95] *Id.,* 1226.

[96] *Id.,* 1197.

[97] *Id.,* 1198.

[98] *Id.,* 1199 et 1200.

types d'informations personnelles, ce qui implique que ces informations peuvent faire l'objet d'une attente légitime[99].

Pour Sergent, comme l'approche des tribunaux est faussée, il croit que leur analyse devrait se concentrer sur les usages reconnus dans la société ou sur l'émergence de mécanismes techniques permettant d'exclure les tiers pouvant porter l'atteinte. Cependant, il souligne que le problème des usages réside dans le fait qu'ils ne peuvent créer d'attente légitime de vie privée lorsqu'une technologie est toute récente. L'analogie avec le courrier postal le prouve. Les gens y ont recours car, en elle-même, la nouvelle technologie ne crée pas d'attente légitime de vie privée. Aussi, si cette analogie s'avère non fondée, la société se retrouve sans guide pour appréhender la situation. Il ne saurait non plus être question d'attente universelle lorsque les propriétaires des systèmes imposent un contrôle sur l'information à leurs usagers, même si cela s'avère contraire à la propre attente de ces derniers. Tant que ces questions ne sont pas résolues, nous dit Sergent, il ne peut exister une attente légitime fondée sur l'usage reconnu dans la société. Ainsi, la question n'est pas de savoir si les usagers, en utilisant un service électronique choisissent d'abandonner librement leur droit à la vie privée dans leur courrier électronique, mais bien de savoir quels types de systèmes devraient-ils être forcés d'utiliser ? Pour Sergent, il n'est pas assuré que les gestionnaires de grands réseaux considéreront nécessairement la vie privée comme étant d'une importance capitale[100].

## 48. Les situations particulières donnant ouverture à une intrusion dans la vie privée

Nous entrons maintenant au coeur du sujet, soit dans l'analyse des diverses situations risquant de donner ouverture à une intrusion dans la vie privée des usagers des environnements électroniques. Nous nous pencherons d'abord sur les questions reliées à la protection des données personnelles et aux sous-questions qui en découlent, soit l'élaboration de profils de consommation ainsi que la sécurité transactionnelle. Viendra

---

[99] *Id.,* 1201, 1202 et 1203.

[100] *Id.,* 1226 et 1227.

ensuite l'étude de la problématique reliée à l'interception d'une communication électronique, plus particulièrement dans les cas de réception non-désirée d'informations et d'intrusion dans le courrier électronique. D'autres types de situations peuvent donner ouverture à une intrusion dans la vie privée des usagers de l'espace cybernétique, notamment la publication ou à la diffusion, par un média d'information électronique, d'informations à caractère personnel ou de photographies. Ils ne seront cependant pas étudiés dans le cadre du présent texte.

### 48.1 L'utilisation, la cueillette, la conservation ou la transmission de données personnelles

De façon générale, l'un des pôles sensibles de la protection de la vie privée et des renseignements personnels dans les environnements électroniques concerne justement la façon d'utiliser, de recueillir, de conserver et de transmettre les données personnelles, en d'autres termes le traitement des données. Ces données personnelles pourront être de divers ordres, données transactionnelles, numéro identificateur, numéro

d'assurance sociale ou d'assurance maladie, données médicales[101], etc. Ce qui semble cependant constituer le noyau dur des préoccupations observées est relatif au traitement réservé aux données transactionnelles. À cet égard, on remarque des craintes, fondées ou non, à deux niveaux particuliers. En effet, l'établissement de profils de consommation à l'aide de données transactionnelles et la sécurité transactionnelle elles-mêmes sont au coeur des problématiques soulevées par la protection des données personnelles. Aussi avons-nous voulu, dans un premier temps, aborder la problématique du traitement des données personnelles dans sa globalité, pour ensuite nous pencher, au paragraphes I et II du chapitre I de la deuxième partie, sur les questions particulières que nous venons de soulever.

Comme on le sait, l'un des principaux problèmes rencontré à l'égard de la protection des données personnelles pour le Québec, qui possède déjà une loi de protection des renseignements personnels tant dans le secteur privé que dans le secteur public, c'est précisément la protection des données personnelles québécoises hors frontières, là où la législation s'avère soit non

---

[101] Au Québec, la question de la confidentialité du dossier médical a été abordée par le Comité consultatif sur l'autoroute de l'information. En effet, à la page 19 de son rapport le Comité identifiait le respect de l'information confidentielle du dossier médical comme étant une condition primordiale de réussite de l'utilisation de l'autoroute de l'information pour la réforme du service de santé. En page 20, le Comité soulignait que "la méfiance de la population envers la capacité de la technologie de préserver le caractère confidentiel de l'information" constitue un des obstacles importants à franchir pour ce faire. Pour remédier au problème et assurer cette confidentialité, le Comité, à la recommandation 7. 2, propose au gouvernement d'utiliser des solutions d'ordre technique, la technologie permettant, nous dit le Comité, de protéger de façon plus sûre la confidentialité des dossiers que les modes actuels de circulation et d'archivage. Le Comité recommandait également la sensibilisation des différentes associations et corporations professionnelles à ces enjeux et la définition d'un code d'éthique en matière de protection de l'information qui serait adopté par l'ensemble des partenaires du réseau. Nous reviendrons sur cette question plus loin. Pour l'instant, voir COMITÉ CONSULTATIF SUR L'AUTOROUTE DE L'INFORMATION, *Inforoute Québec : Plan d'action pour la mise en oeuvre de l'autoroute de l'information*, Québec, Gouvernement du Québec, 1995, p. 23. Pour une analyse plus détaillée des problèmes reliés à la confidentialité et à la sécurité des dossiers médicaux voir Adele A. WALLER and Deborah FULTON, Deborah K.,*The Electronic Chart : Keeping It Confidential and Secure* (Avril 1993) *26 Journal of Health and Hospital Law* 104. Voir également Terri Finkbine, ARNOLD, *Let Technology counteract Technology : Protecting the Medical Record in the Computer Age* (Hiver 1993) *15 Hastings Communications and Entertainment Law Journal (COMM-ENT)* 455-494.

suffisante, soit tout simplement inexistante[102]. Aussi, le lecteur voudra bien noter que sur les questions reliées à la protection des données personnelles, le droit américain, qui est par ailleurs déjà très engagé dans l'étude des questions juridiques relatives à l'espace cybernétique, marque un net recul par rapport au droit québécois et européen, ce dernier s'étant notamment doté d'instruments de protection des données personnelles qui constituent de véritables modèles en la matière[103].

Également, le lecteur comprendra qu'il existe une étroite relation entre les problèmes découlant de la protection des données personnelles et la possibilité pour une personne de contrôler la circulation de l'information la concernant[104]. Par exemple, la reconnaissance générale, dans les environnements électroniques, d'un droit d'accès aux données personnelles semblable à celui que contient la loi québécoise, pourrait atténuer certaines craintes soulevées par l'établissement et la revente de profils de consommation par les opérateurs d'un réseau. En contrepartie, la négation de tout droit de contrôle sur l'information personnelle risquerait de créer une incertitude chez l'usager et pourrait, au bout du compte, freiner ses élans vers les nouvelles technologies.

Avant toute chose, il y a lieu de souligner que les problèmes liés à la protection des renseignements personnels ne constituent pas, en eux-mêmes, un phénomène exclusif aux environnements électroniques. Cependant, cette problématique semble indubitablement liée au développement des technologies de l'information, l'évolution de l'un entraînant une mouvance

---

[102]On n'à qu'à penser, à cet égard, à l'absence d'instrument législatif protégeant les données personnelles dans le secteur privé, tant au Canada anglais qu'aux États-Unis.

[103]Il est à noter que certains auteurs américains, dont Reidenberg comme nous le verrons ci-après, exercent de fortes pressions pour que les États-Unis adoptent une loi de protection des renseignements personnels dans le secteur privé inspiré des modèles européens. Pour une analyse plus approfondie des problématiques reliées à la protection des données personnelles en droit américain, le lecteur pourra notamment se référer au texte de Paul M. SCHWARTZ, *Privacy and Participation : Personal Information and Public Sector Regulation in the United States*, (1995) 80 *Iowa Law Review* 553.

[104]Sur la revendication d'un droit de contrôle sur l'information voir la section A du paragraphe I du chapitre I de la première partie.

chez l'autre[105]. Ainsi, comme le fait remarquer Reidenberg, le développement des technologies de l'information et la formation de réseaux informatiques a grandement contribué à augmenter le volume d'informations personnelles disponibles ainsi qu'à éliminer les méthodes traditionnelles de collecte des données, qui présentaient moins de danger à cet égard. Cette prolifération des ordinateurs, l'apparition de fournisseurs d'informations et l'interconnexion des systèmes informatiques a donc, par ricochet, diminué la responsabilité et l'imputabilité dans le traitement de l'information personnelle.

Reprenant les principes fondamentaux en matière de gestion de l'information personnelle[106], Reidenberg confirme que le système de droit américain, que ce soit les lois fédérales ou étatiques qu'il juge construites trop étroitement, ou les torts de common law qui lui semblent limités, ne protège pas de façon cohérente et systématique la cueillette, la conservation et la transmissions des données dans le secteur privé[107]. En fait, l'enchevêtrement de toutes ces dispositions lui donne à penser que les obligations des entités qui manipulent les informations personnelles sont trop difficiles à cerner[108]. Il ajoute que la majorité des entreprises américaines ne sont pas préoccupées par ces problèmes et que la globalisation des réseaux les rend vulnérables aux mesures réglementaires des autres juridictions à l'égard de la protection de la vie privée. Il importe

---

[105]Déjà en 1986, Segal montrait que les compagnies de câble offrant des services interactifs pouvaient porter atteinte à la vie privée des usagers de trois manières différentes. Premièrement, par la compilation de données personnelles pouvant être rattachés à un utilisateur particulier. Deuxièmement, par la publication de telles informations. Troisièmement, par l'utilisation du service de câblodistribution comme instrument de surveillance. Voir SEGAL, G. R., *The Threat From Within : Cable Television and the Invasion of Privacy*, 7 *Computer Law Journal* 89, 91.

[106] Voir également à cet égard Joel R. REIDENBERG, *Setting Standards for Fair Information Practice in The U. S. Private Sector*, (1995) 80 *Iowa Law Review.*

[107] Voir également sur la protection de la vie privée dans le secteur privé en droit américain Joshua D. BLACKMAN, *A Proposal for Federal Legislation Protecting Information Privacy Across The Private Sector,* (Nov. 1993) *9 Santa Clara Computer and High-Technology Law Journal* 431-468 ; Joel R. REIDENBERG, *loc. cit.,* note 105.

[108]Lire également REIDENBERG et GAMET-POL, *loc. cit.,* note 31, 113.

donc, nous dit Reidenberg, de restructurer l'approche juridique américaine à cet égard[109].

À son avis, l'approche européenne[110] pourrait certes servir d'exemple. Aussi, comme l'information personnelle circule au-delà des frontières nationales, toute adoption de nouveaux droits devrait se faire au palier fédéral. Posant qu'il faut tenter de trouver un équilibre entre les préoccupations relatives à la vie privée et les enjeux commerciaux sous-tendus par l'adoption de telles mesures, il prône une approche flexible au détriment d'une approche purement générale qui rendrait cet équilibrage difficile à réaliser. Soulignant qu'aux États-Unis, le développement de mécanismes souples soulève des questions de mise en oeuvre, il considère que si des principes d'application générale étaient créés pour s'appliquer de façon systématique à la collecte de données, une façon d'assurer cette flexibilité serait de créer un comité de surveillance sur la vie privée. Cet organisme n'aurait pas le pouvoir d'adopter des règlements spécifiques sur la protection des renseignements personnels, mais posséderait l'autorité nécessaire pour déterminer si les codes de conduite de l'industrie équilibrent convenablement le respect de droits protégeant les renseignements personnels et les intérêts commerciaux. Cet organisme pourrait également promouvoir des lignes directrices relatives à la vie privée pour les entreprises et assurer l'immunité à celles respectant le code de conduite de l'industrie. Les compagnies prises en défaut pourraient être l'objet d'actions privées ou publiques[111].

Probablement le premier auteur à cerner avec autant d'acuité la problématique liée à la protection des renseignements personnels dans les environnements électroniques, Karim Benyekhlef, pour sa part, fait remarquer que les nouveaux environnements électroniques, qui supposent l'interconnexion des réseaux et l'interaction informatisée, décuplent la masse d'informations à caractère personnel disponible. Ce phénomène, qu'il qualifie de “dépossession informationnelle”, suscite une série de questions

---

109 Joel REIDENBERG, *Privacy in the Information Economy : A Fortress or Frontier for Individual Rights ?* , (1992) 44 *Federal Communications Law Journal* 195.

110 Reidenberg analyse d'ailleurs les instruments internationaux européens dans Joel R. REIDENBERG, *loc. cit.,* note 105.

111 *Id.,* 238 et suiv.

quant aux mécanismes de protection de la vie privée existants :

> *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*[112].

Aussi, le professeur Benyekhlef précise-t-il que le caractère résolument international des réseaux de communication soulève de difficiles questions liées à la protection transnationale des données à caractère personnel, notamment au niveau du principe de l'équivalence :

> *La protection apportée par une législation nationale en la matière ne peut en effet qu'être limitée géographiquement. Cette délocalisation de l'information a alors incité plusieurs législateurs européens à assortir leurs lois de protection des renseignements nominatifs de dispositions soumettant l'exportation de données personnelles vers l'étranger à des contrôles ou autorisations préalables. Nous savons que les nouvelles voies électroniques de communication permettent de contourner la législation mise en place sur un territoire national par la simple exportation des données personnelles, soumises à un*

---

[112] Karim BENYEKHLEF, *Les normes internationales de protection des données personnelles et l'autoroute de l'information*, dans *Le respect de la vie privée dans l'entreprise*, Actes des Journées Maximilien Caron (17 mars 1995), texte inédit, version manuscrite, 38.

> *corpus de règles précises en vertu de la loi, vers des pays dépourvus de toute législation sur la protection des renseignements nominatifs*[113].

En effet, l'adoption de dispositions législatives prohibant toute transmission de données personnelles vers un pays dont le droit interne n'assure pas une protection satisfaisante des données nominatives met en opposition deux principes fondamentaux, le droit au respect de la vie privée et la libre circulation de l'information[114]. C'est donc dans l'optique d'harmoniser le domaine des législations de protection des renseignements personnels que l'OCDE adopte, en 1980, les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* [115] 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* [116]. Comme le fait remarquer le professeur Benyekhlef, ces deux instruments consacrent l'essentiel des principes fondamentaux en matière de gestion de l'information personnelle :

---

[113] *Id.,* p. 4.

[114] Karnow pose également le problème de cette manière dans Curtis A. KARNOW, *The Encrypted Self : Fleshing Out the Rights of Electronic Personnalities*, *loc. cit.,* note 27. Sur les questions relatives à la sécurité et la confidentialité dans les contrats d'échange de données informatisées voir Amelia BOSS, *Electronic Data Interchange Agreements : Private Contracting Toward a Global Environment*, (1992) 13 *Northwestern Journal of International Law & Business* 31.

[115] Les Lignes directrices, auxquelles Le Canada a adhéré en 1984, ne constituent qu'une simple recommandation.

[116] La Convention européenne est, pour sa part, un document juridiquement contraignant. Cette dernière est entrée en vigueur en 1985 suite à sa ratification par cinq pays membres du Conseil de l'Europe. Pour une étude détaillée de ces traités internationaux voir Karim BENYEKHLEF, *loc. cit.,* note 111, 7 et suiv.

> *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*[117].

Récemment, la Commission européenne adoptait une directive qui, pour le professeur Benyekhlef, constituera “sans doute la norme internationale de référence en matière de protection des données personnelles” :

> *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*[118].

Cette directive, qui s'applique indistinctement au secteur public et privé, consacre, à l'instar des instruments l'ayant précédé, la plupart des principes fondamentaux en matière de gestion de l'information personnelle, allant à

---

[117] *Id.,* 10.

[118] *Id.,* 16 et suiv.

certains égards plus loin que les dispositions existantes[119]. Elle reconnaît, en outre, la complémentarité que peut apporter la voie autoréglementaire au plan normatif. Comme le fait remarquer le professeur Benyekhlef, *[...] il ne s'agit bien que de complémentarité. En d'autres mots, cette voie ne saurait à elle seule satisfaire aux exigences de la directive*[120].

Fait essentiel, le principe d'équivalence[121], que l'on retrouvait tant dans les *Lignes directrices* que la *Convention européenne*, se retrouve aussi dans le texte de la Directive. Selon le professeur Benyekhlef, il clarifie même la question de la protection équivalente, aménageant un standard qui pourrait

---

[119]Comme le souligne le professeur Benyekhlef, en vertu de l'article 7, les données personnelles ne peuvent être collectées *que si la personne concernée y consent indubitablement ; si elles sont nécessaires pour l'exécution d'un contrat ou de mesures précontractuelles ; si elles sont nécessaires pour respecter une obligation légale à laquelle le responsable du traitement est soumis ; si elles sont nécessaires à la sauvegarde de l'intérêt vital 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*. Pour sa part, l'article 12 reconnaît le principe de la participation. Comme le souligne Karim Benyekhlef, *il va cependant 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 le concernant. [...]* L'article 14 constitue une innovation intéressante par rapport aux autres instruments internationaux en la matière. Il prévoit que la personne fichée peut s'opposer, à tout moment et dans certains cas, pour des raisons prépondérantes tenant à sa situation particulière à ce que des données le concernant fassent l'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 inspiré 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 l'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.)". Pour une étude plus approfondie des dispositions de la directive voir Karim BENYEKHLEF, *loc. cit.*, note 111, 17 et suiv.

[120]*Id.*, 23.

[121]Le professeur Benyekhlef définit ainsi ce principe : *un pays ne s'opposera pas à la transmission de données personnelles vers un pays tiers pourvu que ce dernier assure, dans son droit interne, une protection aux données personnelles qui équivaut en substance à celle existant dans le pays exportateur*. Voir Karim BENYEKHLEF, *loc. cit.*, note 111, 26.

être qualifié de principe d'adéquation[122] :

> *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*[123].

Ces précisions étant apportées, il y a lieu de se questionner, avec le professeur Benyekhlef, sur l'applicabilité des normes internationales aux nouvelles voies électroniques de communication. De façon générale, ces dispositions établissent des procédures et pratiques qui ont, entre autres, pour but d'assurer à la personne concernée un contrôle sur ses informations personnelles. Comme le fait remarquer M. Benyekhlef, *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*

---

[122]Karim Benyekhlef pose qu'en l'absence d'indications précises sur le sens à donner à la notion de protection équivalente, il faut s'en remettre aux instruments de mise en oeuvre prévus par les instruments internationaux. Ainsi, sous les Lignes directrices qui autorise l'autoréglementation, cette voie pourrait satisfaire le principe de l'équivalence. Par contre, sous la Convention européenne, où c'est le droit interne de chaque État qui doit assurer les principes fondamentaux en matière de gestion de l'information personnelle, la voie réglementaire risquerait de ne pas satisfaire au principe de l'équivalence. Voir à cet égard Karim BENYEKHLEF, *loc. cit.*, note 111, 28 et 29.

[123]La directive définit de cette manière ce qu'on doit entendre par protection adéquate : *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.* Voir Karim BENYEKHLEF, *loc. cit.*, note 111, 29. Pour une étude du principe d'équivalence et du principe d'adéquation en droit européen voir Paul W. SCHWARTZ, *European Data Protection Law and Restrictions on International Data Flows*, (1995) 80 *Iowa Law Review* 471.

*importante d'informations personnelles*[124]. Transposant son raisonnement aux environnements électroniques il précise le champ d'application de ces normes :

> *[...] 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*[125].

Le professeur Benyekhlef se demande ensuite si ces principes fondamentaux sont en adéquation avec l'environnement électronique qui émerge ? À cet égard, il note, avec le professeur Poullet, que ces dispositions ont été créées pour régir le traitement d'informations recueillies *a priori*, tandis que les environnements électroniques supposent le traitement de données nées *a posteriori* par l'utilisation du service lui-

---

[124] *Id.*, 37.

[125] *Id.* Évidemment, ces principes ne couvrent pas les cas d'interception du courrier électronique ou les situations d'accès non autorisé à des sites contenant des données personnelles. Ainsi, comme le précise Karim Benyekhlef : *[...] la protection de la vie privée sur les nouvelles voies électroniques de communication ne se limite pas aux simples questions afférentes aux principes fondamentaux en matière de gestion de l'information personnelle. Ainsi, la possibilité d'échanger des messages électroniques sans faire l'objet d'une interception par un tiers ou même par l'État ou sans faire l'objet d'une surveillance par son employeur, par exemple, s'inscrit dans une problématique certes associée au droit à la vie privée, mais tout de même distincte de celle relative à la gestion de l'information personnelle telle qu'envisagée par les normes internationales examinées en première partie. Il ne s'agit pas de déplorer l'inapplicabilité de ces normes à ces situations. Celles-ci n'ont pas été, en effet, élaborées pour répondre à ces interrogations. D'autres normes doivent alors être développées ou adaptées pour corriger ces atteintes au droit à la vie privée. Il faut donc bien comprendre que les principes fondamentaux en matière de gestion de l'information personnelle n'ont pas vocation à régir toutes les situations soulevant le problème du droit à la vie privée dans le cyberespace. Par ailleurs, il nous semble que les atteintes potentielles les plus graves et les plus nombreuses au droit à la vie privée sont couvertes, de prime abord, par ces principes fondamentaux. En effet, les organismes publics et les entreprises commerciales sont, sans aucun doute, les principaux détenteurs de renseignements personnels. Cette formidable accumulation de données constitue, en soi, une menace beaucoup plus importante au droit à la vie privée que les exactions de quelques individus*. Voir BENYEKHLEF, *loc. cit.*, note 111, 38. Nous analyserons pour notre part ces problématiques au chapitre II de la deuxième partie.

même. Y a-t-il des dispositions qui ne résistent pas à cette usure du temps ? Selon le professeur Benyekhlef, deux concepts fondamentaux sont remis en cause, celui de “données à caractère personnel” et de “fichier automatisé”. Quant à la notion de “données à caractère personnel”, le libellé des trois instruments internationaux analysés lui semble *suffisamment large pour englober ces nouvelles applications techniques*[126]. Quant à la notion de “fichier automatisé” des *Lignes directrices* et de la *Convention Européenne*, elle vole en éclats car *les données sont aujourd'hui éparpillées et ne s'intègrent donc plus dans un ensemble ordonnancé et unique (fichier)*[127]. Cependant, le projet de directive de la Commission européenne, amendé par la Position commune de 1995, abandonne la notion de “fichier automatisé”. Pour M. Benyekhlef, cela n'implique pas pour autant que les *Lignes directrices* ou la *Convention européenne* soient obsolètes :

> *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.*

---

[126] Voir Karim BENYEKHLEF, *loc. cit.*, note 111, 39.

[127] *Id.*, 40.

> *[...] 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*[128].

Constatant les multiples fonctionnalités potentielles des autoroutes de l'information et leur caractère résolument international, le professeur Benyekhlef croit qu'il faut, parallèlement à ces instruments, développer des règles complémentaires ou spécifiques pour encadrer l'exercice des principes qu'ils reconnaissent. Le fait que la protection des renseignements personnels ne soit pas uniforme, à preuve l'absence de législation générale protégeant ces données tant aux États-Unis[129] qu'au Canada anglais, ajouté à l'intangibilité du cyberespace, soulève de sérieuses questions à l'égard du principe d'équivalence :

> *Comment assurer une application effective de ces règles [de protection des données personnelles] lorsque l'usager est domicilié à Montréal et que le serveur, une entreprise commerciale, a sa place d'affaires à la Nouvelle-Orléans ou à Hong Kong ? Quelle autorité assurera l'application et la sanction de ces règles ? Comment déterminer la violation de ces règles dans un environnement aussi volatil et insaisissable ? Même si, par hypothèse, toutes les nations*

---

[128] *Id.*, 42 et 43.

[129] Reidenberg écrit d'ailleurs qu'il est urgent , en regard du principe d'équivalence, que les États-Unis adoptent des principes fondamentaux en matière de gestion de l'information personnelle : *Networks and information transmissions are global in nature, and few would deny that divergent norms in a global information economy pose problems. Consequently, information standards cannot be developed solely on a national level. Indeed, the European Commission has noted that if countries were to adopt varying standards, efforts to safeguard a high level of protection could be nullified by transfers to other countries in wich the protection provided is inadequate. To accomplish true data protection then, American standards of fair information practice must be interoperable with worldwide trends in data privacy. Only in this way can we maintain the competitive position of american business on the Global Information Infrastructure*. Lire REIDENBERG et GAMET, *loc. cit.*, note 31, 110 et 111.

> *étaient dotées d'une loi de protection des données personnelles, le problème de l'intangibilité et de la délocalisation continuerait à se poser : quelle loi appliquer ? quelle autorité est compétente ? comment assurer l'exercice des droits d'accès et de correction de la personne concernée ? comment cette dernière peut-elle déterminer l'existence d'un traitement automatisé la concernant ? comment concilier les différences normatives qui ne manqueront pas d'affliger les instruments pertinents*[130] *?*

L'application pratique et opérationnelle des normes internationales n'étant pas aisée, Karim Benyekhlef suggère qu'une coopération internationale est essentielle, si l'on veut garantir la protection de la vie privée sur les inforoutes. Parallèlement, des mécanismes complémentaires comme l'autoréglementation, le principe de proximité, le développement d'un standard de type ISO 9000 et la voie contractuelle, pourraient contribuer, en épaulant les normes internationales, à atteindre cet objectif[131].

En effet, le développement de normes réglementaires par des associations d'entreprises, des gestionnaires de réseau, des fournisseurs d'information, des réseaux de communication et des usagers, en conjonction avec les autorités publiques, pourrait selon Karim Benyekhlef assurer une protection complémentaire de la vie privée informationnelle, malgré les déficiences qu'on peut relever à l'égard du contrôle et de la sanction de ces normes. Ces acteurs, qu'il qualifie “d'agents de proximité”, car ils se retrouvent au coeur de l'action, seraient les mieux placés pour répondre efficacement aux problèmes soulevés dans le cyberespace. On pourrait donc aller plus loin sur la voie autoréglementaire et leur confier, nous dit M. Benyekhlef :

> *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*

---

[130] Voir BENYEKHLEF, *loc. cit.,* note 111, 44.

[131] *Id.,* 45.

*l'action normative entreprise par les autorités publiques. Mais au-delà de l'élaboration et de la conception de normes sectorielles ou particulières, on pourrait également leur confier la tâche de mettre en oeuvre ces normes. En d'autres termes, les agents de proximité devraient assurer l'application des normes élaborées. C'est là, nous semble-t-il, une des seules manières de répondre adéquatement à la délocalisation et à l'intangibilité de l'information circulant dans le cyberespace. Puisque l'information est délocalisée, il convient également de délocaliser les tâches d'élaboration* et *de mise en oeuvre ou d'application des normes. Autrement, les autorités publiques ne pourront jamais assurer le respect des règles qu'elles auront édictées.*

*Le principe de proximité nous semble une solution concrète susceptible de faciliter la normalisation des inforoutes. Le caractère international de celles-ci s'oppose, en effet, à toute solution normative uniquement globale ou générale. Une telle approche se heurte à d'immenses difficultés pratiques d'application. Le principe de proximité a pour avantage de localiser ou de régionaliser, en quelque sorte, la résolution des problèmes ou des conflits suscités par un environnement électronique transnational. En fait, ce principe est le pendant, d'une certaine manière, du principe de subsidiarité que l'on retrouve en droit européen. Selon le principe de subsidiarité, il convient de laisser aux instances nationales ou locales le soin de régler les difficultés qui ne peuvent être raisonnablement traitées au plan communautaire. Il importe de rappeler que l'action des agents de proximité doit s'inscrire dans le cadre normatif général mis de l'avant par le législateur national ou par un accord international. Autrement dit, les normes conçues et appliquées par les agents de proximité tirent leur légitimité et leur licéité du fait qu'elles complètent ou explicitent le cadre normatif général. Bien évidemment, il s'agit de prévoir des mécanismes garantissant l'indépendance des agents de proximité afin d'éviter leur inféodation à des intérêts clientélaires ou financiers*[132].

---

[132] *Id.*, 46.

Par ailleurs, l'Association canadienne des standards (ACS) élabore en ce moment, avec la collaboration du secteur privé, de certaines associations de consommateurs et des autorités publiques, un code de conduite standard relatif à la vie privée[133]. Ce code, qui serait applicable au secteur privé, intégrerait les normes afférentes à la protection des données personnelles aux standards de gestion des entreprises, au même titre que les règles comptables reconnues dans le traitement des états financiers. Un audit pourrait même être effectué et comprendrait, pour emprunter les termes du professeur Benyekhlef, *l'analyse des modalités de gestion de l'information personnelle au regard du standard pertinent*. La norme développée pourrait ultérieurement devenir un standard international (ISO 9000), reconnu et uniforme, de gestion[134].

Enfin, Karim Benyekhlef souligne que la voie contractuelle peut constituer une voie complémentaire ou substitutive. Ainsi, une partie désirant exporter des données personnelles vers un pays dépourvu de toute législation en la matière pourra le faire dans la mesure où ce dernier s'engagera à respecter contractuellement les principes fondamentaux en

---

[133]Dans le rapport qu'il a rendu public récemment, le Comité consultatif sur l'autoroute de l'information recommande que l'État fédéral prenne l'initiative en matière de mise en oeuvre de la protection des renseignements personnels et de la sécurité des communications sur l'inforoute, avec la participation des gouvernements provinciaux et territoriaux, des organismes publics et privés ainsi que des organisations de consommateurs. En ce qui concerne le respect de la vie privée et la protection des renseignements personnels, le Comité recommande l'adoption d'une loi cadre exigeant des détenteurs de renseignements personnels qu'ils rencontrent les exigences du Code type CSA. Ces détenteurs sont aussi invités à s'engager dans l'harmonisation des normes canadiennes et internationales en la matière, par l'adoption de technologies respectueuses des principes de respect de la vie privée, ainsi que par l'éducation du public. Pour ce qui est de la sécurité des communications, le Comité recommande l'établissement d'un niveau adéquat de protection et l'adoption d'une politique canadienne de cryptage des communications se distinguant de l'approche américaine actuelle. Il souligne l'urgence d'établir une administration de la certification des clefs publiques d' encryptage. Voir notamment The Information Highway Advisory Council, *Rules for the Info Highway ?* , (Octobre 1995) 1 *Privacy Files* 4.

[134]Voir BENYEKHLEF, *loc. cit.,* note 111, 48.

vigueur dans la loi du pays exportateur[135]. Toutefois, cette solution ne doit pas être perçue comme une panacée à tous les maux :

> *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. 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*[136].

---

[135]En 1992, le Conseil de l'Europe, conjointement avec la Commission européenne et la Chambre de commerce internationale, a entrepris la rédaction d'un contrat-type applicable aux flux transfrontières de données à caractère personnel. Voir à cet égard Conseil de l'Europe, *Contrat-type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de données et Rapport explicatif* Strasbourg, T-PD (92) 7 révisé, 2 novembre 1992. Voir Karim BENYEKHLEF, *loc. cit.,* note 111, 48.

[136]*Id.,* 49 et 50. Reidenberg semble également avoir ses réserves sur la solution contractuelle : *Traditionally, the business community opposes the establishment of legal standards ; it prefers to resort to self-regulation to assure fair standards for treatment of personal information in American society. Yet, the experiences resulting in legislation and the discomfort of prominent businesses with industry practices show that the sectoral restrictions on the treatment of information have not been sufficient.* Lire REIDENBERG et GAMET-POL, *loc. cit.,* note 31, 114.

En conclusion, le professeur Benyekhlef pose que les principes fondamentaux en matière de gestion de l'information personnelle consacrés dans les documents internationaux paraissent en mesure de garantir la protection de la vie privée sur les inforoutes. Cependant, en raison de l'intangibilité du cyberespace et la délocalisation des acteurs télématiques, il est d'avis que leur applicabilité, en pratique, semble difficile. C'est pour cette raison qu'une coopération internationale lui paraît primordiale, en conjonction avec le développement des diverses voies complémentaires mentionnées ci-haut[137].

### 48.1.1 La compilation de données statistiques relatives à la consommation des abonnés

L'une des principales problématique découlant de l'utilisation, de la cueillette, de la conservation ou de la transmission de données personnelles dans les environnements électroniques concerne l'élaboration de profils de consommation personnels à l'aide de données transactionnelles[138]. En effet, si un consommateur peut, dans les environnements électroniques, effectuer différents types de transactions à partir de son domicile, y a-t-il lieu de craindre que des informations afférentes à ces transactions soient collectées, analysées et utilisées aux fins de dresser des profils de consommation qui permettraient aux commerçants électroniques de cibler leur clientèle en fonction des besoins, du style de vie ou des choix d'achats du consommateur ? Doit-on redouter, dès lors, que des informations concernant la vie privée soient collectées lors de transactions et utilisées à

---

[137]Voir BENYEKHLEF, *loc. cit.*, note 111, 51.

[138]*The multiplication of interactive communications increases the possiblity of hidden surveillance of private citizens. Industries obtain bits of personal information from many sources. Interactive communications give the transaction details such as those collected through a credit card telephone call. Likewise, calls to toll free numbers, mail order purchases, as well as subscription lists from publications, and purchasing patterns at stores offer a great deal of information about individuals. Even public records provide information to an industry : property records, for example, indicate the purchase price of an individual's home and any outstanding mortgage amounts. Those items of information are then cross-referenced and combined to establish detailed profiles of individuals. Most citizens are unaware of the uses to wich such collected information is put.* Joel REIDENBERG et Françoise GAMET-POL, *loc. cit.*, note 31, 121.

mauvais escient ? La possibilité de coupler[139] une multitude de renseignements personnels conservés dans divers fichiers à l'insu des personnes concernées pourrait-elle avoir des conséquences négatives sur ces derniers, par exemple empêcher l'accès à certains services ? Comme le fait remarquer Karim Benyekhlef :

> *Ce n'est pas tant l'achat, dans ce dernier cas de figure, qui constitue un danger pour la vie privée que la possibilité pour le serveur commercial de dresser un profil des habitudes de consommation de l'usager (données transactionnelles). Ce profil devient une précieuse source de données personnelles qui peut être vendu à d'autres entreprises entraînant par là, bien souvent, un détournement des finalités premières de collecte*[140].

La lecture d'un texte comme celui de Segal, qui date de 1986, montre que la problématique de la compilation de données relatives à la consommation des abonnés et, partant, l'établissement de profils de consommation, n'est pas nouvelle. Il est en effet déjà loisible aux entreprises de câblodistribution, et ce depuis plusieurs années, de compiler des données sur les préférences de consommation des utilisateurs, sur leurs transactions financières de même que sur leurs opinions personnelles ou politiques. Ainsi, les câblodistributeurs ont depuis longtemps déjà acquis cette possibilité de développer et de maintenir un portrait à jour des activités et des préoccupations politiques, économiques et sociales des usagers du service[141].

Plus récemment, Louis Harris & associates et Alan Westin se sont intéressés à la question, dans le cadre d'un sondage mené aux États-Unis en

---

[139]Voir Kenneth James LANGAN, *Computer Matching Programs : A Threat to Privacy ?* , (1979) 15*Columbia Journal of Law and Social Problems* 143 et Rubin E. CRUSE, *Invasions of Privacy and Computer Matching Programs : A Different Perspective*, (1992) XI *Computer/Law Journal* 461.

[140]Voir BENYEKHLEF, *loc. cit.*, note 111, 35.

[141]SEGAL, G. R., *The Threat From Within : Cable Television and the Invasion of Privacy*, (1986) 7 *Computer Law Journal* 89. Voir également WASHBURN, P., Electronic Journalism, Computers and Privacy, 3 *Computer Law Journal* 189, 191.

juin-juillet 1994[142]. D'entrée de jeu, Harris et Westin soulignent que les hauts coûts reliés au développement et à l'exploitation de services électroniques interactifs inciteront les fournisseurs de services à tenter de compiler des informations sur les usagers, ce qui leur permettrait de mieux découper les applications offertes en fonction des besoins du consommateur. Au surplus, connaissant le nom et l'adresse des utilisateurs, ils pourraient effectuer des campagnes de marketing mieux ciblées[143].

L'un des volets les plus intéressants du sondage montre que la population américaine ne croit pas que l'adoption de lois ou de règlements par le gouvernement est souhaitable pour solutionner les problèmes reliés à la vie privée. Comme le souligne Westin, 73% des répondants opteraient plutôt pour l'adoption de politiques volontaires de la part des industries. Un autre volet du sondage montre que 43% des répondants ont de grandes préoccupations à l'égard de la protection de leur vie privée dans le cadre d'activités transactionnelles[144].

Cependant, 52% des répondants prétendent qu'ils seraient intéressés à ce qu'on leur présente de la publicité basée sur leurs habitudes de consommation. Lorsque questionnés directement sur la possibilité d'établissement d'un profil de consommation basé sur leurs habitudes de consommation, 51% des répondants se sont dit préoccupés par cette question. De ce nombre, 61% se disaient concernés par la question de confidentialité à l'égard des informations qui les concernent. En outre, le sondage présentait aux répondants quatre types de pratiques visant à sauvegarder cette confidentialité. Une proportion de 77% juge important qu'on informe le consommateur à l'avance sur les profils et comment ils seront utilisés. Permettre à l'usager un contrôle sur les types et les temps de publicité a été jugé important par 76% des répondants. Également, une

---

142 Louis HARRIS et Alan F. WESTIN, *Privacy of Consumer Transaction Records in Future Home Interactive Services : What the Public Says - What the Public Wants, (Reports from and Commentaries on a National Survey of Consumers, Interactive Services, and Privacy)*, présenté dans le cadre du *Fifth Conference on Computers, Freedom and Privacy*, June-July 1994, disponible sur Internet à l'adresse :

http://www-techlaw.stanford.edu/CFP95.Program.html

143Voir BENYEKHLEF, *loc. cit.*, note 111, 36.

144*Id.*, 41.

proportion de 74% jugeait important de permettre au consommateur de réviser l'information contenue dans son profil. Enfin, 70% des répondants estiment important de permettre à l'utilisateur d'indiquer quel profil peut être utilisé pour la publicité[145].

En conclusion, Westin infère de ce sondage que les fournisseurs de services devront adopter des types de règles semblables à celles proposées dans le sondage s'ils veulent rallier la majorité des usagers[146]. La bonne nouvelle dans leur cas semble être le fait que le public pense qu'on devrait leur donner une chance d'adopter ces politiques sur une base volontaire, plutôt que d'avoir recours à une intervention législative[147].

À la lumière de ce sondage, Mary J. Culnan pose que les citoyens semblent prêts à échanger une protection absolue de leur vie privée contre des bénéfices sociaux ou économiques, tout en s'attentant à ce que l'information les concernant soit traitée équitablement. Selon elle, ce sondage indique clairement que les consommateurs veulent connaître les règles du jeu et exercer un contrôle sur la façon de traiter l'information qui circule à leur sujet. Tout se résumerait donc, selon Culnan, à identifier ce qui constitue une pratique équitable et ce qui ne l'est pas. Permettre au consommateur un “opting-out”, c'est-à-dire un contrôle sélectif sur l'information qui le concerne, lui semble devoir figurer au coeur d'une entente éventuelle entre les parties afin que les consommateurs puissent la percevoir comme étant juste. Outre ces question, Culnan soulève un point important n'ayant pas été abordé dans le sondage : quelle est la réaction des gens au transfert d'informations personnelles sur la consommation à des entreprises tierces[148].

Un sondage mené au Canada, en 1995, a également tenté de cerner les inquiétudes, l'attitude ainsi que les expériences vécues par les Canadiens en

---

[145] *Id.*, 43.

[146] Cela rejoint l'opinion de Reidenberg lorsqu'il écrit : *For networks to develop and sustain the confidence of their participants, citizens and businesses must both be afforded a high degree of involvement in the decisions about the circulation of identifying data*. Lire REIDENBERG et GAMET-POL, *loc. cit.*, note 31, 109.

[147] Voir BENYEKHLEF, *loc. cit.*, note 111, 44.

[148] *Id.*, 44 et 45.

regard de leur vie privée informationnelle[149]. D'autres sondages avaient été menés, auparavant, sur la question générale de la protection de la vie privée, mais ces sondages n'apportaient que peu de lumière sur la question de savoir quels types d'usage des données personnelles paraissent acceptables aux citoyens.

De façon générale, ce sondage montre qu'une proportion de 76% des canadiens croit qu'elle a moins de contrôle sur l'information qui la concerne qu'il y a dix ans[150]. Les Canadiens seraient particulièrement préoccupés par l'échange de données personnelles entre les divers organismes, particulièrement lorsque l'entreprise privée est en cause. En fait, ils se sentent plus préoccupés pour leur vie privée, dans une proportion de 90%, lorsque l'entreprise privée est en cause, cette proportion chutant à 70% lorsque l'État seul est concerné[151].

Un constat à *l'effet que la question du contrôle sur l'information est fondamentale émerge particulièrement de l'ensemble du sondage. Ainsi, il appert que les Canadiens ne sont pas dérangés, dans une proportion de 79%, par l'utilisation de données les concernant, ceci tant qu'ils en sont tenus au courant et qu'ils peuvent y mettre un terme. Une proportion de 95% des Canadiens veut être informée des méthodes de collecte ainsi que de l'usage qui sera fait des données personnelles. Les Canadiens insistent, dans une proportion de 94%, pour que leur consentement soit obtenu avant que ces données ne soient divulguées à d'autres entreprises. Également, ils estiment que les innovations technologiques ne devraient pas placer sur eux un fardeau plus considérable à l'égard de la protection de leurs renseignements personnels (82%). De plus, ils désirent savoir comment ces nouvelles technologies peuvent affecter leur vie privée (86%)*[152].

---

[149]Voir sur les résultats de ce sondage Philippa LAWSON et Marie VALLÉE, *Canadians Take their Information Personal,* (Octobre 1995) 1 *Privacy Files* 4.

[150]Ce résultat semble être compatible avec la lecture que fait Reidenberg de la situation américaine lorsqu'il écrit : *At present, both citizens and businesses in the United States lack confidence in our information-based society. A majority of Americans believe that they have lost control of their personal information*. Lire REIDENBERG et GAMET-POL, *loc. cit.,* note 31, 108.

[151]Voir Philippa LAWSON et Marie VALLÉE, *loc. cit.,* note 148, 5.

[152]*Id.*

Selon les résultats obtenus par les sondeurs, il appert que 95% des canadiens disent avoir déjà vécu une violation de leur intimité informationnelle par la réception d'appels inopportuns. Les sondeurs établissent également une corrélation entre la perception reliée à l'intrusion dans la vie privée informationnelle et l'opinion des gens à l'égard de sa justification. Ainsi, lorsqu'une majorité des répondants conclut qu'une pratique est intrusive, une majorité des répondants conclut également qu'elle est injustifiée, sauf dans le cas des tests de dépistage de drogues par l'employeur[153].

L'opinion des répondants à l'égard du caractère intrusif d'une pratique et de sa justification serait également liée à l'appréciation de leurs conséquences. En fait, les canadiens seraient aussi concernés par l'utilisation des données personnelles que les méthodes de collecte et de divulgation. Par exemple, une proportion de 90% des répondants considère comme une intrusion le fait pour un hôpital de transférer des informations médicales à une compagnie d'assurances, alors qu'un transfert d'informations médicales de pharmacien à pharmacien est considéré intrusive par seulement 15% des répondants. Pareillement, 42% des Canadiens voient la réception d'appels d'organismes de charité comme une intrusion. Cette proportion passe à 61% lorsque la sollicitation vient d'une compagnie de télémarketing. Les sondeurs expliquent ces résultats en posant que la population canadienne fait preuve de pragmatisme dans son appréciation de l'utilisation de renseignements personnels. En fait, elle évaluerait les situations au cas par cas et tiendrait compte de multiples facteurs. Dans le dernier exemple, le type d'entreprise effectuant la sollicitation (organisme de charité vs. entreprise privée) ainsi que la nature de l'appel (venir en aide aux démunis par opposition à la recherche de profits) seraient des facteurs importants à considérer[154].

Pour les sondeurs, il paraît clair que les Canadiens ne voient pas la protection de l'information personnelle en termes absolus ou abstraits. La perception reliée au degré d'intrusion et à la justification de certaines pratiques varie en fonction d'une multitude de facteurs. La vie privée, en elle-même, ne serait qu'un de ces facteurs. Les principaux facteurs

---

153 *Id.,* 6.

154 *Id.,* 6 et 7.

influençant la perception des canadiens comprendraient les bénéfices sociaux ou personnels découlant de la transaction, le degré de consentement, la connaissance par le répondant du processus de contrôle sur la transaction, le type d'information en jeu ainsi que le degré de confiance à l'égard des institutions impliquées. Les enjeux liés au contrôle sur les renseignements personnels et aux conséquences (bénéfiques ou nuisibles) de leur utilisation sont néanmoins ceux qui auraient l'impact le plus marqué sur les niveaux d'inquiétude et d'acceptation. Ces enjeux sont probablement ceux qui détermineront, nous disent les sondeurs, les préférences de la population quant aux types de systèmes et de services offerts sur l'inforoute[155].

Un autre volet de l'étude démontre que les Canadiens ne connaissent pas, de façon générale, les lois, la réglementation ainsi que les divers programmes qui visent à protéger les données personnelles. Également, un très faible nombre des répondants s'est effectivement prévalu de son droit d'accès à l'information[156]. Enfin, il semble qu'aux termes du sondage, la population canadienne n'accorde que très peu d'appui à des solutions fondées sur l'autoréglementation (7%). L'intervention législative de l'État n'est guère mieux prisée cependant (21%). Il semble que les Canadiens désirent participer activement, dans une proportion de 69%, à l'élaboration de solutions pour enrayer la problématique de l'utilisation des données personnelles[157].

Dans un autre ordre d'idées, Michael Stern propose une solution originale susceptible de résoudre la problématique des profils de consommation. Il s'agirait de laisser au consommateur, par le biais d'un programme informatique de gestion, un agent mobile, le soin de révéler les informations qu'il juge à propos. Il n'est donc plus ici question de collecter des informations à tous vents et de bâtir un profil de consommation. C'est plutôt le consommateur qui exprime un besoin à son agent mobile, via un réseau électronique. Ce programme informatique posséderait la capacité de chercher, de compiler, de transmettre et d'organiser l'information selon les

---

155 *Id.*, 7.

156 *Id.*, 8.

157 *Id.*, 8 et 9.

demandes de l'usager[158]. Ainsi, par exemple, Pierre tape sur son clavier : “Je veux des billets pour le spectacle des Stones le 10 août. Qu'y a-t-il de disponible ? “L'agent mobile entre en action, traite l'information et la renvoie à Pierre en lui disant que tout est vendu. Ou encore Pierre tape sur son clavier : *Avertis-moi s'il y a une baisse des actions de Anémone Aérospatiale*. Le même processus s'exécute, l'agent mobile avertit Pierre qu'une chute de trois dixième de point a été enregistrée à 14h00. Le programme pourrait même aller jusqu'à organiser l'agenda de Pierre : *Vérifie s'il y a des billets de moins de 50$ pour le prochain concert de Pavarotti à Montréal et réserve deux places si je suis en ville cette journée-là*”. Réponse de l'agent mobile : *Confirmé pour le 13 janvier, Stade Olympique, sièges 7 et 8 rangée 541. Coût total 59$*.

L'avantage d'un tel système, pour Stern, tient dans le fait que c'est le consommateur qui détient le contrôle de l'information, contrairement aux programmes conventionnels où il ne sait pas que des renseignements le touchant ont été collectés et, à plus forte raison, n'y a pas accès non plus que le contrôle. Plutôt que de voir leurs intérêts identifiés par d'autres, les consommateurs pourraient donc eux-mêmes exprimer leurs intérêts. Cela permettrait, selon Stern, d'enrayer les problèmes reliés à la protection des données personnelles. Ainsi, un utilisateur pourrait commander à son agent de refuser systématiquement de répondre à certains types d'enquêtes ou de demandes. Également, l'utilisateur pourrait mandater un agent mobile afin de vérifier la banque de données contenant son profil de consommation et demander à ce dernier de l'avertir si quelque chose y était changé. Un utilisateur pourrait, en outre, demander à son agent mobile de ne révéler son numéro de téléphone personnel qu'à des personnes prédéterminées. Fin de compte, le consommateur serait maître des informations personnelles le concernant, il y aurait accès et pourrait connaître les changements apportés à son profil[159].

---

[158]Michael STERN, *Mobile Agents : Providing Control to the Consumer*, présenté dans le cadre du *Fifth Conference on Computers, Freedom and Privacy*, 1994, p. 47, disponible à :

http://www-techlaw.stanford.edu/CFP95.Program.html

[159]*Id.*, 48 et 49.

### 48.1.2 La sécurité transactionnelle et l'identification individuelle

Au-delà de l'utilisation des données transactionnelles aux fins de dresser des profils sur les habitudes de consommation des utilisateurs d'un réseau, se pose la question de la sécurité transactionnelle et de l'identification individuelle. En effet, dans le cadre des transactions, les usagers seront appelés à fournir des renseignements personnels tels un numéro de carte de crédit ou encore leur numéro de permis de conduire[160]. Dans certains cas, on leur demandera évidemment de s'identifier. Or donc, outre la question du traitement des données que nous avons abordée ci-dessus, se surgit également la question de savoir par quels mécanismes l'on pourra garantir que ces renseignements personnels ne seront pas interceptés par des hackers. On l'aura deviné les solutions techniques, notamment l'encryptage, la signature électronique ainsi que l'anonymat semblent paver une voie royale à cet égard[161].

En effet, des membres d'un groupe de travail, réuni à l'occasion *du Fifth Conference on Computers, Freedom & Privacy* et dirigés par Roger Clarke, se sont penchés sur la problématique des transactions dans les

---

[160]Sur les questions de sécurité, de confidentialité et de protection des données en EDI voir Amelia H. BOSS, *Electronic Data Interchange Agreements : Private Contracting Toward a Global Environment*, (1992) 13 *Northwestern Journal of International Law & Business* 31, 54 et suiv. Sur l'utilisation du numéro d'assurance sociale comme identifiant personnel voir T. V. WEBER, *Privacy at Risk in the Age of Information : Does the Social Security Number Reveal Too Many Secrets ?* (Nov. 1993) *5 National Trial Lawyer* 61. Sur les questions de sécurité transactionnelle voir D. A. DOHENY, and G. J. FORRER, *Electronic Access to Account Information and Financial Privacy*, (Sept. -Oct. 1992) 109 *Banking Law Journal* 436.

[161]À cet égard, la lecture des actes du colloque *Faire des affaires en toute sécurité sur les autoroutes de l'information* tenu à Montréal les 30 et 31 août 1995 peut s'avérer intéressante. Voir notamment Michael S. BAUM, "Secure Electronic Commerce : the Next Wave" in *Faire des affaires en toute sécurité sur les autoroutes de l'information*, Actes du colloque présenté par l'Institut Mondial EDI, Montréal, 30-31 août 1995 ; Al Pickering, *The Security Challenge and Public Key Infrastructures on the Information Highway*, *loc. cit.* ; Pierre TRUDEL, *Internet et commerce électronique : réglementation et autoréglementation*, *loc. cit.* ; Alan ASAY, *Introduction to the Law and Technology of Digital Signatures*, *loc. cit.*

environnements électroniques et de ses incidences sur la vie privée[162]. D'emblée, force nous est de constater qu'ils envisagent l'anonymat et le pseudo-anonymat comme des moyens essentiels de protéger la vie privée des consommateurs dans ces lieux.

Dans un premier temps, ils abordent la notion de transaction identifiable, qu'ils définissent comme étant une opération suffisamment précise pour identifier l'individu en cause, par exemple les transactions réalisées avec une carte de crédit ou une carte-débit. Ils remarquent que le 20ème siècle a amené une forte augmentation de l'information disponible à l'égard du gouvernement et des diverses entreprises et organismes. En contrepartie, le développement de la technologie a de plus en plus favorisé le traitement à distance avec ces institutions. Cette distance entre les acteurs aurait amené les parties à s'accorder moins de confiance, les corporations et les gouvernements répondant à cette perte de confiance avec des mesures de contrôle propres à éviter les abus, la fraude et les pertes. Pour eux, il paraît certain qu'il existe présentement un “impératif administratif” qui veut que les transactions entre les individus et les organisations soient nécessairement identifiées. Cet impératif aurait été couplé avec un autre, celui voulant qu'il soit nécessaire d'appliquer les technologies de l'information aux procédés du gouvernement et des entreprises. Il serait donc clair, dans l'esprit des employés de ces diverses institutions, que l'individu refusant de décliner son identité est nécessairement un fraudeur et qu'il doit être traité comme tel[163].

En second lieu, ils traitent de l'identification erronée. Il semble que l'un des enjeux majeurs pour les corporations évoluant dans les environnements électroniques, ainsi que pour les consommateurs par ricochet, soit de s'assurer que l'information concernant l'identification tirée des transactions réalisées n'est pas ambiguë, erronée ou incorrecte. Cela pourrait en effet mener, par exemple, à l'appropriation non-détectée par un tiers d'un numéro, tel celui d'une carte de crédit, qui permettrait ultérieurement l'identification

---

[162]Voir CLARKE, R. et autres, *The Scope for Transaction Anonymity and Pseudonymity, présenté dans le cadre du Fifth Conference on Computers, Freedom and Privacy*, June-July 1994, disponible sur Internet à l'adresse

http://www-techlaw.stanford.edu/CFP95.Program.html

[163]*Id.,* 108.

individuelle d'une personne. Le développement de méthodes d'identification qui suscitent un bon degré de confiance est par conséquent essentiel[164].

Dans ce contexte, l'anonymat, qui réfère à l'absence d'éléments identifiants lors d'une transaction, semble être une façon adéquate de protéger la vie privée informationnelle des individus des dangers ou de l'embarras qu'une divulgation pourrait susciter. Ainsi, on pourrait protéger dans plusieurs cas les intérêts des deux parties, en l'absence d'identification de l'individu. En fait, plutôt que d'identifier l'individu, on authentifierait son éligibilité ou sa capacité à prendre part à la transaction[165].

Aussi, il existerait trois façons différentes d'envisager la situation. Une première approche, qui est actuellement celle prônée par le gouvernement, est d'asseoir la protection des données personnelles sur des lois particulières qui confirmeraient le droit des agences gouvernementales de collecter, d'utiliser et d'échanger l'information. Cette optique exclurait tout recours à une technologie favorisant l'anonymat, comme l'argent électronique par exemple. Il y a aussi la tendance contraire, celle de conférer aux usagers un droit de contrôle sur l'information qui les concerne, soit au moyen d'une reconnaissance constitutionnelle d'un tel droit, soit en leur cédant un droit de propriété intellectuelle sur les données les concernant. La troisième solution consisterait à trouver un équilibre entre ces intérêts opposés[166].

Par conséquent, il serait possible que la qualification du caractère dominant des intérêts corporatifs, par delà les simples principes fondamentaux en matière de gestion de l'information personnelle, les codes de conduite et les mécanismes d'autorégulation, soit remise en perspective. Au lieu de proposer un vaste ensemble de principes, on pourrait possiblement mieux faire avec une succession de négociations isolées dans des contextes particuliers. Dans plusieurs pays, les relations avec les fournisseurs de services financiers, les agences gouvernementales, les services de santé et les agences de marketing pourraient être des points de départ pour un équilibrage dans la balance des intérêts en jeu. Dans ce

---

164 *Id.*

165 *Id.,* 209.

166 *Id.,* 210.

dernier cas, le pseudo-anonymat pourrait être un moyen privilégié d'atteindre cette équilibre[167].

## 48.2 L'interception, la communication ou l'utilisation d'une communication électronique

Dans les environnements électroniques, l'interception, la communication ou l'utilisation d'une transmission électronique constitue également une situation pouvant donner ouverture à une atteinte à la vie privée[168]. Deux cas de figure doivent être principalement considérés, soit la réception non désirée d'informations ainsi que l'intrusion dans le courrier électronique. Fait à noter, il ne s'agit plus ici de traiter du problème des données personnelles, comme c'était le cas au chapitre I de la deuxième partie, mais bien d'envisager les problèmes pouvant découler du traitement accordé aux communications électroniques.

### 48.2.1 La réception non désirée d'informations

Il est logique de croire que, dans les environnements électroniques, il existe la possibilité qu'un usager soit victime d'une atteinte à sa vie privée en raison de la réception d'informations non désirées, phénomène que l'on identifie aussi par l'anglicisme “junk mail”. Par exemple, on peut penser que la réception d'informations à l'encontre du désir exprimé par un usager de ne pas recevoir de publicité, de la part d'une entreprise donnée, pourrait donner lieu à une violation de la vie privée de cet usager. Dans ce cas, l'atteinte ne serait pas provoquée par la révélation d'informations personnelles mais bien par l'intrusion dans l'intimité du courrier électronique.

Il y a lieu de supposer que, dans un tel cas, la gravité de l'atteinte serait

---

167 *Id.,* 211 et 212.

168 Voir généralement John M. WEGNER, *Home Interactive Media : An Analysis of Potential Abuses of Privacy,* (Winter 1985) 29 *Journal of Broadcasting & Electronic Media* 51-63. Sur l'interception dans les télécommunications voir Heather ROWE, and Geraldine PROULDER, *A Review of the Right to Privacy, with Emphasis on Interception of Communications (United Kingdom) (Telecommunications Special Issue),* (Nov. -Déc. 1993) *9 Computer Law & Practice* 224-233.

fonction du caractère intrusif du média impliqué et de la quantité d'information acheminée. En effet, comme le souligne Branscomb, les inconvénients à cet égard semblent plus grands dans les environnements électroniques que dans l'environnement physique. Ainsi, un usager peut perdre plusieurs minutes au télédéchargement d'une seule publicité tandis que le fait de jeter au panier une circulaire papier ne nécessite que quelques secondes[169].

Dans le même ordre d'idées, elle étoffe son point de vue en relatant les mésaventures de deux avocats associés, Canter et Siegel, qui avaient décidé de publiciser leurs activités juridiques via un envoi de messages massif sur Internet. À l'époque où ils posaient ce geste, la publicité commerciale était jugée inacceptable par les utilisateurs du réseau. Inondés de messages de reproches, les deux compères se sont vu couper l'accès au réseau par le gestionnaire de réseau. Pour Branscomb, il existe un fort potentiel pour que l'autoréglementation des usagers soit suffisante pour enrayer les problèmes dans de tels cas[170]. Cependant, le fait d'interdire la publicité dans les groupes de discussion lui semble raisonnable, parce que cela constitue une intrusion dans l'inviolabilité qui ne porte pas atteinte à la liberté d'expression commerciale, conformément à la jurisprudence américaine[171].

Également, il pourrait être possible d'aborder ce problème au moyen d'une analogie avec la réception de circulaires papier ou d'appels téléphoniques importuns. Dans ce dernier cas, il faut noter que la réglementation met en cause deux valeurs fondamentales. D'une part, toute réglementation qui viendrait restreindre la capacité des agents de télémarketing d'effectuer de la sollicitation téléphonique implique le premier amendement, donc la liberté d'expression. D'autre part, leur permettre de faire des appels sans restrictions semble constituer une

---

[169]Voir BRANSCOMB, *loc. cit.,* note 8, 1674.

[170]*Id.,* 1659.

[171]Voir *Rowan* v. *United States Post Office Department*, 397 U. S" 728, 735-38 (1970).

intrusion dans la vie privée[172]. L'interdiction totale de la sollicitation téléphonique est cependant considérée par les tribunaux américains comme une atteinte à la liberté d'expression commerciale[173]. Quoiqu'il en soit, nous croyons, outre la possibilité d'avoir recours à ces analogies, qu'il faudra se demander dans la phase subséquente si la réception d'informations non désirées a véritablement comme fondement le droit au respect de la vie privée ou si cette problématique ne devrait pas être envisagée d'un autre angle, celui de la protection du consommateur ou du harcèlement par exemple.

### 48.2.2 L'intrusion dans le courrier électronique

L'une des principales situations risquant de mettre en jeu la protection de la vie privée dans les environnements électroniques est assurément celle de l'intrusion dans le courrier électronique[174], plus particulièrement dans le

---

[172]DARMSTADTER, H. C., *Regulation of Unsollicited Telephone Calls : an Argument For a Liability Rule*, (1985) 5 *Computer Law Journal* 393. Voir également sur la question de la réception d'appels non désirés Mark S. NADEL, , *Rings of Privacy : Unsolicited Telephone Calls and the Right of Privacy*, (1986) IV *Yale Journal on Regulation* 99-129 ; Marilyn R. KAPLAN, *Commercial Speech and the Right to Privacy : Constitutional implications of Regulating Unsolicited Telephone Calls*, (1980) 15 *Columbia Journal of Law and Social Problems* 277.

[173]*Id.*,, 403.

[174]Vandagriff, dans un court texte, prétend que l'utilisation de l'encryptage et de la signature électronique permet de sécuriser les communications électroniques (email) d'une façon supérieure à la protection que peut offrir une lettre ou un fax. Voir à cet effet D. P., VANDAGRIFF, *Who's Been Reading Your E-Mail ? Two Easy-to-Use Tools Can Protect Privacy, Integrity of Documents*, (May 1995) 81 *ABA Journal* 98 ; n'ont pu être consultés parce que non encore disponibles Lois R.,WITT, *Terminally Nosy : Are Employers Free to Access Our Electronic Mail ?* , (1992) 96 *Dickinson Law Review* 545 ; Donald R. McCARTNEY, *Comment : Electronic Surveillance and the Resulting Loss of Privacy in the Workplace*, (1994) 62 *UMKC Law Review* 859 ; Nicolas TERRY, *The Monitoring of Electronic Mail in the Private Sector Workplace : An Electronic Assault on the Employee Privacy Rights*, (1991) 4 *Software Law Journal* 493.

cadre de la relation employeur-employé[175]. Aussi, il y a tout d'abord lieu de poser la problématique de façon globale pour ensuite identifier les rationalités sur lesquelles se fondent les employeurs pour revendiquer la possibilité de contrôler les communications électroniques de leurs employés[176]. En outre, il conviendra de dégager les valeurs antinomiques[177] en présence, notamment l'intérêt commercial légitime de l'employeur vis-à-vis de la vie privée et le droit à la confidentialité du courrier électronique de l'employé. Ainsi, comme le souligne Jennifer Griffin :

> *The scope of privacy protection that each legal mechanism provides varies. Therefore, the reasonableness of the employee's expectation of privacy differs, depending on whether the claim is for a common law, statutory, or constitutional violation of privacy. Ultimately, the resolution of the issue will require the balancing of the employer's interest in controlling employee conduct and use of company property against the employee's expectation of privacy in communicating without unwarranted surveillance by the employer*[178].

Avant toute chose, posons d'abord la problématique de façon générale en précisant les diverses circonstances où pourraient survenir une atteinte à la vie privée résultant d'une interception ou d'une intrusion d'une communication électronique. Selon Jennifer Griffin, il existerait cinq étapes

---

[175]Pour un exposé général sur la question de la vie privée dans le milieu de travail et sur la surveillance par des moyens électroniques voir David NEIL KING, *Privacy Issues in the Private-Sector Workplace : Protection from Electronic Surveillance and the Emerging Privacy Gap*, (1994) 67 *South California Law Review* 441.

[176]Il sera également intéressant, dans la phase subséquente, de s'intéresser aux pouvoirs normatifs qui autorisent les employeurs à agir ainsi. Voir à cet effet Andrée LAJOIE, *Pouvoir disciplinaire et tests de dépistage de drogues en milieu de travail : illégailté ou pluralisme*, Québec, Éditions Yvon Blais, 1995.

[177]Voir notamment à cet égard Jennifer GRIFFIN, *The Monitoring of Electronic Mail in the Private Sector Workplace : An Electronic Assault on Employee Privacy Rights*, (Oct. 1991) 4 *Software Law Journal* 493 et David NEIL KING, *loc. cit.*, note 174, 443.

[178]*Id.*, 502.

différentes où une communication électronique peut être interceptée par une autre personne que le destinataire initial. Premièrement, le contenu du message peut être dévoilé lorsque le tiers non-autorisé le voit sur l'écran de l'expéditeur ou lorsqu'il entre dans ses fichiers électroniques. Deuxièmement, une interception peut avoir lieu pendant la transmission. Troisièmement, une partie non-autorisée peut avoir accès au message par le biais de la boîte aux lettres du destinataire. Quatrièmement, l'interception peut survenir lorsque le message est imprimé. Cinquièmement, l'interception peut avoir lieu lorsque le message est entreposé dans le système[179]. Comme le souligne Griffin, les problèmes découlent généralement du fait que les opérateurs de courrier électronique copient et archivent les messages transmis dans le but de les conserver, au cas où certains messages importants seraient perdus ou effacés. Or ces copies peuvent contenir autant de matériel personnel que des messages liés au travail. Ainsi, un employeur n'effectuant que des contrôles de routine pourrait néanmoins en venir à lire des messages personnels[180].

La problématique étant posée de façon globale, il convient ensuite d'identifier quelques rationalités soutenant l'idée qu'un contrôle des messages électroniques par l'employeur est nécessaire. Ainsi, tout comme un employeur veut contrôler l'abus dans l'utilisation des appels interurbains par ses employés, un employeur voudra également s'assurer qu'il n'en existe pas dans l'utilisation du courrier électronique. Par exemple, à l'instar du téléphone, le courrier électronique pourrait être utilisé pour communiquer à des tiers des secrets commerciaux ou de l'information confidentielle concernant l'entreprise[181]. Une surveillance du courrier électronique des employés permettrait également à l'employeur de s'assurer leur compétitivité et leur loyauté[182]. En contrepartie, on oppose que les

---

179*Id.,* 500.

180Voir GRIFFIN, *loc. cit.,* note 176, 501.

181Voir à cet égard Charisse CASTAGNOLI, *Someone's Been Reading my E-mail ! Privacy Protection for Electronic Mail Users* in the US and the EC (Telecommunications Special Issue)" (Nov. -Déc. 1993) *9 Computer Law & Practice* 215.

182Voir Laurie THOMAS LEE, *Watch your E-mail ! Employee E-mail Monitoring and Privacy Law in the Age of the Electronic Sweatshop*, (1994) 28 *John Marshall Law Review* 139, 145.

employés ont un droit à la dignité humaine qui implique qu'ils n'aient pas à craindre de laisser leur droit à la vie privée au placard lorsqu'ils franchissent le seuil de leur lieu de travail[183].

Avant d'entrer plus directement au coeur du sujet et d'ainsi examiner plus attentivement les valeurs qui entrent en conflit, il convient de rappeler que, la majorité des textes portant sur l'intrusion dans le courrier électronique nous venant d'auteurs américains, il existe généralement quatre types de mécanismes législatifs propres à assurer la protection de la vie privée dans ce contexte en droit américain, soit la common law, le quatrième amendement, le droit étatique et le droit statutaire[184]. Aussi, ces différents mécanismes et la protection qu'ils offrent à la confidentialité des communications électroniques seront analysés dans l'ordre.

En ce qui a trait à la protection offerte par la common law, Jennifer Griffin souligne que, dans le contexte de l'emploi, l'attente légitime de vie privée d'une personne s'étend à sa personne, à ses objets personnels, à ses communications privées, à sa vie privée hors travail et à ses opinions. Un employeur met donc en cause la vie privée d'un employé lorsqu'il conduit secrètement une surveillance sur l'un de ces éléments[185]. Aussi, dans le milieu de travail, le *tort* d'intrusion dans l'intimité découle généralement de la méthode utilisée par l'employeur pour obtenir de l'information sur ses employés.

À ce jour, en common law, les tribunaux ne se sont penchés que sur les

---

[183]*Id.*, 144.

[184]Dans le contexte plus particulier du droit québécois, comme nous le verrons lors de la phase subséquente, il y aura lieu de considérer tout particulièrement les articles 35, 36(1) et (2) du *Code civil du Québec*, l'article 8 de la *Charte canadienne*, les articles 3 et 5 de la *Charte québécoise* ainsi que les articles 183 et suiv. du *Code criminel*.

[185]Voir GRIFFIN, *loc. cit.*, note 176, 503.

cas d'écoute électronique de conversations téléphoniques[186]. Une règle générale en découle, nous dit Griffin : écouter la conversation d'un employé constitue une intrusion dans ses affaires privées. Cependant, ce sera à l'employé de prouver l'écoute et l'employeur pourra s'exonérer en prouvant le consentement de la victime, qu'il soit exprès ou tacite, ou en invoquant un intérêt commercial légitime[187]. Aussi, comme le souligne Griffin, les tribunaux américains en appliquant la common law ne condamneront l'employeur que si sa conduite était "outrageusement intrusive". En prouvant que son activité de contrôle n'avait pour but que de s'assurer l'efficacité de l'employé, l'employeur s'en tirera à coup sûr.

Compte tenu des similarités existant entre le courrier électronique et le téléphone, Griffin souligne que les employeurs pourraient en déduire que l'attente de vie privée des usagers d'un service de courrier électronique est identique à celles des usagers d'un service téléphonique. Griffin estime cependant que, le courrier électronique permettant l'amalgame d'une plus grande quantité d'information et offrant plus de souplesse à l'employeur en ce qu'il lui permet d'avoir accès à des messages déjà entreposés, les tribunaux devraient distinguer les deux technologies et leur appliquer des standards différents. Sinon, la common law ne pourra pas offrir une protection suffisante aux employés utilisant le courrier électronique dans le contexte du travail[188].

Comme nous l'avons souligné, aux États-Unis, le quatrième amendement protège les employés du secteur public contre les intrusions

---

[186]Comme le E-mail est transmis par le biais d'un réseau de télécommunications, il pourrait, selon Droke, être assujetti aux dispositions régissant l'écoute électronique. En fait, selon lui, comme le message transmis l'est par le biais d'un clavier, il existe une similitude avec le télégraphe qui lui est inclus dans ces dispositions. Un tribunal pourrait donc décider, par analogie, d'appliquer une loi à une situation pour laquelle elle n'avait pas été envisagée. Voir notamment à cet égard Michael W. DROKE, *Private, Legislative and Judicial Options for Clarification of Employee Rights to the Content of their Electronic Mail Systems* (Hiver 1992) *32 Santa Clara Law Review* 171, 182 et suiv. Voir également WINTERS, *The New Privacy Interest : Electronic Mail in the Workplace* (Printemps 1993) *8 High Technology Law Journal* 197, 222 et suiv.

[187]Voir GRIFFIN, *loc. cit.,* note 176, 505. Voir Laurie Lee THOMAS, *loc. cit.,* note 181, 161 et suiv.

[188]*Id.,* 506 et suiv.

dans leur vie privée provoquées par une fouille ou une perquisition[189]. Cependant, cette protection ne couvre pas les employés du secteur privé qui font l'objet d'une fouille par leur employeur sans que l'État ne soit en cause[190]. Ainsi, une fouille sous le quatrième amendement devra rencontrer l'attente de vie privée légitime que l'on retrouve dans la société[191]. Traditionnellement, nous dit Winters, les employés ont joui d'une mince protection de la vie privée dans le milieu de travail[192], les tribunaux semblant vouloir favoriser les intérêts de l'employeur parce qu'il possède les prémisses où se déroule le travail ainsi que l'équipement de communication

---

[189]Voir le chapitre II, paragraphe I de la première partie.

[190]Voir Thomas R. GREENBERG, *Comment, E-Mail and Voice Mail : Employee Privacy and the Federal Wiretap Statute*, (1994) 44 *Am. U. L. Rev.* 219. Julia Turner BAUMHART, *The Employer's Right to Read Employee E-mail : Protecting Property or Personal Priving ?* (Automne 1992) *8 The Labor Lawyer* 923-948. Dans ce texte, Baumhart analyse sommairement la protection offerte par le quatrième amendement à la vie privée des employés de l'État. Voir également à cet égard Charisse CASTAGNOLI, *loc. cit.,* note 180, 217 ; Steven WINTERS, *loc. cit.,* note 185, 200 et suiv ; Michael W. DROKE, *loc. cit.,* note 185, 175.

[191]Voir notamment Steven WINTERS, *loc. cit.,* note 185, 200 et suiv. Pour sa part, Droke a tenté de définir quelle pourrait être une expectative de vie privée légitime dans le cas du courrier électronique. Pour lui, parce que ce type de technologie sous-tend dans la plupart des cas l'usage d'un code d'accès, plusieurs employés auront des attentes subjectives de vie privée lors de l' utilisation du système. Reste à savoir si cette expectative est raisonnable. Selon Droke, les tribunaux devront considérer une multitude de facteurs. Dans un premier temps, il devront prendre en considération le fait de savoir si l'employé a été avisé qu'une fouille aurait lieu et que l'employeur pouvait avoir accès au système. En second lieu, les tribunaux devront considérer le type de système impliqué. En effet, un système qui permet à l'employé de se créer un code d'identification personnel créera une expectative moins grande que le système où c'est l'employeur qui l'impose. L'environnement de travail risque aussi d'être un facteur déterminant. Ainsi, il est logique de croire qu'un employé qui travaille dans un secteur technologique de pointe risque de connaître les dangers relatifs à l'interception du courrier électronique. Son expectative de vie privée est donc moins grande que l'employé qui n'a aucune connaissance de ce genre de possibilité. Aussi, le degré d'expertise technique de l'employé pourrait également être considéré. Enfin, la Cour devra considérer le libellé de la politique que l'entreprise s'est donnée à l'égard de la confidentialité du courrier électronique, si une telle politique existe. Voir à cet égard Michael W. DROKE, *loc. cit.,* note 185.

[192]Voir au même effet Laurie Lee THOMAS, *loc. cit.,* note 181, 148 et 149.

par le biais desquelles sont conduites les affaires touchant l'activité de l'entreprise. En effet, on considère que l'employeur aurait de bonnes raisons de contrôler l'activité de ses employés, de façon à assurer la qualité et la quantité de travail produit de même que pour se prémunir contre les vols ou la fraude. Winters souligne, en outre, que même la Cour suprême a décidé de favoriser l'employeur dans la balance des intérêts parce que les intérêts de l'employeur du secteur public vis-à-vis un milieu de travail efficace supplantent les intérêts des employés à l'égard de la protection de leur vie privée[193].

Aussi, la question principale pour lui consiste à se demander si le développement des technologies de l'information a débalancé cet équilibre au point qu'il faille envisager de mieux protéger la vie privée des employés ? Pour Winters, la Cour suprême américaine a défini de façon incorrecte, depuis l'affaire Ortega[194], les valeurs de la société à l'égard de la vie privée dans le milieu de travail, essentiellement parce qu'elle s'est fondée sur une conception éculée de la vie privée et du milieu de travail, contraignant du même coup les tribunaux inférieurs à suivre cette fausse piste[195]. Cette décision, nous dit Winters, suggère que les employeurs ont un besoin illimité d'accéder aux bureaux de leurs employés afin de maintenir leur efficacité. Au contraire, il y aurait tout lieu de croire, nous dit-il, que c'est

---

[193]Voir WINTERS, *loc. cit.,* note 185, 201.

[194]Winters base son argumentation sur l'analyse de l'affaire O'Connor v. Ortega, où un médecin étant l'objet d'une enquête administrative a vu des employés de l'hopital entrer dans son bureau, fouiller ses tiroirs verrouillés et saisir certains de ses documents. Selon l'analyse de Winters, la décision rendue dans cette affaire suggère que les employés du secteur public n'ont pas ou peu de vie privée dans leur milieu de travail tant que la fouille ou la perquisition est reliée au travail. Cette décision implique que, à plus forte raison, les employés du secteur privé ne bénificient pas, eux non plus, de protection à cet égard. Par conséquent, suivant ce raisonnement, un employé du secteur public utilisant un service de courrier électronique ne serait pas protégé par le quatrième amendement si les intrusions dans sa vie privée étaient motivées par des raisons reliées au travail. Voir à cet égard l'analyse exhaustive de WINTERS, *id.,* 202 et suiv.

[195]Winters analyse en effet les décisions subséquentes des tribunaux inférieurs et conclut qu'elles n'offrent pas une protection adéquate de la vie privée des employés dans leur milieu de travail. Voir à cet effet WINTERS, *loc. cit.,* note 185, 211 et suiv, en particulier 219.

une protection accrue de la vie privée des employés qui, en envoyant un message positif à ces derniers, leur permettra de maintenir cette efficacité. Cela aurait comme effet, en bout de ligne, de fortifier la relation de confiance employeur-employé[196].

Au surplus, un contrôle illimité du courrier électronique pourrait, selon Winters, constituer un désavantage au niveau de la compétitivité de l'employeur. En effet, l'utilisation d'une technologie comme le courrier électronique rehaussant les standards de compétitivité et d'efficacité de l'entreprise, il y a un risque que la décision de contrôler assidûment ce type de communication ait un effet dissuasif sur l'utilisation de cet outil par les employés[197]. En outre, Winters souligne que la décision ci-dessus discutée ne tient pas compte de la dignité personnelle de l'employé. Généralement, en tant que société, on considère que chaque personne a besoin d'un degré minimal de dignité pour fonctionner avec équilibre. Pourquoi devrait-il en être autrement dans le milieu de travail[198] ? Il serait, somme toute, logique de croire que plus un employé passe de temps au travail, plus il a besoin d'intimité pour être efficace.

En droit étatique, il existe deux instruments susceptibles de garantir la protection de la vie privée des employées. D'une part, les diverses constitutions des États, de l'autre les différentes lois étatiques. Quant aux constitutions étatiques, Laurie Lee Thomas précise qu'elles ne prévoient, en majeure partie, aucune protection pour l'employé du secteur privé en milieu de travail. En fait, la constitution de l'État de la Californie est l'une des seules à protéger les employés du secteur privé, par le biais d'une disposition dont le libellé est similaire à celui du quatrième amendement[199]. Cependant, Thomas souligne qu'il est pour l'heure excessivement difficile de savoir comment les tribunaux de l'endroit balanceraient les intérêts de l'employeur vis-à-vis ceux des employés, dans un cas d'atteinte fondé sur l'intrusion dans le courrier électronique. Elle en conclut qu'il sera intéressant

---

196 *Id.,* 209.

197 *Id.,* 210. Voir au même effet GRIFFIN, *loc. cit.,* note 176, 495 et 522.

198 Voir WINTERS, *loc. cit.,* note 185, 211.

199 Voir à cet égard Laurie Lee THOMAS, *loc. cit.,* note 181, 147 et 149 et suiv.

de suivre le développement de la jurisprudence dans cet État[200].

En ce qui a trait à la protection de la confidentialité du courrier électronique par le biais de la législation étatique, Thomas nous dit que, de façon générale, les États ont incorporé les dispositions du *Electronic Communications Privacy Act of 1986* (ECPA) à leur droit interne[201]. Winters, qui a également envisagé cette problématique sous l'angle des lois étatiques, s'est quant à lui particulièrement penché sur l'affaire Shoars[202], où une employée poursuivait son superviseur en vertu des dispositions du Code pénal de la Californie relatifs à l'écoute électronique, pour avoir intercepté et lu son courrier électronique[203]. Pour Winters, la Cour a refusé la demande notamment parce que les mots magiques “courrier électronique” n'étaient pas inclus dans le libellé des dispositions sur lesquelles la poursuite s'appuyait. Il souligne également qu'il est inacceptable qu'un tribunal refuse de reconnaître la violation de la vie privée d'un employé à moins qu'une disposition législative expresse ne prohibe ce comportement. Pour lui, en rejetant la demande parce que l'action ne satisfait pas aux termes des dispositions actuelles de la loi, la Cour favorise les intérêts de l'employeur par défaut. Winters croit en effet que la Cour aurait à tout le moins dû refuser de rendre jugement, au motif que c'est au législateur d'étendre la protection de la vie privée au courrier électronique[204]. Quoiqu'il en soit, soulignons que la protection du courrier électronique par le biais des

---

[200] *Id.,* 150.

[201] *Id.,* 158. Nous analysons le ECPA dans les paragraphes suivants.

[202] Shoars v. Epson Am., Inc., No. BC007036 (Super. Ct. Cal filed Marc. 12, 1991). Voir également dans la même optique Bourke v. Nissan Motor Corp., No. YC 003979 (Super. Ct. Cal filed Jan. 4, 1991) ; Washington Fed'n of State Employees & Ron Collins v. Department of Labor & Indus. State of Wash., No. 90 2 02130 8 (Super. Ct. Wash. filed Sept. 10, 1990). Pour un commentaire sur ces décisions voir Jennifer J. GRIFFIN, *loc cit.,* note 176. Voir également Laurie THOMAS LEE, *loc. cit.,* note 181, 142.

[203] Pour une analyse détaillée de cette décision voir WINTERS, *loc. cit.,* note X, 185 et suiv. Voir également Michael W. DROKE, *loc. cit.,* note 185, 171, David Neil KING, *loc. cit.,* note 174, 468 et Michael TRAYNOR, *Computer E-Mail Privacy Issues Unresolved : How Extensively Can an Employer Monitor Messages ? (Legal Tech),* (31 janv. 1994) *The National Law Journal*, S2.

[204] Voir WINTERS, *loc. cit.,* note 185, 232 et 233.

constitutions étatiques n'a donné, jusqu'ici, que de maigres résultats.

Abordons maintenant la question de la protection du courrier électronique par le biais d'une disposition statutaire fédérale. Quel instrument peut donc garantir la confidentialité que les employés du secteur privé s'attendent à retrouver dans leurs communications électroniques[205] ? Le ECPA peut-il assurer cette protection ? Pour répondre à cette question, il convient d'abord de cerner globalement l'étendue de cet instrument législatif. Ruel Torrez Hernandez a, le premier, analysé comment le ECPA peut aider à solutionner les problèmes relatifs aux cas d'intrusion dans le courrier électronique[206]. Ayant examiné brièvement le champ d'application du ECPA, il souligne que cette loi protège divers types de communications électroniques, y compris celles entreposées après leur transmission, comme un courrier électronique conservé dans l'ordinateur du récepteur du message pour une consultation subséquente[207]. En vertu de cette loi, le fait d'intercepter intentionnellement une communication électronique constitue une infraction[208]. Est également illégal le fait, pour quiconque, de s'introduire dans un système sans y être autorisé et ainsi d'altérer, d'obtenir ou de révéler la teneur des communications entreposées[209]. De plus, le

---

[205] *Id.,* 222.

[206] Hernandez examine dans un premier temps la jurisprudence antérieure à l'adotion de cette loi ainsi que la loi sur l'écoute électronique pour en conclure que ces instruments n'offraient pas de protection adéquate au caractère privé du courrier électronique. Voir Ruel Torres HERNANDEZ, *ECPA and Online Computer Privacy*, 41 *Federal Communications Law Journal* 17, 25 et suiv. Une version antérieure de ce texte peut également être consultée, voir Ruel HERNANDEZ, *Computer Electronic Mail and Privacy*, disponible sur le serveur David Loundy présente également une analyse similaire des dispositions du ECPA dans David LOUNDY, *E-Law 3. 0 : Computer Information Systems Law and System Operator Liability Revisited*, gopher. eff. org (1995). Voir également Julia Turner BAUMHART, *loc. cit.,* note 189 ; Charisse CASTAGNOLI, *loc. cit.,* note 180 ; Steven WINTERS, *loc. cit.,* note 185.

[207] Voir au même effet Thomas GREENBERG, *loc. cit.,* note 189, 232 et suiv. Voir également Julia Turner BAUMHART, *loc. cit.,* note 189, 925 ; Jennifer GRIFFIN, *loc. cit.,* note 176, 515.

[208] Section 2511. Voir également Thomas GREENBERG, *loc. cit.,* note 189, 232 et suiv ; Julia Turner BAUMHART, *loc. cit*., note 189, 929 et suiv. et Michael W. DROKE, *loc. cit.,* note 185, 172.

[209] Section 2701. Voir également Thomas GREENBERG, *loc. cit.,* note 189, 234 et suiv ; Julia Turner BAUMHART, *loc. cit*., note189, 925 et suiv.

ECPA prévoit qu'aucune intrusion dans le courrier électronique ne peut être effectuée par les autorités sans un ordre de Cour. La charge de la preuve repose toutefois sur les épaules de l'utilisateur du système[210].

Sont également protégées, en vertu du ECPA, les communications électroniques qu'un utilisateur a cherché à tenir privées à l'aide des applications disponibles à cette fin dans le système. En contrepartie, il n'y aura pas de responsabilité pour l'accès non-autorisé à des fichiers qui ont été conçus pour être facilement accessibles par le grand public[211]. Également, le ECPA prohibe l'accès, l'interception ou la divulgation de communications électroniques en voie de transmission ou entreposées lorsque le réseau est configuré pour en faire respecter le caractère privé. Ne seraient cependant pas prohibés les mêmes gestes posés à l'égard d'un réseau accessible au grand public. Pour les commentateurs, cette loi protège donc spécifiquement contre l'intrusion de crackers ou d'employés non-autorisés[212].

Ces précisions étant apportées, il convient de se demander si le ECPA constitue une solution au problème que rencontre le droit américain vis-à-vis de la protection de la confidentialité du courrier électronique des employés du secteur privé. Le ECPA, qui offre une bonne protection contre l'intrusion de crackers ou d'employés non-autorisés, offre-t-il une protection similaire aux employés à l'égard de l'intrusion de leur employeur ?

Lorsqu'un message est en phase de transmission, il est assujetti aux dispositions de la section 2511 qui prohibe, de façon générale, l'interception

---

[210]Voir Ruel HERNANDEZ, *ECPA and Online Computer Privacy*, 29, 30 et 31 et David LOUNDY, *loc. cit.*, note 205.

[211]Voir au même effet Michael W. DROKE, *loc. cit.*, note 185, 180. Selon Hernandez, il y a au moins deux façons d'échapper à la couverture de ces dispositions de la loi. Premièrement, ne pas offrir de systèmes e-mail privés. Pour ce faire, le gestionnaire de réseau n'a qu'à décréter, par le biais d'un "disclaimer", que tout le matériel du système est accessible au public en général. Certains seraient même allés jusqu'à avertir leurs usagers que leurs systèmes n'étaient pas à l'abri des "crackers". L'autre façon de contourner la loi, tout en prohibant l'accès au courrier électronique privé, serait d'encoder les messages, ce qui les rendrait indéchiffrables pour les autorités qui voudraient en prendre connaissance. Voir HERNANDEZ, *loc. cit.*, note 205, 32.

[212]*Id.*, 39. Voir au même effet Julia Turner BAUMHART, *loc. cit.*, note 189, 923. Voir également DROKE, *loc. cit.*, note 185, 183.

d'une communication électronique mais prévoit qu'il n'est pas illégal pour un employé ou un opérateur du réseau impliqué dans la transmission d'une communication, d'intercepter, de dévoiler ou d'utiliser cette dernière afin d'assurer le service dans le cours normal de son travail ou de protéger le droit de propriété de l'employeur à l'égard du système[213]. Lorsque le message est arrivé à destination et entreposé, il est soumis aux dispositions de la section 2701[214]. Sous cette section, un employeur qui exploite un service de messagerie électronique peut intentionnellement examiner tout ce qui circule sur son réseau, que ce soit pour un contrôle de qualité ou non. De plus, une entreprise pourrait même, en vertu de la section 2702(b)(5),

---

[213]*Id.,* 39 et suiv. Voir BAUMHART, *loc. cit.,* note 189, 931 ; DROKE, *loc. cit.,* note 1856, 181 et THOMAS, *loc. cit.,* note 181, 156. . Voir également Thomas GREENBERG, *loc. cit.,* note 189, 236 qui constate que *: Congress failure to limit routine observation and random monitoring with respect to electronic communications systems may have been intentional. This variation in treatment appears predicated on the belief that electronic communications services had a greater need for such observation and monitoring as a means to properly route message traffic. Thus, section 2511 (2)(a)(i) leaves E-mail messages susceptible to random interception, and accordingly more vulnerable to privacy invasions than voice mail messages.* Voir également David LOUNDY, *loc. cit*., note 205, note 304. Loundy ajoute, par la même occasion, que la section 2701 permet aux autorités de demander à un opérateur de réseau, avant l'obtention de mandat de perquisition, de faire des copies des données entreposées, de sorte que l'information litigieuse pourra être conservée.

[214]Voir notamment GREENBERG, *loc. cit.,* note 189, 248.

divulguer le contenu des communications électroniques de son réseau afin de protéger ses intérêts commerciaux[215].

Cette dualité dans le traitement de la communication électronique, c'est-à-dire des limitations plus strictes lorsque le message est en voie de transmission, moins strictes lorsqu'il est entreposé, crée pour Greenberg une situation irrationnelle. Ayant analysé la jurisprudence relative à l'interception d'appels téléphoniques sous le ECPA, Greenberg fait ressortir que les employés n'ont pas automatiquement d'attente légitime de vie privée lorsqu'ils utilisent le réseau téléphonique de l'employeur[216]. Cependant, le

---

[215]Voir au même effet GRIFFIN, *loc. cit.,* note 176, 517. Hernandez, analysant les faits d'une affaire réglée hors cour, Thomson v. Predaina, précise cependant que, dans une situation impliquant des communications entreposées, un gestionnaire de réseau qui, ayant récupéré un message privé dans le système le rendrait ensuite public, devrait être tenu responsable en vertu du Titre II du ECPA et du *Cable Communications Policy Act*. Rappelons que dans cette affaire, la demanderesse Thomson poursuivait Predaina en dommages pour une somme de 112, 250$. Selon la plainte, Thomson échangeait de la correspondance privée (e-mail) sur le "BBS" opéré par Predaina. Après avoir lu les messages reçus, elle les effaçait régulièrement. Predeina aurait semble-t-il récupéré ces messages effaçés et les aurait postés sur le réseau, les rendant du même coup publics. La demanderesse Thomson fonde d'abord son action sur le Titre I du ECPA (*Wire and Electronic Communications Interception and Interception of Oral Communications*). Sous cette section, toute personne dont une communication électronique a été interceptée, divulguée ou utilisée en violation de ce chapitre a un recours civil où il peut exiger tout remède approprié contre l'auteur de la violation. La seconde cause d'action de la demanderesse est fondée sur le Titre II du ECPA (*Stored Wire and Electronic Communications and Transactional Record Access*). Une violation de cette section survient lorsque quelqu'un accède intentionnellement et sans autorisation à une communication privée entreposée dans un système ou circulant dans le réseau. Constitue également une violation de cette section le fait de divulguer, en connaissance de cause, le contenu d'une telle communication à quelqu'un d'autre que son destinataire. Le dernier motif de poursuite de la demanderesse Thomson était fondé sur le Titre VII du "Cable Communications Policy Act of 1984". Cette disposition concerne la publication ou l'utilisation non-autorisée d'une communication. Selon Hernandez, cette section est construite de façon à réguler la conduite des personnes qui ont la charge de faciliter la réception des transmissions. À ce titre, Hernandez est d'avis que cette loi s'applique à un opérateur de "BBS". Voir Ruel T. HERNANDEZ, *loc. cit.*, note 205, 37 et suiv. Voir également sur l'affaire *Predina* Edward M. Di CATO, *Operator Liability Associated with Maintaining a Computer Bulletin Board* (Oct. 1990) 4 *Software Law Journal* 147, 151.

[216]Voir également Michael TRAYNOR, *loc. cit.,* note 202, S2.

contrôle par l'employeur prévu à la section 2511 ne peut s'exercer que dans un cadre précis qui, nous dit Greenberg, protège les intérêts des employés à la vie privée[217]. Par analogie, Greenberg croit que ces approches devraient être appliquées aux communications électroniques. Ainsi, sous la section 2511, l'employeur ne pourrait exercer son contrôle que dans des circonstances précises. En contrepartie, cependant, la section 2701 donne carte blanche au fournisseur du service de communications électroniques pour contrôler les communications entreposées. Pour Greenberg, le fournisseur de services, dans ce contexte, sera presqu'assurément l'employeur. C'est donc dire que ce dernier pourrait échapper à la responsabilité de la section 2511 en attendant qu'une communication soit entreposée pour en prendre connaissance ce qui, pour lui, constitue une protection inacceptable de l'attente légitime de vie privée des employés du secteur privé[218].

N'étant pas protégés de façon adéquate par le ECPA[219], les employés du secteur privé devront, nous dit Greenberg, s'appuyer sur d'autres loi fédérales, étatiques ou sur la common law pour assurer leur droit à la confidentialité des communications électroniques. Il y aurait donc lieu, dans ce contexte, de balancer les intérêts des employeurs à l'égard d'informations

---

[217]En effet, deux approches ont été retenues par les tribunaux. Dans la première, fondée sur le contenu de la communication, l'employeur ne peut assurer un contrôle sur cette communication que pour s'assurer qu'elle est personnelle et non reliée à ses intérêts commerciaux. Dans la deuxième, les tribunaux se demandent si l'employeur a un motif corporatif légitime de contrôler les communications de ses employés. Voir GREENBERG, *loc. cit.,* note 189, 247. Voir au même effet GRIFFIN, *loc. cit.,* note 176, 516. Voir également Julia Turner BAUMHART, *loc. cit.,* note 189, 933. Baumhart souligne qu'un employeur désirant détecter un abus dans le système pourrait le faire adéquatement en contrôlant seulement l'information transactionnelle, i. e. l'expéditeur, le récepteur et la durée de la transmission. Des incongruités dans la longueur, le nombre ou les parties impliquées pourraient alerter l'employeur et lui permettre d'identifier quelles communications ont besoin d'un contrôle plus précis.

[218]Voir GREENBERG, *loc. cit.,* note 189, 249. Hernandez en arrive aux mêmes conclusions, dans un texte cependant moins limpide que Greenberg. Voir également GRIFFIN, *loc. cit.,* note 176, 518.

[219]Pour sa part, Griffin conclut qu'aucun instrument ne protège valablement le droit à la confidentialité du courrier électronique des employés dans le milieu de travail. Voir GRIFFIN, *loc. cit.,* note 176, 526 et 527.

touchant la conduite et la performance de leurs employés avec les attentes raisonnables de vie privée de ces derniers. De plus, Greenberg estime que le ECPA devrait être amendé de façon à garantir une protection adéquate aux employés du secteur privé[220].

Pour Julia Baumhart cependant, adopter aveuglément la position voulant que le ECPA n'impose pas de limitations d'accès aux employeurs qui possèdent leurs propres systèmes équivaudrait à ignorer l'intention du Congrès lors de son adoption, qui était d'introduire une parité dans la protection des communications personnelles, sans égard au type de médium utilisé dans la transmission[221]. De plus, il ne lui apparaît pas évident que tous les employeurs pourront bénéficier de cette exception, plusieurs employeurs souscrivant à un service de courrier électronique au lieu d'en être possesseurs[222]. Aussi, pour Baumhart, les compagnies qui croient que le Congrès n'a pas voulu assujettir au ECPA les entreprises dans leur rôle d'employeurs le font à leur péril. Pour elle l'employeur qui accède aux messages entreposés, seulement dans le but de restaurer un message perdu, n'a probablement pas à s'inquiéter autant que celui qui y accède pour d'autres raisons que celles reliées à l'entretien du système. C'est pourquoi, selon elle, l'employeur prudent tiendra compte de l'attente de vie privée des employés jugée raisonnable dans d'autres contextes[223].

---

[220]Voir GREENBERG, *loc cit.,* note 189, 250, 251, 252.

[221]Voir Julia Turner BAUMHART, *loc. cit.,* note 189, 926.

[222]*Id.,* 927. Voir au même effet WINTERS, *loc. cit.,* note 185, 230.

[223]Voir BAUMHART, *loc. cit.,* note 189, 928 et 929.

Quoiqu'il en soit, tant Greenberg que Baumhart s'entendent pour dire que les employeurs devraient opter pour une solution contractuelle du conflit[224]. Pour ce faire, Greenberg propose que l'employeur distribue aux employés une politique claire concernant le courrier électronique, indiquant notamment qu'il pourra y avoir accès sans notifier l'employé. Il devrait également informer les employés que le service de courrier électronique doit être utilisé dans le cadre du travail et que les messages entreposés dans le système sont considérés appartenir à l'entreprise. L'entreprise devrait aussi donner aux employés les motifs raisonnables qui pourraient la pousser à fouiller leur courrier électronique, de façon à ce que la légitimité de cette démarche ne fasse aucun doute. La connaissance de cette politique par les employés réduira considérablement leurs attentes en matière de confidentialité. On peut cependant se demander si une approche fondée sur le consentement[225] n'isolera pas définitivement les employeurs de toute responsabilité, compte tenu du fait que l'employé a de moins en moins de choix quant à ses condition de travail dans le contexte économique actuel[226]. Plus globalement, il y a peut-être également lieu de se demander si l'approche contractuelle n'est pas simplement le moyen, pour les employeurs, de légitimer le contrôle patronal.

À l'instar de Greenberg, Baumhart croit que les employeurs désirant assurer un contrôle sur le courrier électronique devraient faire circuler dans leur personnel une politique claire précisant dans quelles circonstances et pour quelles raisons des contrôles sont nécessaires. Ainsi, l'employeur qui aura précisé à ses employés que le courrier électronique ne doit pas être utilisé pour des conversations personnelles parce que cela entraîne des dépenses indues et qui aura spécifié qu'il entend exercer un contrôle sur ce courrier pour éviter les abus, atteint deux objectifs fondamentaux.

---

[224]Pour sa part, Droke a rédigé une politique type qui va dans le même sens que les remarques de Baumhart et de Greenberg. Voir à cet effet DROKE, *loc. cit.*, note 185, 191. Voir également CASTAGNOLI, *loc. cit.*, note 180, 221.

[225]Baumhart, rappelant que le ECPA reconnaît le consentement, tant exprès que tacite, comme une exception aux prohibitions vis-à-vis de l'accès et de l'interception des communications électroniques, pose que l'employeur pourrait légitimer dans certains cas le contrôle du courrier électronique en donnant un avis à cet effet aux employés. Voir au même effet GRIFFIN, *loc. cit.*, note 176, 516, 518.

[226]Voir pour une opinion similaire GRIFFIN, *loc. cit.*, note 176, 525.

Premièrement, les employés seront moins enclins à abuser du système en sachant qu'il est contrôlé. Deuxièmement, l'employeur a montré au tribunaux qu'il veut préserver sa propriété plutôt que d'empiéter sur la vie privée de ses employés[227].

Cette approche contractuelle semble rejoindre celle de Trotter Hardy. En effet, pour lui, la question du caractère privé du courrier électronique doit être posée de la façon suivante : les employés ont-ils un droit à la vie privée relativement à leur courrier électronique ? Les employés devraient-ils pouvoir envoyer des notes à d'autres employés ou à des personnes hors de l'entreprise sans avoir à s'inquiéter que leur messages seront lus par un superviseur ? En contrepartie, les employeurs devraient-ils avoir un droit de savoir si leurs employés révèlent des secrets industriels par cette voie ? Dans ce contexte, on peut se demander si on devrait permettre à un employeur, par exemple un administrateur de réseau, de vérifier le courrier électronique de tiers qui pourrait être dommageable à ses intérêts[228].

Pour Hardy, il apparaît évident que l'employeur et l'employé se retrouvent déjà dans une relation contractuelle, ce qui lui fait mentionner que le coût additionnel entraîné par la négociation d'une entente entre eux sur cette question serait minimal. Il souligne également que le degré de désir de la part des employés et des employeurs relativement à une politique à ce sujet risque de varier d'une entreprise à l'autre. Par exemple, certaines entreprises de haute technologie voudront se prémunir contre le dévoilement de secrets commerciaux en ayant accès au courrier électronique de leurs employés alors que pour d'autres, cela ne paraîtra pas nécessaire[229]. En ce sens, une approche contractuelle serait beaucoup mieux adaptée aux besoins de tous.

Examinant les approches qui permettraient de résoudre cette question, il mentionne qu'une loi, la “Privacy for Consumers and Workers Act”, privilégiant la résolution du conflit par une approche uniforme a été

---

[227]Voir BAUMHART, *loc. cit.,* note 189, 934, 935 et 947.

[228]Trotter HARDY, *loc. cit.,* note 66, 1008 et 1009.

[229]*Id.*, 1032.

présentée au Congrès[230]. Hardy évoque également la possibilité que les lois étatiques sur l'écoute électronique puissent être utilisées, soulignant au passage que des pressions s'exercent au Canada afin qu'une loi protégeant la vie privée soit adoptée. Ayant évoqué ces diverses possibilités, Hardy en vient à la conclusion que les coûts minimes d'une solution contractuelle et les besoins variables des entreprises et des employés quant à la protection du courrier électronique montrent qu'une réponse législative uniforme ne serait pas appropriée dans les circonstances. Au contraire dit-il, cette situation présente tous les signes permettant de croire à la réussite d'une solution contractuelle. Dans les faits, cette entente pourrait prendre la forme d'un code de conduite adopté par l'entreprise et remis aux employés. De tels codes existent d'ailleurs, selon Hardy, ce qui prouverait que la solution contractuelle est déjà appliquée en pratique[231].

Outre l'approche contractuelle consistant en l'adoption, par l'entreprise, d'une politique de confidentialité à l'égard du courrier électronique, Michael Droke insiste sur l'importance d'instaurer des contrôles physiques, comme des mots de passe additionnels ainsi que des codes d'accès variables, pour empêcher l'accès non-autorisé au système. L'entreprise devrait également instituer un contrôle administratif sur les opérations du réseau, qui prédéterminera les personnes en charge de policer le système et les méthodes acceptables pour ce faire[232]. Il propose également une autre approche qui permettrait, selon lui, de mieux protéger la confidentialité du courrier électronique. Il ne s'agirait, en fait, que de renverser l'actuelle charge de la preuve et de laisser à l'employeur le soin de prouver que le système n'était pas confidentiel. En d'autres termes, on tiendrait pour acquis que le système était confidentiel, jusqu'à preuve du contraire[233].

---

[230]Aux derniènes nouvelles, elle n'avait pas encore été adoptée. Cette loi paraît néanmoins être, pour certains commentateurs, une réponse efficace à la problématique du courrier électronique dans le milieu de travail. Voir à cet égard David Neil KING, *loc. cit.,* note 174, 472 et suiv. ; Michael TRAYNOR, *loc. cit.,* note 202, S3 ; *Contra* Laurie Lee THOMAS, *loc. cit.,* note 181, 167, 170 et suiv.

[231]Trotter HARDY, *loc. cit.,* note 66.

[232]Voir DROKE, *loc. cit.,* note 185, 187 et suiv.

[233]*Id.,* 193. Droke suggère aussi l'adoption d'une nouvelle disposition législative, qu'il a lui-même rédigée. Voir à cet effet *id.,* 195.

Pour Laurie Lee Thomas, le moyen d'arriver à balancer équitablement les intérêts des employeurs et ceux des employés pourrait être l'adoption d'une loi fédérale souple, visant à prévenir les intrusions de l'employeur dans la vie privée de son employé. Un tel instrument pourrait permettre un contrôle "raisonnable" par l'employeur qui aurait un intérêt commercial légitime. Pour ce faire, l'employeur devrait obligatoirement utiliser le moyen de contrôle le moins intrusif possible, tout en limitant au maximum l'accès, l'utilisation ainsi que la divulgation des informations obtenues lors de la surveillance. De plus, l'employeur aurait l'obligation de notifier l'employé du type de contrôle qu'il entend exercer et de l'utilité de celui-ci. Cette loi pourrait également obliger l'employeur à adopter une politique de contrôle répondant à certains objectifs pré-établis, comme l'identification des raisons acceptables d'exercer le contrôle ou encore la fourniture de moyens de sécurité propres à prévenir l'accès non-autorisé[234].

Pour sa part, Charisse Castagnoli envisage la résolution du conflit d'une façon différente. Après avoir constaté que le droit américain offre peu de garanties à l'égard de la protection du courrier électronique, elle pose que le courrier électronique répond aux critères relatifs à la cueillette, au traitement et à l'entreposage des données personnelles de la Directive de la Convention européenne[235]. Pour elle, si le courrier électronique est assujetti à la Directive, il devra donc être protégé de façon conforme à cet instrument[236]. Considérant le projet de directive supérieur à l'approche américaine, Castagnoli estime que le gouvernement américain devrait s'en inspirer. À l'instar de Greenberg, de Baumhart et de Hardy, elle prône également l'établissement de politiques par l'employeur visant à encadrer le droit de contrôle de celui-ci sur le courrier électronique de ses

---

[234]Pour plus de précisions sur ces objectifs et la solution de Thomas lire Laurie Lee THOMAS, *loc. cit.,* note 181, 172 et suiv.

[235]Voir Charisse CASTAGNOLI, *loc. cit.,* note 180, 218 et 219. Mme Castagnoli croit en effet que le courrier électronique correspond à la définition de données personnelles, qu'il est rattachable à une personne, qu'il fait l'objet d'un traitement au même titre qu'une donnée personnelle et qu'il n'est pas spécifiquement exclu du terme de la Directive.

[236]Castagnoli reprend dans son texte les divers points saillants de la Directive, dont le principe de l'équivalence, et les transpose au courrier électronique. Voir à cet effet *id.,* 219 et suiv. Pour une analyse en profondeur de ces dispositions voir Karim BENYEKHLEF, *loc. cit.,* note 111.

employés”[237].

## 49. Conclusion

Comme nous avons tenté de le démontrer dans ce texte, la protection de la vie privée et des renseignements personnels dans les environnements électroniques suscite maintes préoccupations auprès des usagers potentiels des inforoutes, que l'on pense seulement à la revendication d'un droit de contrôle sur l'information et d'un droit à l'anonymat. Surgissent également diverses interrogations quant aux possibilités décuplées d'intrusion dans l'intimité qu'offre l'espace cybernétique par le biais, notamment, d'activités telles la compilation de données personnelles aux fins d'établir un profil de consommation ou encore, plus simplement, d'intrusions dans le courrier électronique. À cet égard, l'exercice d'identification des enjeux et des problématiques auquel nous nous sommes livrés dans cette première phase de notre étude est fort riche d'enseignements et de constats.

Au-delà cet énoncé général, qui pourrait être qualifié de platonique par certains, nous en convenons, il ne nous paraît cependant pas possible, pour l'heure, de tirer des conclusions plus approfondies de l'exégèse que nous avons compilée. Cette première démarche accomplie et l'état des questions substantiel dressé, il conviendrait maintenant de s'attacher à dégager les rationalités que sous-tendent les normativités dégagées dans le cadre de la présente étude. À cet égard, il serait trop facile de se contenter de comparer les lois québécoises aux solutions relevées et de combler les vides se présentant ici et là.

En effet, pour assurer l'adéquation du cadre juridique et réglementaire québécois aux environnements électroniques, notamment dans le cas de la protection de la vie privée et des renseignements personnels, il ne suffira pas de se demander si telle ou telle loi doit être amendée et, dans l'affirmative, de quelle façon. L'approche qu'il convient d'adopter consiste plutôt à s'interroger sur le fondement même du pouvoir normatif. Concrètement, cela implique qu'il faudra par exemple vérifier si les rationalités à l'appui de la protection de l'anonymat en droit québécois sont fondées sur des préceptes qui s'avèrent toujours pertinents dans le cadre d'un

---

[237] Voir CASTAGNOLI, *loc. cit.,* note 180, 221.

environnement dématérialisé. Ces rationalités identifiées, il s'agira ensuite de se demander quelle est la meilleure façon, pour le pouvoir normatif, de protéger les droits et valeurs en cause. Il pourra y avoir à cet effet une pluralité de voies possibles, par exemple l'adoption de nouvelles lois, le recours à l'auto-réglementation, à une approche contractuelle ou même à des représentations auprès d'instances internationales. Quoiqu'il en soit, les fruits de cette première étude devraient nous permettre d'atteindre cet objectif dans le cadre des phases subséquentes de la recherche. En fait, une seconde étape, la phase II du mandat du Groupe de recherche sur le cadre juridique et réglementaire des environnements électroniques est déjà en cours et devrait d'ailleurs faire l'objet d'une publication ultérieure. Ce n'est que lorsque ce travail d'analyse, d'adaptation et de transposition juridique aura été accompli qu'il deviendra possible de tirer véritablement des conclusions éclairées.

# LE DROIT D'AUTEUR DANS LE CONTEXTE DU DEVELOPPEMENT DE LA "SOCIETE DE L'INFORMATION"[1]

**Valérie CASTILLE**

**Assistante à l' Université de Gand Droit des médias - Droit d'auteur**

> *La Société de l'Information constitue dès à présent une réalité dans la mesure où les réseaux existants sont déjà utilisés à des fins commerciales, éducatives et de recherche, grâce à l'utilisation des technologies de communication numériques. Par ailleurs, il importe de signaler que ces réseaux ont évolué essentiellement en fonction de systèmes de normes de communication ouverts et que le contenu des échanges qui ont lieu sur ces réseaux n'est actuellement protégé qu'en partie par les droits de propriété intellectuelle*[2].

Avant d'analyser quelques grandes questions que soulève actuellement l'application de la protection du droit d'auteur dans la société de l'information, nous souhaitons préciser que cette analyse a seulement pour but de tracer les quelques grands principes du droit d'auteur à respecter sur des oeuvres informatiques. Nous ne prétendons nullement pouvoir dresser un tableau complet de toutes les préoccupations suscitées par le développement de la "Société de l'Information".

La question cruciale que nous tenterons de résoudre est celle de savoir si les oeuvres informatiques peuvent bénéficier de la protection de la loi relative au droit d'auteur et aux droits voisins.

---

[1]Ce texte contient les développements d'un exposé fait à l'Université de Louvain-la-Leuve le 20 mars 1996.

[2]Livre Vert de la Commission européenne, *Le droit d'auteur et les droits voisins dans la Société de l'Information*, 19 juillet 1995, COM (95) 382 final, p. 7.

Dans l'affirmative, le système actuel permet-il suffisamment la protection des oeuvres informatiques ou faut-il prévoir l'introduction de nouveaux droits (exclusifs) ? Il va de soi que cette question cruciale se pose non seulement au niveau national, mais également au niveau communautaire ainsi qu'au niveau international.

## 50. Le principe de la territorialité de la protection par le droit d'auteur

### 50.1 Le principe de territorialité

En contraste avec le caractère global, mondial, voire universel du Réseau des réseaux Internet, la protection du droit d'auteur reste - tout comme les autres droits intellectuels - en principe confinée par ses frontières territoriales.

### 50.2 Nécessité d'harmonisation internationale du droit d'auteur au-delà des frontières nationales

Déjà au siècle passé, le principe de territorialité avait suscité de nombreux problèmes, il s'était avéré nécessaire de procéder à l'harmonisation de certains principes relatifs au droit d'auteur à l'échelle internationale.

Au niveau international il existe déjà depuis 1886 la *Convention de Berne pour la protection des oeuvres littéraires et artistiques*. Cette Convention de Berne a pour mérite d'avoir instauré la règle du traitement national. L'application de cette règle implique que la protection du droit d'auteur qui est accordée aux nationaux, est également accordée aux ressortissants de pays tiers qui font parties de la Convention de Berne.

Depuis 1952 il existe également une Convention Universelle sur le droit d'auteur[3] et depuis 1961 une Convention de Rome[4] établissant pour la première fois une protection des droits voisins.

Nous terminons en citant le récent *Accord relatif aux aspects des droits de propriété intellectuelle qui touchent au commerce, y compris le commerce des marchandises de contrefaçon* (ADPIC)[5]. L'accord ADPIC reprend entièrement les dispositions de la Convention de Berne pour les droits d'auteur et partiellement les dispositions de la Convention de Rome en ce qui concerne les droits voisins.

### 50.3 Nécessité d'harmonisation européenne du droit d'auteur au-delà des frontières nationales

Comme nous pouvons l'apprendre quotidiennement par les journaux, il règne au niveau européen un souci permanent de minimaliser les disparités dans les législations des différents Etats membres, et ceci afin de supprimer les entraves à la libre circulation des personnes, services, marchandises et capitaux du “Marché intérieur”.

Au niveau communautaire un certain degré d'harmonisation de protection du droit d'auteur et des droits voisins a été réalisé ces dernières

---

[3]Convention Universelle sur le droit d'auteur et Protocoles annexes, signés à Genève le 6 septembre 1952 et approuvés par la loi du 20 avril 1960, M. B., 30 août 1952.

[4]Convention internationale sur la protection des artistes-interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion du 26 octobre 1961. Cette Convention n'a toujours pas été ratifiée par l'Etat belge.

[5]MAIER, P., *Le processus de négociation de l'accord TRIPS* et FRANCON, A., *Les droits d'auteur et les droits voisins : principes substantiels,* dans red. DOUTRELEPONT, C., L'Europe et les enjeux du GATT dans le domaine de l'audiovisuel., Bruylant, Bruxelles, 1994, 141 - 147 et 149 - 153.

GAUBIAC, Y., *Une dimension internationale nouvelle du droit d'auteur : L'accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce de l'accord de Marrakech instituant l'organisation mondiale du commerce*", RIDA, 1995, n° 166, p. 3 - 55 ;

années, grâce à l'adoption de 5 directives européennes[6], la dernière directive du 11 mars 1996 concerne la protection juridique des bases de données[7], conçue par souci d'un régime juridique des bases de données trop disparates, voire insuffisant dans les différents Etats membres.

### 50.4 Nécessité d'harmonisation accrue du droit d'auteur dans le cadre du développement de la "Société de l'Information"

En ce qui concerne ce débat au niveau communautaire, nous soulignons l'existence d'un Livre Vert[8] de la Commission européenne du 19 juillet 1995 concernant *Le droit d'auteur et les droits voisins dans la Société de l'Information*. Ce Livre Vert[9] de la Commission européenne a pour mérite de poser des questions pertinentes concernant des aspects particuliers de la protection du droit d'auteur et des droits voisins. Grâce à un questionnaire détaillé qui fait partie du Livre Vert, les milieux concernés ont été invités

---

[6]Directive 91/250/CEE du Conseil du 14 mai 1991 sur la protection juridique des programmes d'ordinateur, J. O. C. E., 17 mai 1991, L 122/42 ;

Directive 92/100/CEE du Conseil du 19 novembre 1992 relative au droit de location et de prêt et à certains droits voisins du droit d'auteur dans le domaine de la propriété intellectuelle, J. O. C. E., 27 novembre 1992, L 346/61 ;

Directive 93/83/CEE du Conseil du 27 septembre 1993 relative à la coordination de certaines règles du droit d'auteur et des droits voisins du droit d'auteur applicables à la radiodiffusion par satellite et la retransmission par câble, J. O. C. E., 6 octobre 1993, L 248/15 ;

Directive 93/98/CEE du Conseil du 29 octobre 1993 relative à l'harmonisation de la durée de protection du droit d'auteur et de certains droits voisins, J. O. C. E., 24 novembre 1993, L 290/9 ;

[7]Directive 96/9/CE du Conseil du 11 mars 1996 concernant la protection juridique des bases de données, J. O. C. E., 27 mars 1996, n° L 77/20 ;

[8]Livre Vert de la Commission européenne, *Le droit d'auteur et les droits voisins dans la Société de l'Information*, 19 juillet 1995, COM (95) 382 final.

[9]Pour une analyse critique : VISSER, D., *Groen papier over auteursrecht van E4@DG15. cec. be. Het Groenboek Auteursrecht en naburige rechten in de Informatie- maatschappij,* Mediaforum, 1995, n) 10, 118 - 121.

par la Commission européenne à exprimer leur point de vue et aider à élaborer un cadre juridique - harmonisé au niveau communautaire - de protection juridique et technique du droit d'auteur et des droits voisins des oeuvres informatiques.

La question primordiale posée dans le Livre Vert est de savoir si les effets de la technique numérique occasionneront une “simple évolution” ou plutôt une “révolution” dans le domaine du droit d'auteur et des droits voisins.

### 50.5 “Droit d'auteur” versus “copyright” ?

Par souci d'être complet, nous nous devons de signaler que les débats menés (aux niveaux international et communautaire) sont alimentés par l'opposition “droit d'auteur” et “copyright”. N'entrant pas dans notre propos d'approfondir[10] cette opposition vieille comme le monde, il nous faut souligner que l'existence même de ces deux régimes n'est pas de nature à faciliter une harmonisation. Traditionnellement, le régime du droit d'auteur place l'auteur (droit de la personnalité) au centre de la protection, alors que le régime du copyright[11] se focalise[12] sur les aspects plus mercantiles.

---

[10]Pour ceci nous renvoyons à l'ouvrage de STROWEL, A., *Droit d'auteur et copyright. Divergences et convergences. Etude de droit comparé*, Bruylant, 1993, 722 pages.

[11]Pour une analyse "copyright" du problème qui nous préoccupe : JONES, S., *Multimedia and the superhighway : exploring the rights minefield*, Communications Law, Vol. 1, n°1, 1996, 29 - 37.

[12]Pour avoir une idée plus précise des problèmes actuels du copyright (et leurs divergences et convergences avec le système du droit d'auteur), nous renvoyons à GURNSEY, J., *Copyright Theft*., Aslib Gower, Hampshire, 1995, 196 p.

## 51. Principes généraux de la loi relative au droit d'auteur

### 51.1 Introduction

La nouvelle loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins[13], est (pour la majeure partie) entrée en vigueur le 1er août 1994. Elle remplace l'ancienne loi du 22 mars 1886 sur le droit d'auteur[14]. La date récente de cette loi présente l'avantage que celle-ci contient déjà bon nombre de dispositions - par transposition - des directives énoncées dans le paragraphe précédent. En ce qui concerne la transposition de la Directive concernant les bases de données, celle-ci prévoit la transposition des dispositions dans les différentes législations nationales au plus tard pour le 1er janvier 1998[15].

A côté de cette nouvelle loi générale, il existe également une loi spécifique[16] en date du 30 juin 1994 relative aux programmes d'ordinateur. Le régime de protection des programmes d'ordinateur n'a donc finalement pas été intégré dans la loi (générale) sur le droit d'auteur. Pour les questions non-réglées dans la loi spécifique, la loi générale sera d'application.

---

[13]La loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins, a été publiée dans le M. B. du 27 juillet 1994. De nombreux errata relatifs à cette loi ont été publiés dans les M. B. du 5 et 22 novembre 1994. Cette loi a déjà été modifiée par la Loi du 3 avril 1995, M. B., 29 avril 1995.

[14]Loi du 22 mars 1886 sur le droit d'auteur, M. B., 26 mars 1886.

[15]Rien n'interdit d'aller plus vite et de commencer dès aujourd'hui à réfléchir à cette exercice de transposition : STROWEL, A., *La directive communautaire sur les bases de données : quelle transposition en droit belge ?*, AM, 1996, 92.

[16]Loi spécifique du 30 juin 1994 concernant les programmes d'ordinateur, M. B., 27 juillet 1994. Errattum, M. B., 5 novembre 1994.

Eu égard au propos de ce chapitre, nous ne commenterons que quelques grands principes de la loi générale, sans approfondir la loi spécifique de protection des programmes d'ordinateur[17].

Les aspects généraux de la loi générale que nous commenterons dans ce chapitre sont au nombre de six :

* l'objet du droit d'auteur ;

* le sujet du droit d'auteur ;

* un aperçu des droits d'auteur (patrimoniaux (droits exclusifs, un droit à rémunération, exceptions) et moraux) ;

* l'exploitation contractuelle des droits patrimoniaux ;

* le respect des droits d'auteur ;

* la gestion des droits d'auteur.

## 51.2 Objet de la protection par le droit d'auteur

### 51.2.1 Absence de formalités

Tout comme sous l'application de l'ancienne loi, la nouvelle loi sur le droit d'auteur de 1994, offre une protection ex lege à n'importe quelle création, ce qui veut dire qu'aucune formalité ne doit être accomplie par un auteur pour que l'oeuvre puisse bénéficier de la protection du droit d'auteur.

---

[17]Pour une analyse de cette loi, nous citons e. a. BRISON, F. et TRIAILLE, J. P., *La nouvelle loi sur la protection des programmes d'ordinateur, dans le sillage de la loi sur le droit d'auteur*, J. T., 1995, 141 - 145 ; VAEL, L., *Auteursrechtelijke bescherming van software. De wet van 30 juni 1994*, T. G. R., 1995, 98 - 123 et STROWEL, A., *La loi belge du 30 juin 1994 sur les programmes d'ordinateur : vers un droit d'auteur sui generis ?*, RIDA, 1995, n° 164, 173 - 233.

### 51.2.2 Les conditions de la protection par le droit d'auteur

Toute création répondant aux conditions cumulatives d'originalité et de forme concrète, bénéficient de la protection accordée par la loi sur le droit d'auteur et les droits voisins.

#### *51.2.2.1 Forme concrète ?*

La loi sur le droit d'auteur offre protection aux oeuvres exprimée dans une forme concrète[18].

Les idées en soi ne sont donc pas protégées[19]

#### *51.2.2.2 L'originalité ?*

Donner une définition de la notion d'originalité n'est certes pas aisé étant donné l'existence de différentes catégories d'oeuvres.

Toutefois en 1989, la Cour de Cassation[20] a eu à deux reprises l'occasion de clarifier la notion d'originalité[21]. Dans ces deux arrêts de la Cour de Cassation il ressort clairement que la notion “d'originalité” requiert à la fois “la marque d'une personnalité”[22] et “l'effort intellectuel”[23].

---

[18]Pour de plus amples détails concernant la condition de la forme concrète, nous citons e. a. BERENBOOM, A., *Le Nouveau Droit d'Auteur et les droits voisins*, Larcier, 1995, n° 33 - 35.

[19]BUYDENS, M., *La protection des idées originales : droit d'auteur, responsabilité civile ou droit de la personnalité ?* , Ing. Cons., 1993, n° 3 - 4, 61 - 75.

[20]Cour de Cassation, 27 avril 1989, Pas., 1989, I, 908 et Cour de Cassation, 25 octobre 1989, Pas., 1990, I, 238.

[21]STROWEL, A., *L'originalité en droit d'auteur : un critère à géométrie variable*, J. T., 1991, p. 513-518.

[22]Cour de Cassation, 25 octobre 1989, Pas., 1989, I, 239 - 241.

Cette clarification de la Cour de Cassation n'évite pas que les juges se laisseront guider par une appréciation personnelle de ces deux éléments, qui se veut subjective[24] par définition.

#### *51.2.2.3 Un caractère artistique ?*

Alors que dans le passé, certains juges estimaient que le caractère artistique (ou esthétique) formait une troisième condition de fond indispensable, la Cour de Cassation a clairement exprimé dans les arrêts précités que les jugements[25] qui refusaient pour motif d'absence de "valeur artistique" une protection par le droit d'auteur aux créations, violent les dispositions légales sur le droit d'auteur.

### 51.2.3 Les différentes catégories d'oeuvres

#### *51.2.3.1 Les catégories dans la loi générale*

La lecture de la loi générale de 1994 relative au droit d'auteur et aux droits voisins, nous apprend que le législateur n'a pas énuméré de façon limitative les différentes catégories d'oeuvres auxquelles la loi générale peut offrir une protection dans les conditions précitées.

Les différentes catégories d'oeuvres (dites traditionnelles) énoncées dans la loi générale sont les oeuvres littéraires, les oeuvres plastiques, les photographies, les oeuvres sonores et les oeuvres audiovisuelles. A côté de règles générales applicables à toutes catégories d'oeuvres confondues, chaque catégorie d'oeuvres connait des dispositions particulières (p. ex.

---

[23]Cour de Cassation, 27 avril 1989, Pas., 1990, II, 903 - 910 : *Attendu que pour qu'une photographie puisse bénéficier de la protection légale, il faut mais il suffit qu'elle soit l'expression de l'effort intellectuel de son auteur, condition indispensable pour donner à l'oeuvre le caractère d'individualité nécessaire pour qu'il y ait création.*

[24]Cette subjectivité d'appréciation est dénoncée e. a. par MALLET-POUJOL, N., *Marché de l'information. Le droit d'auteur injustement "tourmenté" ...,* RIDA, 1996, n° 168, p. 93 - 203.

[25]Voir les deux notes précédentes.

section 2 contient des dispositions particulières aux oeuvres littéraires ; section 3 contient des dispositions particulières aux oeuvres plastiques, etc.)

Excepté pour les oeuvres littéraires[26], le législateur n'a pas (voulu) défini(r) les différentes catégories d'oeuvres.

Cette absence de définitions de ces notions offre l'avantage de les rendre non-ankylosantes.

#### *51.2.3.2 L'oeuvre logicielle dans la loi spécifique*

Ci-dessus, nous avons déjà mentionné l'assimilation aux oeuvres littéraires. La protection accordée par la loi spécifique concernant les programmes d'ordinateur s'applique à toute forme d'expression d'un programme d'ordinateur.

Les idées et principes à la base de tout élément d'un programme d'ordinateur, y compris ceux qui sont à la base de ses interfaces, ne sont pas protégés par le droit d'auteur[27].

#### *51.2.3.3 Parmi quelle catégorie devons-nous ranger les oeuvres informatiques ?*

Etant donné l'existence de dispositions particulières pour chaque catégorie d'oeuvre traditionnelle, il nous semble opportun de réfléchir à cette question. Dans la littérature trois solutions différentes sont souvent avancées :

**a/** soit elles peuvent être qualifiées en tant qu'oeuvre audiovisuelle ;

**b/** soit en tant qu'oeuvre logicielle ;

**c/** soit en tant que base de données.

---

[26] Art. 8, § 1er *:* Par oeuvres littéraires, on entend les écrits de tout genre, ainsi que les leçons, conférences, discours, sermons ou toute autre manifestation orale de la pensée.

[27] Art. 2, al. 2 de la loi spécifique.

La directive européenne concernant la protection de la structure[28] des bases de données connaît un champ d'application large. Le considérant n°17 de la directive donne une définition du terme “base de données” :

> *Tout recueil d'oeuvres littéraires, artistiques, musicales ou autres, ou de matière telles que textes, sons, images, chiffres, faits et données ; qu'il doit s'agir de receuils d'oeuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles ; qu'il s'ensuit qu'une fixation d'une oeuvre audiovisuelle, cinématographique, littéraire ou musicale en tant que telle n'entre pas dans le champ d'application de la présente directive.*

Etant donné le caractère général de cette contribution, nous renvoyons à d'autres auteurs pour une étude approfondie de ce problème de qualification[29].

Une autre question qui est soulevée concerne l'éventuelle suppression des différentes catégories d'oeuvres.

Cette question qui - au stade actuel de commercialisation et d'usage d'oeuvres informatiques - semble aller fort loin, nous force à réfléchir[30] quant à la rédaction future de nouvelles législations dans le domaine du droit d'auteur et des droits voisins.

---

[28]Voir le considérant n° 15 de cette directive mentionnant explicitement que cette protection vise la structure de la base, et donc pas le contenu de la base de données.

[29]Ce problème de qualification d'une oeuvre numérique a déjà fait couler beaucoup d'encre. SIRENELLI, P., *La qualification de l'oeuvre multimédia*, in Le Multimédia. Marché, Droit et pratiques juridiques, Presses universitaires de France, 1996, 41 - 58.

[30]Cette question est également abordée par VOORHOOF, D., *Multimedia en auteursrecht. Afschermen en beschermen van informatie. Juridische problemen rond de beschikbaarheid en de reproduktie van informatie (tekst-beeld-klank) op één drager*, in X, Multimedia. Interactiviteit, kennisspreiding., Stichting Boek, Diepenbeek , 1995, p. 111.

## 51.3 Le sujet du droit d'auteur

### 51.3.1 La qualité d'auteur

#### *51.3.1.1 L'auteur (originaire) ne peut être qu'une personne physique*

L'article 6 de la loi générale stipule de façon non équivoque que *: Le titulaire originaire du droit d'auteur est la personne physique qui a créé l'œuvre*. De ce premier paragraphe de l'article 6 de la loi il suit qu'une personne morale ne peut être le titulaire originaire d'une oeuvre. Il va de soi qu'une personne morale pourra exercer les droits d'auteur après cession de ceux-ci par le titulaire originaire.

#### *51.3.1.2 Présomptions légales de qualité d'auteur et co-auteur*

Afin que des tiers puissent savoir qui est l'auteur originaire d'une création, la loi prévoit trois présomptions légales :

> *Est présumé auteur, sauf preuve contraire, quiconque apparaît comme tel sur l'oeuvre, du fait de la mention de son nom ou d'un sigle permettant de l'identifier*[31].
>
> *L'éditeur d'un ouvrage anonyme ou pseudonyme est réputé, à l'égard des tiers, en être l'auteur*[32].
>
> *En ce qui concerne les oeuvres audiovisuelles, le législateur a prévu :*
>
> *Outre le réalisateur principal (...) sont présumés, sauf preuve contraire, auteurs d'une oeuvre audiovisuelle réalisée en collaboration :*

---

[31] Art. 6, § 2 de la loi générale.

[32] Art. 6, § 3 de la loi générale.

> ***a/*** *l'auteur d'un scénario ;*
>
> ***b/*** *l'auteur de l'adaptation ;*
>
> ***c/*** *l'auteur des textes ;*
>
> ***d/*** *l'auteur graphique pour les oeuvres d'animation ou les séquences d'animations d'oeuvres audiovisuelles qui représentent une part importante de cette oeuvre ;*
>
> ***e/*** *l'auteur des compositions musicales avec ou sans paroles spécialement réalisées pour l'œuvre*[33].

#### *51.3.1.3 et l'identification numérique ?*

Dans son Livre Vert, la Commission européenne a consacré une section entière aux systèmes techniques d'identification et de protection. Tout au long de ce Livre Vert, la Commission européenne semble être optimiste quant aux possibilités techniques futures pour l'identification de la protection des oeuvres et des prestations[34].

### 51.3.2 La durée de protection de septante ans post mortem auctoris

#### *51.3.2.1 Règles générales*

L'article 2, §1 de la loi mentionne cette durée de protection très longue :

---

[33] Art. 14 de la loi générale.

[34] Livre Vert de la Commission européenne, COM (95), 382 final, p. 79 - 83.

> *Le droit d'auteur se prolonge pendant septante ans*[35] *après le décès de l'auteur au profit de la personne qu'il a désignée à cet effet ou, à défaut, de ses héritiers conformément à l'article 7.*

La durée de protection doit être calculée à partir du 1 janvier de l'année suivant le décès de l'auteur. A partir du moment où la durée de septante ans s'est écoulée, l'oeuvre tombe dans le domaine public, ce qui veut dire que chaque personne pourra utiliser l'oeuvre “librement”, donc sans autorisation ni rémunération quelconque.

#### *51.3.2.2 Règles spécifiques*

La loi générale prévoit également des règles spécifiques concernant la durée de protection. Ces règles spécifiques sont toutes groupées dans l'article 2 de la loi générale et concernent :

* l'oeuvre qui est le produit d'une collaboration (par exemple : une oeuvre audiovisuelle) (art. 2, § 2) ;

* l'oeuvre anonyme ou pseudonyme (p. ex. Hergé) (art. 2, § 3) ;

* l'oeuvre publiée par volumes, parties, fascicules, numéros ou épisodes (par exemple : Le Larousse)(art. 2, § 4) ;

* les photographies (art. 2, § 5) ;

* les oeuvres posthumes (art. 2, § 6).

---

[35]Comparée à l'ancienne loi, la durée de protection est augmentée de 20 années. Cette durée de septante ans après la mort de l'auteur est devenu obligatoire dans chaque Etat membre depuis le 1 juillet 1995, conformément à la Directive 93/98/CEE du Conseil du 29 octobre 1993 relative à l'harmonisation de la durée de protection du droit d'auteur et de certains droits voisins, J. O. C. E., 24 novembre 1993, L 290/9.

## 51.4 Aperçu des droits d'auteur

### 51.4.1 Introduction

Le système actuel du droit d'auteur et des droits voisins connaît d'une part les droits pécuniers et d'autre part les droits moraux.

Alors que les droits pécuniers peuvent facilement être cédés ou donnés en licence - par voie contractuelle - par leurs titulaires originaires, les droits moraux sont quasiment inaliénable, ce qui implique que dans l'hypothèse où un auteur aurait cédé tous ses droits patrimoniaux à quelqu'un d'autre, il gardera toutefois la possibilité d'exercer ses droits moraux.

### 51.4.2 Les droits patrimoniaux

Les droits patrimoniaux qui existent dans le chef des auteurs et des titulaires des droits voisins sont soit des droits exclusifs soit des droits à rémunération.

L'article premier § 1 de la loi générale reconnaît à l'auteur le droit exclusif d'autoriser la "reproduction" ainsi que le droit exclusif de la "communication au public" par un procédé quelconque. Le "droit de suite" est un troisième droit patrimonial accordé à l'auteur[36], contrairement aux deux droits précédents, le droit de suite est inaliénable.

#### *51.4.2.1 Le droit de reproduction*

Contrairement au terme "droit de communication au public", le terme "droit de reproduction" semble indiquer que ce droit exclusif s'applique aussi bien aux reproductions à usage public qu'à usage privé. Nous verrons dans ce chapitre que cette allégation devra être nuancée.

---

[36]Etant donné que le droit de suite ne s'applique qu'aux enchères publiques d'oeuvres plastiques, le droit de suite ne sera pas examiné par nous. Le droit de suite est mentionné dans les articles 11 - 13 de la loi générale.

Consécutivement nous analyserons le droit exclusif de reproduction et le droit à rémunération de reproduction.

#### 51.4.2.1.1 La règle : l'exclusivité, le monopole de l'auteur

L'article 1er, § 1er de la loi générale définit le droit exclusif de reproduction de la façon suivante :

> *L'auteur d'une oeuvre littéraire ou artistique a seul le droit de la reproduire ou d'en autoriser la reproduction, de quelque manière et sous quelque forme que ce soit.*

La loi poursuit :

> *Ce droit comporte notamment le droit exclusif d'en autoriser l'adaptation ou la traduction*[37]*. Ce droit comprend également le droit d'en autoriser la location ou le prêt.*

#### 51.4.2.1.2 L'exception : licence légale pour usage privé

Dans les trois suivants (la copie privée, la réprographie, le prêt public) le législateur belge a prévu de façon explicite que - contrairement à la règle du monopole - l'auteur ou le titulaire du droit voisin devra tolérer l'usage privé (d'une reproduction) de son oeuvre. Comme énoncée plus haut, la loi générale du 30 juin 1994 a instauré des licences légales, au nombre de trois.

---

[37]Exemple : Le roman *Hiroshima mon amour* de Marguerite Duras, déjà adapté pour le cinéma, sera mis en scène en néerlandais par le metteur en scène flamand Guy Cassiers. J. W. H., Marguerite Duras en scène et en néerlandais dans le texte, Le Soir, 30 mai 1995.

Il s'agit ici donc de deux droits distincts, notamment celui du droit d'adaptation d'une part et celui du droit de traduction de l'autre.

En compensation pour la perte de l'exclusivité dans le chef de l'auteur ou le titulaire du droit voisin, le législateur a prévu un droit à une rémunération.

Les modalités du “droit à une rémunération” pour l'auteur ou le titulaire du droit voisin sont laissées aux bons soins du Roi.

**La copie privée[38]**

Cette licence légale s'applique uniquement aux copies privées d'oeuvres sonores et audiovisuelles.

* **a/** Le droit à rémunération :

Pour le droit à rémunération, le législateur a fait appel à une technique forfaitaire aussi bien pour les supports audio et vidéo que pour les appareils audio et vidéo.

* **b/** Perception de rémunération :

La perception de rémunération est effectuée par la société de gestion Auvibel[39].

* **c/** Répartition de rémunération :

La répartition de rémunération se fait également par la même société de gestion, à raison d'un tiers aux auteurs ; artistes-interprètes ou exécutants et producteurs de phonogrammes et d'oeuvres audiovisuelles.

* **d/** Remboursement de rémunération :

L'article 57 de la loi générale mentionne 5 catégories auxquelles la rémunération perçue sera remboursée, dont p. ex. les aveugles, les malvoyants, les sourds, malentendants ainsi que les institutions reconnues, créées à l'intention de ces personnes.

---

[38]Chapitre V (art. 59 - 60 - 61) de la loi générale du 30 juin 1994 relative au droit d'auteur et aux droits voisins.

Pour une analyse récente (avec tableau comparatif) nous renvoyons à MAEYAERT, P., *De privé-kopie van geluids- en audiovisuele werken*, IRDI, 1996, p. 122 - 130.

[39]Arrêté royal du 2 octobre 1995 chargeant la société Auvibel d'assurer la perception et la répartition des droits à rémunération pour copie privée, M. B., 17 octobre 1995.

En ce qui concerne la “copie privée”, nous signalons l'existence d'un arrêté royal d'exécution du 28 mars 1996 relatif au droit à rémunération pour copie privée des auteurs, des artistes-interprètes ou exécutants et des producteurs de phonogrammes et d'oeuvres audiovisuelles[40].

**La reprographie**

La “reprograhie”[41] s'applique uniquement aux copies à usage personnel ou à usage interne des oeuvres fixées sur un support graphique ou analogue.

* **a/** Le droit à rémunération :

Les auteurs et les éditeurs d'oeuvres fixées sur un support graphique ou analogue ont droit à une rémunération pour chaque copie à usage personnel ou interne.

* **b/** La perception de rémunération :

Les rémunérations seront perçues par la société de gestion Reprobel.

* **c/** La répartition de rémunération :

Les rémunérations seront attribuées à part égale entre les auteurs d'une part et les éditeurs de l'autre.

En ce qui concerne la “reprographie”, l'arrêté royal d'exécution se fait toujours attendre. Cette absence d'arrêté royal d'exécution de

---

[40]A. R. du 28 mars 1996, M. B., 6 avril 1996. Cet A. R. remplace intégralement l'arrêté royal du 23 juin 1995 relatif au droit à rémunération pour copie privée des auteurs, des artistes-interprètes ou exécutants et des producteurs de phonogrammes et d'oeuvres audiovisuelles.

[41]Pour une analyse très intéressante de la rémunération pour copie privée des phonogrammes et vidéogrammes en droit français nous citons l'oeuvre de EDELMAN, B., *Droits d'auteur, droits voisins. Droit d'auteur et marché*, Paris, Dalloz, 1993, p. 211 - 240.

la reprographie a pour effet qu'actuellement la “reprographie” n'est pas encore entrée en vigueur et que par la suite, chaque copie à usage personnel ou à usage interne d'une oeuvre fixée sur un support graphique ou analogue tombe sous le régime commun du droit d'auteur exclusif. L'autorisation préalable de l'auteur ou du titulaire du droit voisin est donc indispensable !

**Le prêt public**

La troisième licence légale “prêt public” s'applique aussi bien au prêt d'oeuvres littéraires ou de partitions musicales qu'au prêt d'oeuvres sonores ou audiovisuelles. La seule différence inscrite dans la loi est que le prêt d'oeuvres sonores ou audiovisuelles ne peut avoir lieu que six mois après la première distribution de l'oeuvre[42].

Autre condition essentielle est que le prêt doit être organisé “dans un but éducatif et culturel par des institutions reconnues ou organisées officiellement à cette fin par les pouvoirs publics”[43].

En ce qui concerne la licence légale de “prêt public” instauré par le législateur, nous devons souligner que le Roi n'a toujours pas déterminé les montants des rémunérations, ni fixé (après consultation des Communautés) une exemption ou un prix forfaitaire à certaines catégories d'établissements reconnus ou organisés par les pouvoirs publics.

[42]Article 23, § 2 de la loi générale.

[43]Art. 23, § 1er de la loi générale.

**51.4.2.1.3 Le droit de reproduction sur une oeuvre informatique.**

La spécificité de la technologie numérique rend possible la transmission et la copie d'un grand nombre d'oeuvres informatiques avec une très grande facilité et une bonne qualité.

***Faut-il ou non, revoir la notion de "reproduction" face à cette évolution de numérisation ?***

**1/** Pour mieux pouvoir répondre à cette question, il nous semble indispensable de rechercher si le droit (exclusif, à rémunération) de reproduction est applicable aux actes normaux dans l'utilisation des ordinateurs.

Exemple de reproduction : la fixation d'une oeuvre par le biais de sa numérisation et du stockage des données numériques sur un support informatique ; l'enregistrement de l'oeuvre sur un support fixe ( par exemple disque dur, disquette d'ordinateur, etc ...).

Par contre, la simple consultation d'une oeuvre on-line[44] et la fixation temporaire de l'oeuvre dans la mémoire interne, destinée exclusivement à permettre la visualisation ponctuelle sur écran, sembleraient ne pas tomber sous l'application du droit de reproduction.

---

[44]Jusqu'à la publication du rapport de la National Information Infrastructure sur la propriété intellectuelle en Amérique), en juillet 1994, personne n'avait jamais envisagé que le simple fait de consulter un exemplaire d'une oeuvre, protégée par le droit d'auteur, puisse porter atteinte à ce droit. [...].

Le rapport interprète la loi relative aux droits d'auteur de manière plus large que le Congrès puisqu'il déclare que le fait de consulter une oeuvre sous forme numérique constitue une atteinte aux droits d'auteur (à moins que le propriétaire des droits n'ait donné son autorisation). [...] Quelles raisons incitent donc les rédacteurs à considérer que la consultation, la lecture, ou toute autre utilisation, constitue une atteinte aux droits d'auteur, lorsques les oeuvres se présentent sous forme numérique ? *Vers une éthique du virtuel*, Dossiers de l'audiovisuel, 1995, 42 - 44.

**2/** Faut-il également instaurer un système de licence légale pour les copies privées d'oeuvres informatiques ou devons-nous le laisser au monopole de l'auteur ou du titulaire du droit voisin ?

**Au niveau national**

Pour pouvoir répondre à cette question nous renvoyons d'abord aux alinéas relatifs à la qualification des oeuvres informatiques et nous soulignons l'importance de la question de la qualification.

Dans l'hypothèse où l'oeuvre informatique ne pourrait être qualifiée comme oeuvre audiovisuelle, il ne peut - à notre sens et dans l'état actuel de la législation - être question d'application de cette licence légale aux oeuvres informatiques.

L'A. R. du 28 mars 1996 (voir supra) semble nous venir en aide en visant également les supports et les appareils informatiques.

L'arrêté royal d'exécution fixe le montant de la rémunération applicable aux supports et appareils informatiques à 0% du prix de vente.

A ce propos il est intéressant de citer quelques passages du Rapport au Roi de cet arrêté royal :

> *Dans l'état actuel des choses, il apparaît que la perte de revenus causée par les actes de reproduction privée d'oeuvres sonores et audiovisuelles effectuées au moyen de supports et d'appareils informatiques est quasiment nulle car la durée du déchargement de sons ou d'images, la perte de qualité en cas de reproduction privée de sons ou d'images diffusées en ligne et l'importance de la mémoire dont il faut pouvoir disposer pour stocker des sons et des images font que les appareils et les supports informatiques qui techniquement permettent la reproduction privée*

> *de sons ou d'images ne sont actuellement pas utilisés de façon significative à cette fin* [45].

**Au niveau communautaire**

Nous avons déjà (voir supra) noté l'optimisme et la foi de la Commission européenne dans des réponses techniques adéquates aux problèmes techniques actuels. Concernant la copie privée, la Commission n'est pas certaine de la nécessité du maintien d'une licence légale :

> *L'évolution de la technique comporte un certain nombre d'avantages importants. Alors que l'utilisation normale d'un photocopieur, d'un magnétophone ou d'un magnétoscope classique permet par définition la copie sans que l'on puisse empêcher celle-ci (à moins de priver ces appareils de cette fonction essentielle), la numérisation permet d'identifier et de limiter, si cela est souhaité, la copie numérique par le particulier de telle ou telle oeuvre ou prestation. Bien entendu, cela suppose que des systèmes techniques soient adoptés de façon généralisée mais le contrôle de l'utilisation des oeuvres redevient possible.*
>
> *Cette évolution doit être prise en compte pour l'évaluation du droit de reproduction dans le domaine du numérique. Ainsi, on peut admettre que les systèmes de copie privée basés sur des prélèvements portants sur les supports et les appareils, en contrepartie de la législation de la copie privée, pourront rester une réponse valable dans les cas où la technique ne permet pas d'empêcher la*

---

[45] Il est important de souligner que l'exemption de rémunération pour les supports matériels et appareils informatiques accordée par le Roi a été vivement critiquée par le Conseil d'Etat comme ayant excédé son pouvoir *: Il s'agit là d'un problème d'interprétation de la loi, que le Roi n'a pas le pouvoir de trancher*, M. B., 6 avril 1996, 8217.

> *copie. Par contre, si des moyens techniques limitant ou empêchant la copie privée sont instaurés, la justification de la licence légale que constitue un système de rémunération s'estompe*[46].

**3/** Les bibliothèques publiques prêteront-elles des cédéroms ou des cédéroms interactifs en masse ?

Deux possibilités existent : soit le visiteur d'une bibliothèque publique consultera le cédérom ou le cédérom interactif sur place, soit le visiteur d'une bibliothèque souhaitera emprunter le cédérom ou le cédérom interactif.

Ce vide juridique actuelle, ne nous permet pas d'extrapoler. Toutefois, il nous semble logique de prévoir pour le prêt public des cédéroms et des cédéroms interactifs, un même régime de licence légale que pour les oeuvres (dites) traditionnelles.

#### *51.4.2.2 Le droit exclusif de communication au public*

##### 51.4.2.2.1 Le principe

L'article 1er, § 1er de la loi générale du droit d'auteur définit le droit exclusif de communication au public de la façon suivante :

> L'auteur d'une oeuvre littéraire ou artistique a seul le droit de la communiquer au public par un procédé quelconque. *Contrairement au droit de reproduction, le droit exclusif de communication est manifestement limité à la communication "au public".*

---

[46] Livre Vert de la Commission européenne, COM (95), 382 final, p. 50.

Ce droit exclusif comprend non seulement l'exécution publique d'une oeuvre ou sa représentation publique[47], mais également l'exposition, la radiodiffusion, la télédistribution, etc ...

**51.4.2.2.2 Le droit de communication au public d'une oeuvre numérisée ?**

Afin de pouvoir définir avec précision le terme "communication au public" dans le domaine numérique, la Commission européenne a demandé aux milieux intéressés - par le biais du questionnaire - de définir quels actes de communication numériques peuvent être considérés comme des "utilisations privées".

A cet effet la Commission européenne mentionne plusieurs formes différentes de communication à prendre en compte[48] :

* Communication par le réseau entre deux personnes privées ;

* Communication par le réseau entre plusieurs personnes privées ("bulletin board service" par exemple) ;

* Communication par le réseau entre une personne privée et une entreprise ;

* Communication par le réseau dans le cadre d'une ou plusieurs entreprises.

---

[47]Comme exemple de l'exercice du droit exclusif de communication au public nous citons le refus de Hugo Claus de représentation de ses pièces de théatres, qui viennent d'être éditées en livre de poche. Vlaeminck, M., Nieuwe toneelstukken van Hugo Claus alleen te lezen. Nieuwe stukken van Claus worden niet gespeeld, De Standaard, 31 mai 1995.

[48]Livre Vert de la Commission européenne, COM (95), 392 final, p. 55.

Les autres questions posées par la Commission européenne illustrent l'exercice difficile et périlleux de la définition de la notion “communication au public”.

### 51.4.3 Les exceptions des droits patrimoniaux

#### *51.4.3.1 Introduction*

Notre loi actuelle de 1994 relative au droit d'auteur et aux droits voisins ainsi que d'autres lois dans la Commission européenne prévoit plusieurs exceptions aux droits patrimoniaux sous forme de régime de liberté, à condition que l'oeuvre ait été licitement publiée. Dans ces cas l'auteur ou le titulaire de la prestation ne pourra interdire l'usage de son oeuvre par un tiers et ni réclamer un droit à rémunération.

##### 51.4.3.1.1 Principe : exceptions limitatives

A condition d'avoir été licitement publié, un tiers peut se prévaloir des exceptions suivantes (énumérées dans les articles 22 et 23 de la loi générale sur le droit d'auteur) :

**1/** La reproduction et la communication au public, dans un but d'information, de courts fragments d'oeuvres ou d'oeuvres plastiques dans leur intégralité à l'occasion de comptes rendus d'événements de l'actualité (art. 22, § 1, 1°) ;

**2/** La reproduction et la communication au public de l'oeuvre exposée dans un lieu accessible au public, lorsque le but de la reproduction ou de la communication au public n'est pas l'oeuvre elle-même (art. 22, § 1, 2°) ;

**3/** La communication gratuite et privée effectuée dans le cercle de famille (art. 22, § 1, 3°) ;

**4/** La caricature, la parodie ou le pastiche, compte tenu des usages honnêtes (art. 22, § 1, 6°) ;

**5/** L'exécution gratuite d'une oeuvre au cours d'un examen public, lorsque le but de l'exécution n'est pas l'oeuvre elle-même, mais l'évaluation

de l'exécutant ou des exécutants de l'oeuvre en vue de leur décerner un certificat de qualification, un diplôme ou un titre dans le cadre d'un type d'enseignement reconnu (art. 22, § 1, 7°) ;

**6/** Les contretypes, copies, restaurations et transferts, effectués par la Cinémathèque royale de Belgique, dans le but de préserver le patrimoine cinématographique (art. 22, § 1, 8°)[49].

#### 51.4.3.1.2 Sont-elles applicables aux oeuvres informatiques ?

Faut-il prévoir les mêmes exceptions générales aux droits exclusifs patrimoniaux ? Il nous semble logique de décider d'appliquer les mêmes exceptions générales.

## 51.5 Le droit moral.

### 51.5.1 Introduction

Dans la nouvelle loi du 30 juin 1994 les droits moraux sont au nombre de trois. L'article 1, § 2 stipule que : *L'auteur d'une oeuvre littéraire ou artistique jouit sur celle-ci d'un droit moral inaliénable. La renonciation globale à l'exercice futur de ce droit est nulle*.

#### *51.5.1.1 Principe : les droits moraux exclusifs*

Les trois droits moraux reconnus, à l'article 1, §2 de la loi générale sont : le droit exclusif de divulger l'oeuvre ; le droit exclusif de revendiquer ou de refuser la paternité de l'oeuvre et le droit au respect de l'oeuvre.

La loi mentionne que le droit de respect de l'oeuvre permet à l'auteur de s'opposer à toute modification de celle-ci et explique : *Nonobstant toute renonciation (de l'exercice du droit moral), il conserve le droit de s'opposer à toute déformation, mutilation ou autre modification de cette oeuvre ou à*

---

[49]Cette sixième exception a éta ajoutée par la Loi portant modification de la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins, M. B., 29 avril 1994.

*toute autre atteinte à la même oeuvre, préjudiciables à son honneur ou sa réputation.*

#### *51.5.1.2 Le droit moral exercé sur une oeuvre informatique*

Il est d'ores et déjà prévisible que la communication interactive sur les réseaux augmentera d'une façon considérable la manipulation des contenus des oeuvres diffusées.

Il est donc indispensable de s'interroger sur les effets éventuels des nouvelles applications technologiques sur l'exercice des droits moraux[50].

> *La Société de l'Information a ceci de particulier que la numérisation totale des oeuvres et des prestations ainsi que l'interactivité sur les réseaux rendent celles-ci transformables, colorisables, réductibles, etc. avec de plus en plus de facilité. Ainsi par exemple, le temps viendra où n'importe qui pourra modifier les couleurs d'un film ou remplacer les visages des interprètes et renvoyer le film modifié sur le réseau [51].*

En 1992 déjà, une audition consacrée au droit moral et organisée par la Commission européenne avec les milieux intéressés avait clairement mis en lumière, l'existence des divergences d'opinions concernant le renforcement éventuel des droits moraux.

Alors que d'une manière générale, les représentants des auteurs et des artistes interprètes avaient plaidé pour un droit moral à renforcer, les représentants de l'édition du secteur de la presse, des producteurs, des radio-diffuseurs et des employeurs manifestent des réserves quant à un renforcement du droit moral estimant que le droit moral constitue un facteur

---

[50]THERY, I., *Le droit moral dans l'oeuvre multimédia*, in Le multimédia, Marché, droit et pratiques juridiques, Presses universitaires de France, 1996, p. 59 ss.

[51]Livre Vert de la Commission européenne, COM (95), 382 final, p. 65.

d'incertitude important pour l'exploitation des oeuvres et contribue de cette façon à décourager les investissements[52].

La Commission européenne de son côté précise dans son Livre Vert que dans le contexte de la Société de l'Information la question du droit *moral se pose d'une façon plus aiguë que précédemment. En effet, les moyens technologiques numériques permettent de transformer les oeuvres d'une manière plus aisée*[53]. Une des questions de la Commission européenne soulève la possibilité de règler les questions liées au droit moral par voie contractuelle[54]. La question de la Commission de prévoir *des "présomptions d'acceptations de certaines modifications par le fait même de l'accord donné par l'auteur pour la numérisation*", nous semble très dangereuse et menacer les propres fondements du droit moral.

## 52. Nécessité d'introduction de nouveaux droits d'auteur (exclusifs, à rémunération) ?

Dans le Livre Vert de la Commission européenne, la possibilité d'introduire deux nouveaux droits exclusifs pour les titulaires des droits voisins est mentionnée et semble apparemment être soutenue par la Commission européenne dans son Livre Vert.

Il s'agirait premièrement d'un droit de transmission/diffusion numérique, et deuxièmement d'un droit de radiodiffusion numérique.

---

[52]Idem, p. 66 et 67.

[53]La Commission estime qu'il convient d'examiner la question de savoir si le manque d'harmonisation actuel constitue une situation qui demeure acceptable dans le nouvel environnement numérique. Livre Vert de la Commission européenne, COM (95), 382 final, p. 67.

[54]Idem, p. 67, question n°2.

### 52.1 Le droit de transmission / diffusion numérique

Ce nouveau droit exclusif est réclamé par les producteurs de phonogrammes, qui craignent de voir échapper leur propre marché de tout contrôle. Ce droit pourrait être limité à la transmission numérique point-à-point. *Dans cette perspective, la transmission ou la diffusion numérique couvrirait notamment la transmission d'un ordinateur personnel ou autre appareil numérique d'une personne privée ou d'une base de données vers un ou plusieurs ordinateur(s) personnel(s) ou autres appareils numériques de personnes privées ou d'entreprises. Ainsi, un système de vidéo à la demande par lequel les consommateurs demandent qu'on leur transmette électroniquement les oeuvres cinématographiques de leur choix serait couvert*[55].

### 52.2 Le droit exclusif de radiodiffusion numérique

Ce droit exclusif-ci est également réclamé par les producteurs des phonogrames et les artistes interprètes ou exécutants et les producteurs de films et les artistes interprètes de ce secteur. Ils réclament un droit d'autoriser ou d'interdire la radiodiffusion des phonogrammes ou des films, au lieu d'un simple droit à rémunération équitable. Surtout le secteur phonographique laisse entendre que ce qui était jusqu'ici considéré comme une utilisation secondaire est en fait devenu un type d'exploitation primordial et que par conséquent, le régime juridique doit suivre cette évolution[56].

### 52.3 Les contrats d’exploitation

#### 52.3.1 Introduction

Un des grands mérites de la nouvelle loi générale sur le droit d'auteur et les droits voisins est d'avoir - enfin - intégré et rendu obligatoire des règles

[55]Idem, p. 56 - 57.

[56]Idem, p. 61 - 64.

contractuelles minimales protégeant l'auteur originaire, lors de la cession (licence, etc.) d'un de ses droits patrimoniaux. L'article 3 de la loi générale instaure des règles générales concernant la cession et la licence des droits patrimoniaux. De nos jours les créateurs font appel à des professionnels pour l'exploitation de leur(s) oeuvre(s). Soucieux de la position trop faible de l'auteur dans les relations contractuelles, le législateur a voulu munir l'auteur de quelques règles contractuelles en sa faveur.

#### *52.3.1.1 Règles générales de cession des droits patrimoniaux*

Les paragraphes 1 et 2 de l'article 3 contiennent six règles générales qui doivent être respectées dans chaque contrat :

**1.** Le contrat ne se prouve que par écrit ;

**2.** Les dispositions contractuelles à cet égard sont de stricte interprétation ;

**3.** Pour chaque mode d'exploitation, la rémunération de l'auteur, l'étendue et la durée de la cession doivent être déterminées expressément ;

**4.** L'oeuvre doit être exploitée conformément aux usages honnêtes de la profession ;

**5.** La cession des droits concernant des formes d'exploitation encore inconnues est nulle ;

**6.** La cession des oeuvres futures n'est valable que pour un temps limité et pour autant que les genres des oeuvres sur lesquelles porte la cession soient déterminés. Le non-respect de ces règles minimales contractuelles est sanctionné.

#### *52.3.1.2 Règles assouplies de cession*

Ce régime strict de règles contractuelles minimales à respecter a toutefois été atténué par le législateur dans les deux situations suivantes :

##### 52.3.1.2.1 L'oeuvre a été créée sur commande

L'article 3, § 3, al. 2 prévoit dans ce cas que les droits patrimoniaux peuvent être cédés - d'une façon plus simplifiée - à celui qui a passé la commande, à condition que :

**1.** L'activité de celui qui a passé la commande relève de l'industrie non culturelle ou de la publicité ;

**2.** L'oeuvre soit destinée à cette activité ;

**3.** La cession des droits patrimoniaux soit expressément prévue.

**52.3.1.2.2 L'oeuvre a été créée en exécution d'un contrat de travail ou d'un statut**

L'article 3, § 3, al. 1er prévoit dans ces deux cas, que les droits patrimoniaux peuvent être cédés - de façon simplifiée - à condition que :

**1.** La cession des droits patrimoniaux soit expressément prévue ;

**2.** La création de l'oeuvre entre dans le champ du contrat ou du statut.

***52.3.1.3 Dispositions particulières***

A côté de ces règles contractuelles générales, la loi a prévu des dispositions particulières pour le contrat d'édition d'une part et le contrat de représentation de l'autre.

Qu'en est-il des cessions des droits patrimoniaux accordées par l'auteur avant l'entrée en vigueur de la loi générale ? Ces cessions du droit de reproduction, valent-elles également (et automatiquement) pour les reproductions numériques ?[57] Quelles règles contractuelles devra respecter un producteur de cédéroms ? Doit-on réfléchir et prévoir de nouvelles règles contractuelles ? Il est évident qu'une réponse à cette question est étroitement liée au problème de la qualification de l'oeuvre informatique.

---

[57]Nous retrouvons également cette question chez : HUGENHOLTZ, P. B., *Het auteursrecht, het internet en de informatiesnelweg*, NJB, 1995, n° 14, p. 517.

## 52.4 Le maintien du droit d'auteur et des droits voisins

Afin de pouvoir maintenir la protection par la loi générale, l'auteur/titulaire/ayant droit dispose de plusieurs instruments juridiques permettant de redresser des agissements illégaux (par exemple : copie illégale d'un livre ; contrefaçon d'une mélodie musicale ; présentation illégale d'une pièce de théâtre).

### 52.4.1 Dispositions pénales

La loi générale contient des dispositions pénales concernant le délit de contrefaçon. Une nouveauté de la loi réside dans le fait *que ceux qui sciemment, vendent, louent, mettent en vente ou en location, tiennent en dépôt pour être loués ou vendus, ou introduisent sur le territoire belge dans un but commercial les objets contrefaits* seront également jugés coupables de ce même délit de contrefaçon.

### 52.4.2 Actions civiles

Autre nouveauté très importante de la loi générale est la possibilité inscrite à l'article 87 d'introduire une action civile en cessation de toute atteinte au droit d'auteur ou à un droit voisin, selon les formes du référé. Cette action en cessation peut être formée à la demande de tout intéressé, d'une société de gestion des droits autorisés ou d'un groupement professionnel ayant la personnalité civile.

Etant donné le propos de cet article, nous ne nous attarderons pas sur les différentes formes de procédures qui existent dans le chef de l'auteur/titulaire/ayant-droit.

Toutefois nous devons souligner qu'ici surgissent également des problèmes de transposition dans le domaine numérique. Comme exemple nous pouvons citer, l'affaire récente du livre “Le Grand Secret” du docteur Gubler (médecin de François Mittérand). Nonobstant l'interdiction de diffusion accordée par le Tribunal en référé, l'ouvrage en entier est apparu sur réseau.

## 52.5 L'exploitation des droits d'auteur et des droits voisins

### 52.5.1 Introduction

Comme nous l'avons expliqué ci-dessus, le caractère exclusif du droit d'auteur et droits voisins a pour conséquence qu'avant tout usage d'une oeuvre ou d'une prestation, l'autorisation doit être demandée et obtenue par l'auteur, le titulaire ou l'ayant-droit en question.

**Exemple :** lorsque nous désirons faire usage d'un poème pour une affiche, nous sommes obligés - avant tout usage - d'en demander l'autorisation. Soit le poète en question gèrera lui-même ses droits (dans ce cas, l'autorisation ou le refus sera donné(e) par l'auteur en personne) soit le poète aura confié la gestion de ses droits à une société de gestion (dans ce cas, la société de gestion mandatée par l'auteur donnera ou non l'autorisation).

Cet exemple est évidemment fort simple. Il est bien clair que dans la pratique journalière les demandes d'usage d'une oeuvre qui affluent auprès des sociétés de gestion sont bien plus complexes.

La complexité atteint un point culminant, lorsque l'on songe à l'exemple suivant : un producteur de multimédia souhaite produire un cédérom sur "Cent ans d'histoire de la Bande Dessinée".

### 52.5.2 Formes différentes de gestion[58]

#### *52.5.2.1 La gestion individuelle*

L'auteur/titulaire/ayant droit gère lui-même l'exploitation de ses droits patrimoniaux. Cette façon-ci est donc la plus directe.

---

[58]Livre Vert de la Commission européene, COM (95) 382 final, p. 70.

#### *52.5.2.2 La présomption légale de cession des droits patrimoniaux*

Dans certaines situations le législateur a instauré une présomption de cession des droits. Dans ces cas-ci, l'auteur ou titulaire originaire ne peut gérer lui-même l'exploitation de ses droits patrimoniaux.

Concernant les oeuvres audiovisuelles par exemple, la loi générale a instauré dans l'article 18 une présomption de cession du droit exclusif de l'exploitation audiovisuelle de l'oeuvre, y compris les droits nécessaires à cette exploitation tels que le droit d'ajouter des sous-titres ou de doubler l'oeuvre.

#### *52.5.2.3 La gestion collective (volontaire, obligatoire) - les sociétés de gestion*

Depuis plusieurs décennies, la gestion individuelle semble de moins en moins efficace et souhaitée pour la gestion de l'exploitation des droits patrimoniaux. De plus en plus l'auteur/titulaire/ayant droit fait appel à une société de gestion. Il incombe alors à cette dernière de donner ou d'obtenir les autorisations et rémunérations requises. Une des plus anciennes sociétés de gestion connue par tous est SABAM.

Le chapitre VII de la loi générale sur le droit d'auteur est consacré aux sociétés de gestion des droits et principalement à l'autorisation qui doit leur être accordée préalablement par le ministre. Depuis la mise en vigueur de la loi générale, nous pouvons parler d'un réel “boom” des sociétés de gestion.

### 52.5.3 Faut-il revoir la gestion actuelle dans le contexte de la Société de l'Information ?

Il va de soi qu'au coeur du débat de la gestion de l'exploitation des oeuvres informatiques, les sociétés de gestion prennent une place primordiale.

A l'occasion d'une audition des milieux intéressés par la Commission européenne au mois de juillet 1994, ces premiers ont répondu à la question que l'intervention des autorités communautaires ne semble pas être

souhaitée à ce stade et qu'il existe toujours la nécessité de maintenir le caractère volontaire de la gestion collective[59].

Toutefois les milieux intéressés sembleraient être favorables à créer des sortes de centres d'administration des droits.

#### *52.5.3.1 Guichet unique : unique solution ?*

La Commission européenne considère *que certaines opérations de regroupement devraient constituer une évolution importante pour les sociétés de gestion collective, qui sont actuellement organisées par secteur et/ou par type d'ayants-droit*[60].

Côté ayants-droit, un tel regroupement sous forme de “guichet unique” donnerait la possibilité aux auteurs, aux artistes interprètes, ainsi qu'aux éditeurs-producteurs de disposer d'un outil permettant d'identifier la paternité d'oeuvres très diverses en rassemblant l'ensemble des répertoires susceptibles d'être sollicités pour les nouvelles technologies.

Côté utilisateurs, un “guichet unique” aura l'avantage de leur procurer les informations qui les intéressent notamment quant aux montants des redevances et des droits cédés[61].

## 53. Conclusion

Notre réponse à la question primordiale posée dans le Livre Vert de la Commission “révolution ou évolution du droit d'auteur ?” opte incontestablement pour “l'évolution du droit d'auteur”.

Nous sommes d'avis que conclure autrement, c’est-à-dire pour la “révolution du droit d'auteur”, nous amènerai à une remise en question

---

[59] Idem, p. 75.

[60] Idem, p. 76.

[61] Idem, p. 76.

éventuelle des propres fondements du régime du droit d'auteur. Ce qui serait à déplorer.

# NOUVELLES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION OU SOCIETE DE L'INFORMATION ?

**Emmanuel Belin**

**Aspirant F.N.R.S., Université Catholique de Louvain**

Ce texte n'a d'autre prétention que de lancer quelques idées sur ce que représente, sur le plan sociologique, la diffusion des nouvelles technologies de l'information et de la communication. Cette problématique se situant hors de mon champ d'investigation, les réflexions présentées ont un aspect spéculatif qui pourra détonner quelque peu avec les autres textes. Ce ton hypothétique est, soit dit en passant, de mise dans presque toutes les publications que j'ai pu lire jusqu'à présent sur le sujet. Dans un premier temps, je présente une réflexion sur la manière dont est généralement abordée la question de la régulation des nouvelles techniques de communication ; dans un second temps, je propose quelques pistes pour élargir la problématique au champs social et culturel.

## 54. Tentative de formalisation

Le sens commun relatif à ce que serait une régulation efficace des nouvelles technologies me paraît pouvoir être ramené à quelques propositions-clé.

1) De nouvelles technologies voient le jour, qui permettent la mise en communication permanente des êtres humains sans égards pour les distances. Ces technologies vont changer radicalement la société, les rapports des hommes entre eux. Cependant, ce changement peut aller vers le meilleur comme vers le pire.

2) Le scénario du "meilleur" porte à la fois sur le plan économique (augmentation de la productivité et création d'emplois), social

(développement de la solidarité sociale, renforcement du lien social) et culturel (rencontres, diversité linguistique).

3) Le scénario du "pire" est envisagé essentiellement sur le plan socio-économique : il consiste à dire que tous les avantages décrits en (2) ne seraient accessibles que pour une partie de la population, essentiellement dans le cadre du *business*. L'autre partie de la population serait exclue de la société de communication (dualisation, isolement) et de ses effets bénéfiques.

L'objectif poursuivi alors, me semble-t-il, est de réfléchir aux moyens à mettre en œuvre pour que ce soit le scénario du "meilleur" qui advienne. Un certain nombre d'hypothèses sont posées :

1) La mise en concurrence d'entreprises privées est la meilleure manière de mettre en place le réseau de câbles (la solution technique du câble optique étant pour le moment la plus souhaitable).

2) Le scénario du pire peut être évité à condition qu'on parvienne à imposer aux opérateurs privés des missions de service universel. La question est évidemment de savoir ce qu'on exigera concrètement de ces opérateurs.

> 2. 1. On exigera d'eux que certains services jugés indispensables soient garantis à chacun, où qu'il habite, à une qualité acceptable et à un tarif raisonnable.
>
> 2. 2. Un débat oppose une conception "individualiste" à une conception "fonctionnaliste" des services visés par cette contrainte. La conception individualiste définit le service universel à partir d'une réflexion sur ce à quoi les hommes ont droit, moralement. La conception fonctionnaliste définit le service universel à partir d'une réflexion sur ce dont la société a besoin, pratiquement. Dans le texte, ce débat est quelque peu effacé par une sorte de postulat : grosso modo, le droit des individus correspond aux nécessités sociales. Le citoyen a droit à ce dont la démocratie a besoin qu'il ait droit, telle semble être la conception du texte. La question se ramène, dès lors, à la suivante : de quoi un individu a-t-il besoin pour ne pas être exclu de la société de la communication ?
>
> 2. 3. La procédure d'évaluation de ce besoin peut être axée sur la demande existante ou sur des expériences de construction de la

demande – puisque ce qui est suffisant aujourd'hui risque de ne plus l'être demain. Pour le moment, il existe des dispositions réglementaires qui tranchent la question. Face à ces dispositions, deux questions se posent : d'abord, celle de leur bien-fondé (sont-elles assez exigeantes pour que soit évité le scénario du "pire", voire réalisé celui du "meilleur" ? ) ; ensuite, celle du bien-fondé d'une solution réglementaire substantielle (une définition procédurale n'est-elle pas plus appropriée, et dans quelles conditions ? ).

2. 4. Une fois déterminé le champ d'application de la contrainte de service universel, reste à savoir comment seront financés les coûts de celui-ci. Deux voies complémentaires sont proposées : d'une part, les péréquations tarifaires, et d'autre part, les subventions publiques (via un fonds de service universel). Les premières impliquent, me semble-t-il, un système de licences et de contrôle ; les secondes impliquent seulement un système de contrôle de l'usage fait des subventions.

De diverses discussions sur le thème, j'ai retenu que, pour pouvoir juger de l'opportunité de la définition de service universel que propose la Commission, plusieurs démarches sont possibles.

1) **Une démarche expérimentale.** L'objectif est ici de mettre en évidence, non plus les risques, mais les potentialités nouvelles offertes par les nouvelles technologies, allant dans le sens du scénario du "meilleur". Ce faisant, on espère convaincre les pouvoirs publics de l'opportunité d'interventions favorisant ce genre d'effets positifs.

2) **Une démarche déductive.** Il s'agit de tenter de prévoir les effets potentiels des innovations étudiées sur toute une série de variables dont la pertinence est définie par une démarche normative.

3) **Une démarche inductive.** Il s'agit ici simplement de réfléchir aux effets prévisibles de divers scénarios d'intervention (marché totalement libre, régulation par divers critères de service universel, ...), "tous azimuts", laissant au commanditaire le soin d'évaluer le caractère souhaitable ou non de ces effets prévisibles.

## 55. Quelques remarques

Il me semble que, dans son état actuel, la réflexion sur le thème traite insuffisamment d'un objectif qui, pourtant, me paraît très important. Cet objectif est la mise en perspective de ce qui se joue dans les décisions réglementaires. Certes, cette question est abordée, mais le ton, technique et précis lorsqu'il s'agit de problèmes réglementaires, technologiques ou économiques, devient souvent idéologique, emphatique lorsqu'on s'intéresse aux aspects sociaux et surtout culturels ; j'ai trouvé que beaucoup d'affirmations communément entendues tombent dans la critique que fait P. Musso :

> *Les nouvelles technologies suscitent, particulièrement en France, des passions et mobilisent un imaginaire annonçant alternativement le meilleur ("société de communication", "sortie de crise" ...) ou le pire (société de contrôle et de la passivité, "développement du chômage", dégradation de l'environnement). [...] D'un côté, des pratiques et des usages diversifiés, de l'autre des mythologies simplificatrices. Tel semble être le sort de toute innovation technique*[1].

Ce que je critique, c'est le postulat selon lequel il suffirait de prendre garde à bien définir la notion de service universel pour que le "mauvais" scénario soit évité, et que le bon soit réalisé. D'abord, je m'interroge sur les conceptions sous-jacentes à la définition du "bon" et du "mauvais" scénario. Ensuite, je doute qu'on puisse réduire la problématique de la société de communication à ses simples aspects technologiques. Autrement dit, pour moi, une technologie n'existe que dans l'usage qui en est fait, cet usage étant presque indépendant de la nature technique des médiums.

---

1 Communiquer demain. Nouvelles technologies de l'information et de la communication, p. 7.

*Emmanuel Bellin*

## 55.1 La question du bon et du mauvais

Considérons d'abord la question du "bon" et du "mauvais". Ce qui paraît clair, c'est que le rêve serait que chacun soit "branché" au réseau. Cela est-il si évident ? La création d'emplois désocialisants, par exemple, vaut-elle réellement mieux que le chômage ? Le mélange des espaces professionnel et familial est-il forcément une bonne chose ? Les exclus se sentiront-ils vraiment "intégrés" derrière leur terminal ? L'impression d'immédiateté propre aux décisions sur réseau ne risque-t-elle pas de favoriser des utopies de démocratie directe (style "minitel") où se confondent espace public et espace privé ? Ces questions de sens commun me laissent penser qu'il vaut au moins la peine de s'interroger sur le postulat selon lequel la société de la communication renforce le lien social. D'autre part, l'utilisation du réseau par les entreprises permet la délocalisation des décisions, rendant tout contrôle étatique illusoire. Ces questions sont à classer sous la rubrique "effets profonds" des NTIC, c'est-à-dire l'impact sur les compétences indispensables de participation à la vie sociale et démocratique. Le raisonnement est que la définition du scénario souhaitable ou non ne peut être établie qu'au terme d'une réflexion sur les usages multiples que permettront les NTIC, réflexion qui doit elle-même se fonder sur des critères puisés tant dans l'optique "individualiste" que "fonctionnaliste" ; il est invraisemblable qu'un enjeu aussi capital que l'engagement de toutes les sociétés industrialisées dans ce mode de fonctionnement ne fasse pas l'objet de recherches prospectives plus poussées. Certaines de ces recherches sont en cours, mais celles-ci se fondent sur une critériologie des effets à mesurer qui ne s'ancre pas dans une réflexion normative explicite. Le plus souvent, ces recherches raisonnent dans une contrainte intellectuelle, qui est qu'on ne peut pas remettre en question le caractère inévitable et bénéfique de ce progrès. Tout se passe comme s'il était demandé aux scientifiques de montrer "en quoi" ces innovations peuvent être utiles, sans que puisse être posée fondamentalement la question de cette utilité. Il semble bien que les enjeux économiques soient tels que la réflexion universitaire courbe l'échine et se contente d'une expertise visant à légitimer les décisions de ses commanditaires (je force sans doute le trait ...).

### 55.2 La question des usages

La question des usages est, de l'avis de tous, extrêmement ambiguë. P. CHAMBAT ("NTIC et représentations des usagers", in A. Vitalis (ed.), *Médias et nouvelles technologies. Pour une socio-politique des usages*, Rennes, Apogée, 1994) constate que les lobbies industriels, les offreurs, détiennent le monopole du discours sur l'usager. Ce discours consiste le plus souvent à réduire cet usager au rôle de consommateur passif, sans réelle remise en question de ce dont il retourne dans les faits. Cette représentation monolithique, indique-t-il, est renforcée dès lors que le marché est seul régulateur des décisions des acteurs :

> *Ce point est à mettre en relation avec la mise en œuvre (ou l'absence de mise en œuvre) de politiques publiques, car celles-ci favorisent l'émergence de débats dès lors qu'elles se traduisent en décisions publiques qui appréhendent l'usager, en tant qu'il constitue la source des demandes d'intervention publique et le destinataire des politiques publiques, autrement que comme un client, un consommateur ou un utilisateur. À cet égard, la privatisation des opérateurs de télécommunications, la déréglementation du secteur et la marginalisation du service public poussent dans le sens, d'une part, d'un affaiblissement de la représentation institutionnalisée des usagers et, d'autre part, d'un renforcement de l'image de l'usager comme utilisateur. [49-50].*

Même quand ils admettent que leurs "clients" utilisent les technologies mises à disposition dans une tout autre optique que l'utilisation "prévue", c'est pour mettre en avant des usages instrumentaux et individuels. La question de la possibilité d'utilisations à des fins collectives (mouvements sociaux, participation politique) n'est jamais posée. De plus,

> *[l]es techniques restent enfermées dans une vision instrumentale qui les appréhende comme des ressources pour l'action et non comme un élément de*

> *transformation des schémas cognitifs, de la perception de soi-même et de l'environnement. Est ici négligé un acquis des études sur la réception de la télévision comme de la sociologie de la lecture qui dissocie les textes du livre et s'enquiert des usages du livre ou de l'imprimé et pas seulement de la réception des textes. L'interrogation, qui était, semble-t-il, celle d'une revue comme Terminal et des pionniers de la micro-informatique, porte ici sur la capacité des utilisateurs de NTIC, en tant qu'utilisateurs, à constituer un mouvement social [52-53].*

Tout cela reste cependant en jachère, car le champ des usages des NTIC a été extrêmement peu analysé jusqu'à présent (à la différence de celui des médias). Deux résultats semblent cependant pouvoir être formulés pour le moment. Le premier concerne la séquence temporelle de pénétration de la nouvelle technologie dans la vie quotidienne :

> *Fantasmes (de l'imaginaire collectif) et grandes manœuvres (des industries et des États) accompagnent l'annonce du lancement et les éventuelles expérimentations sociales. Le second temps, celui où le nouveau produit ou service commence à être utilisé effectivement, donne le plus souvent lieu à des constats de reproduction du mode de vie antérieur, d'absence d'innovation sociale. Au troisième stade, seules quelques innovations se révéleront, au bout de plusieurs décennies, avoir été des catalyseurs de changements dans les structures sociales, les valeurs, les pratiques quotidiennes*[2]

La seconde constatation est que l'appropriation par les usagers correspond plus à une tactique qu'à une stratégie. C'est une logique réactive et non une élaboration à partir d'objectifs. L'usager se manifeste surtout par

---

2 Caroline MORICOT et Victor SCARDIGLI, *La voix sans le regard : Appropriations culturelles du téléphone à domicile,* Paris, MCD/IRESCO, mai 1990, p. 5, cité p. 53.

son décalage par rapport aux attentes des opérateurs, et c'est de cela que vient l'innovation sociale. La capacité d'appropriation innovante varie selon le capital culturel des usagers ; de plus, pour comprendre les usages, il faut tenir compte de variables sociologiques diverses (urbanisation, appartenance préalable à des réseaux sociaux, etc.).

Concernant le cas précis des NTIC, il me semble cependant qu'on puisse aller un peu plus loin. Lorsqu'on dit que ce dispositif permet le "transport de l'information", on cache derrière cette affirmation apparemment simple de nombreuses significations. Si on y regarde de plus près, on s'aperçoit que le concept d'information a un double sens : "objectif" et "subjectif". Le concept "objectif" s'exprime en termes probabilistes : l'information est un signal improbable. Le concept "subjectif" s'exprime en termes pragmatiques : l'information est ce qui permet à celui qui la détient de prendre une décision plus susceptible d'aboutir au résultat escompté. On peut élargir le concept "subjectif" en parlant de "connaissance", qui serait la capacité d'une personne à s'orienter dans le monde et à s'en sentir solidaire.

Quelle est l'utilité de ces distinctions ? Elles permettent de mettre le doigts sur les "malentendus" possibles entre trois registres de discours relatifs aux nouvelles technologies de la communication. Ces registres sont : le discours technique, fondé sur la première définition de l'information. La société de l'information, dans cette optique, c'est l'augmentation exponentielle du nombre de bits sur la planète, c'est-à-dire du taux de connexion des séries, de la systématisation des variations. Le second discours est le discours utilitariste, fondé sur la seconde définition. Ici, la société de l'information est avant tout à comprendre comme la mise à disposition du matériel de prise et de coordination des décisions. C'est ainsi que, par exemple, la mise à disposition d'une base de données économiques est, pour un agent économique, plus importante que la réception d'une photographie porno, alors que ces deux documents ont, du point de vue technique, le même "poids" informationnel. En revanche, et c'est la troisième logique, la photo porno – et il suffit de regarder les listes de discussions d'Internet pour se rendre compte que ce phénomène n'est pas marginal – peut être comprise par d'autres personnes comme une "connaissance", c'est-à-dire comme un contenu de sens qui lui permet de se "retrouver" mieux dans le monde.

Ceci indique à quel point ce que l'on appelle la "société de l'information" n'a pas beaucoup de sens. Les accroissements de

"productivité informationnelle" permis par les NTIC sont extrêmement différent selon ces trois types de "connaissance" ; il va de soi que c'est dans le domaine de la connaissance culturelle que ceux-ci sont les plus faibles. De plus, "l'américanité" du réseau sur le plan culturel, telle qu'elle est préfigurée par Internet pour le moment, est flagrante. Ce facteur contribue à renforcer l'image d'une centralité culturelle des États-Unis. La dualisation entre "branchés" et "débranchés" pourrait bien se doubler d'une dualisation au sein même des "branchés", entre les "pragmatiques" (qui tirent une réelle utilité) et les "dilettantes" ; "pendant que la masse joue au game boy, l'élite gère les millions". Ce problème de l'appropriation différentielle de la technologie selon les groupes sociaux est un des thèmes d'une recherche qui se met en place sous une forme interdisciplinaire. Cette recherche théorique sera menée de front avec une autre recherche, menée dans le cadre de l'objectif 1 par des ingénieurs et des communicateurs, et qui consistera à étudier les multiples usages positifs possibles d'outils techniques.

### 55.3 Des questions plus larges

Sur le plan cognitif, le caractère immédiat et délocalisé, renforcé par tout ce qui touche aux mondes virtuels, renforce la désymbolisation de l'expérience au profit d'une logique de l'imaginaire, de l'immédiat. Or, la symbolisation et le principe de réalité sont au fondement de la démocratie et du sujet moderne. C'est un risque dont parle André Akoun (*La communication démocratique et son avenir*) ; Philippe Breton, dans *L'utopie de la communication*, dénonce la création d'un homme "sans intérieur", qui serait vidé de sa substance par l'immédiateté des relations, leur désancrage du principe de réalité. Ces hypothèses peuvent paraître fantaisistes quand on se place d'un point de vue politique, mais elles ont presque la force d'évidences dès qu'on se place du point de vue de la psychologie cognitive et de la psychanalyse. Cet effet culturel profond comporte des risques du point de vue identitaire, plus encore si on prend en considération les nouvelles formes de télévision qui pourront en émerger. On peut dire, dans ce domaine, que les NTIC sont intrinsèquement relativistes, au moins si leur fonctionnement est régi exclusivement selon les lois du marché. On peut reprendre quelques effets dont je parle pour les médias, comme la fragmentation de l'expérience et de la connaissance, la disponibilisation de schémas cognitifs éclatés, etc.

De nombreux services de proximité peuvent être rendus à distance, comme c'est le cas du téléenseignement. Cependant, il semble clair que quelque chose se perd dans cette médiation. C'est d'autant plus flagrant quand des logiciels sont chargés de veiller à cette éducation : on assiste alors à une standardisation outrancière du savoir ; un hypertexte remplaçant un livre, c'est bien, mais un hypertexte remplaçant un professeur, c'est moins bien. De plus, de telles solutions favorisent un certain type de raisonnement ; il semble assez clair (encore faudrait-il tester toutes ces spéculations) que l'apprentissage informatique est plus approprié à l'enseignement de l'économie classique ou de la statistique inférentielle que de la phénoménologie husserlienne.

Le télétravail favorise l'autonomie de l'individu, mais l'individu n'a pas besoin que d'autonomie. De plus, la sphère professionnelle tend à se fondre avec la sphère privée – les parents sont là, mais pas disponibles. Cette "indisponibilité" ou ce mélange de registres peut avoir des conséquences sur la socialisation, qu'il faudrait étudier. Troisièmement, on imagine bien que la solidarité professionnelle est entravée par ces modes d'organisation du travail. Quatrièmement, de telles formules auront sans nul doute un impact environnemental, notamment en favorisant la désertification des grandes villes, ce qui pourrait n'avoir pas que des conséquences positives, mais aussi en favorisant l'exode rural dans des formules qu'on peut prévoir "résidentielles", c'est-à-dire extrêmement lourdes sur le plan environnemental. Cinquièmement, mais cela est presque un lieu commun, la possibilité de "délocaliser" certains services de proximité augmente considérablement la concurrence mondiale et donc l'instabilité des marchés, et peut dans certains cas nuire gravement à l'emploi dans des pays où le prix du facteur travail est élevé (cas de la Swissair faisant sous-traiter sa comptabilité en Inde, mais également, même pour la main-d'œuvre européenne qualifiée, possibilité de contrats d'expatriement). Ici aussi, la mise au point de solutions réglementaires s'impose.

La confiance dans le mode de transfert d'information que constituent les NTIC, et notamment la possibilité d'identifier tout document de manière certaine au moyen d'une signature électronique, fait du marché électronique le substitut des halles et des bourses, tant sur le plan réel que sur le plan financier. De ce dernier point de vue, comme le montre P. Quéau dans le Monde Diplomatique, il devient possible d'opérer des transactions financières virtuelles, basées simplement sur la confiance réciproque d'opérateurs situés dans différents pays. Cela peut aller jusqu'à la création

de monnaie, hors de tout contrôle des banques centrales. L'achat et la vente d'information doivent pouvoir être efficacement régulés dans une société où celle-ci devient le facteur premier de productivité et constitue des marchés colossaux. Plus généralement, l'intérêt économique des NTIC réside essentiellement dans la possibilité de délocalisation de la production, dans la possibilité d'une indépendance accrue des logiques industrielles par rapport au contexte matériel de leur insertion sociale. Si cela est vrai, on comprend beaucoup mieux l'importance de courants comme la socio-économie, qui insistent sur l'internalisation des externalités du marché. Le marché électronique, au contraire, va dans le sens d'une déconnexion totale des réalités sociales et économiques.

Le plus souvent, les penseurs des NTIC considèrent que les facteurs sociaux et culturels sont, en quelque sorte, des freins à l'amélioration unilatérale des conditions de vie. Ces facteurs sont considérés seulement sous l'angle de la résistance au changement. Pourtant, la sagesse impose de ne pas entrer précipitamment dans la société de l'information ; cette sagesse n'est aucunement garantie par le seul jeu concurrentiel, qui induit plutôt une fuite en avant. Sur le plan politique, la substitution à la problématique du service public de celle du service universel, c'est-à-dire le passage d'une conception qualitative et substantive à une conception purement quantitative et libérale me semble significative. Certes, ce point est important, mais il ne doit pas masquer la nécessité d'une intervention publique européenne sur le plan de l'usage ; et cette indispensable régulation à venir n'est certes pas facilitée par la privatisation dans le domaine de l'infrastructure. Certes il n'est pas possible de revenir sur la libéralisation du processus, pour un schéma d'ordre plus "néo-keynesien". L'importance des enjeux soulignés ici, de manière encore spéculative, il faut en convenir, semble toutefois indiquer la nécessité pour les États et la Communauté de se donner des compétences fortes en matière réglementaire. Celles-ci pourraient reposer sur des systèmes de licences (utilisation de l'espace public), ou encore sur des frontières électroniques (dont il faut noter qu'elles ne peuvent s'appliquer aux réseaux satellites). Des mesures pourraient être prises pour favoriser la visibilité des flux informationnels, comme par exemple des kiosques publics obligatoires pour accéder aux banques de données. Mais avant tout, il s'agit de trouver un moyen de faire internaliser par les opérateurs les externalités positives et négatives de leurs décisions. De ce point de vue, Pierre-Alain MERCIER & Yves TOUSSAINT ("Les usages" in P. MUSSO, *Communiquer demain. Nouvelles techniques d'information et de*

*communication*, Paris, Editions de l'Aube, 1994) notent que toutes les modifications techniques allant dans le sens des NTIC et de l'accélération du temps se sont accompagnées, sur le plan des pratiques, de dispositifs privés de *ralentissement et de stockage* du temps (ex. le répondeur automatique). Sur le plan public, cette idée pourrait être reprise dans l'économie de compteurs qui va naître, sous la forme de caisses sociales électroniques alimentées par les acteurs économiques, ou encore de taxations à l'utilisation. Ces fonds pourraient être utilisés pour contrer les effets négatifs sur le plan socio-politique de cette nouvelle forme de marché.

# TABLE DES MATIERES

**PREFACES**

Michel LEBRUN 7
Benoît LIPS 9

**AVANT-PROPOS**

**PREMIERE PARTIE**

**QUELLES TECHNOLOGIES POUR L'EDUCATION ?**

UNIVERSITE LIBRE DE BRUXELLES : LES BIBLIOTHEQUES 15
1. Technologies nouvelles et bibliothèques virtuelles 15
1.1 Contexte général 15
1.2 Evolution du rôle des bibliothèques 17
1.3 Le projet “PISTE” 18

LES RESEAUX INFORMATIQUES A L'UCL SITUATION ET PERSPECTIVES 21

Auguste LALOUX 21
1. L'interréseau UCL 21
2. Connexion aux réseaux publics 23
3. Services disponibles 23
4. Accès des étudiants 24
5. Des services en croissance 26
6. Le CEDITI 28
7. Perspectives de développement 29

L’INTERRESEAU ULG : UNE PORTE D’ACCES A L’INTERNET MONDIAL 31

Arthur BODSON, Recteur de l'Ulg 31
1. Accès à l’Internet et intérêt de l’Internet 31
2. L’infrastructure physique 32
3. Les équipements des utilisateurs 33
4. Les services 33
5. La formation et l'aide à l'utilisation de l'Internet 34
6. Moyens mis en œuvre - budget 35

OU EN SONT LES NOUVELLES TECHNOLOGIES AUX FACULTES DE NAMUR ? 41

Jean-Pol VIGNERON 41

LES NOUVELLES TECHNOLOGIES A LA F.U.C.A.M. 45

Michel DELATTRE 45

DE “L' EDUCATIONAL TECHNOLOGY” A LA TECHNOLOGIE POUR L'EDUCATION 49

Marcel LEBRUN , Renata VIGNANO 49

*AVANT-PROPOS* *49*

1. Introduction 52
2. De la société complexe 54
3. Aux savoirs complexes 56
4. De la technologie ... 60
5. A l’éducation 65
6. Des méthodes d’éducation 72
7. Aux méthodes pour s’éduquer 74
8. Aux médias 78
9. Conclusion 80

TRANSMISSION DES SAVOIRS ET REGULATION 83

Dominique VERPOORTEN 83

1. Introduction 83
2. Le discours de l’Union : le “gap” et le “challenge” 86
   - 2.1 Les prétentions de la sphère économique 86
   - 2.2 Les technologies pour l'éducation 88
   - 2.3 “Lifelong learning education” et télécoms 89
   - 2.4 Discours différents pour programme semblable 91
3. Ecole, Etat et TI 91
   - 3.1 Les écoles sont-elles des institutions qui fonctionnent finalement sur une logique du contrat ? 91
   - 3.2 Qu'implique, pour l'organisation de l'espace public démocratique, une extension du droit de regard d'agents extérieurs sur la sphère éducative ? 93
   - 3.3 Le service éducatif bat-il en brêche l'idée d'un service public en matière d'éducation ? 94
   - 3.4 Comment développer des systèmes de “mise en phase” de l'offre et de la demande en matière d'APTI ? 96
   - 3.5 APTI : la victoire de l'autodidacte ? 98
   - 3.6 Quel compromis entre décentralisation et intégration ? 98
4. Conclusion 99

LE RESEAU INFO-MUSE 103
Françoise SIMARD 103
1. L'origine 103
2. La mise en place 104
3. L'autoroute de l'information et les nouvelles technologies 104
3.1 L'informatisation des collections 105
3.2 La mise en réseau des institutions 106
3.3 Les résultats escomptés 106
3.4 L'imagerie numerique 107

**DEUXIEME PARTIE**

**QUEL CADRE JURIDIQUE POUR INTERNET ?**

LES ACTIVITES INFORMATIONNELLES ILLICITES DANS LES NOUVEAUX ENVIRONNEMENTS ELECTRONIQUES 113
Mylène BEAUPRE et Sophie HEIN 113
1. Introduction 114
2. La liberté d'expression 115
3. La corruption des moeurs et l'atteinte à l'ordre public 127
3.1 Le matériel obscène et pornographique 127
3.2 Les autres infractions d'ordre sexuel 156
4. Les atteintes à la dignité et à la sécurité des personnes 161
4.1 Le harcèlement *("Stalking")* 162
4.2 Les menaces 173
4.3 Les informations dangereuses 175
4.4 La diffamation criminelle 176
4.5 La propagande haineuse 179
4.6 Les jeux vidéos et autre matériel à caractère violent 188
5. Les atteintes à la vie privée 190
6. Les atteintes à la saine administration de la justice 191
7. Conclusion 193
LES NORMES INTERNATIONALES DE PROTECTION DES DONNEES PERSONNELLES ET L'AUTOROUTE DE L'INFORMATION 199
Karim BENYEKHLEF 199
1. Introduction 199
2. Le droit international de la protection des données personnelles 201
2.1 Les documents internationaux 201
2.2 Le principe de l'équivalence 221
3. L'applicabilité des normes internationales aux nouvelles voies électroniques de communication 228

3.1 Les nouvelles voies électroniques de communication 228
3.2 La vie privée et la protection des données personnelles 231
4. Conclusion 244

DROIT ET INFOROUTE : VERS UNE LEX ELECTRONICA ? 249

Pierre-Luc BOUCHER 249

1. Introduction 249
2. Espace cybernétique et réglementation nationale 250
2.1 Les communautés de réseaux 252
2.2 La *lex mercatoria* : Sources et définition 257
3. *Lex mercatoria* et espace cybernétique 263
3.1 Lex electronica ? 264
3.2 Le commerce électronique et la clause de “non-commercialité” 282
4. Conclusion 291

LA PROTECTION DE LA VIE PRIVEE ET DES RENSEIGNEMENTS PERSONNELS DANS L’ESPACE CYBERNETIQUE 299

Martin MICHAUD 299

1. Introduction 299
2. Les préoccupations et menaces 300
2.1 Les préoccupations 300
2.2 Les principales sources de menaces à la vie privée 328
3. Les situations particulières donnant ouverture à une intrusion dans la vie privée 335
3.1 L'utilisation, la cueillette, la conservation ou la transmission de données personnelles 336
3.2 L'interception, la communication ou l'utilisation d'une communication électronique 365
4. Conclusion 387

LE DROIT D'AUTEUR DANS LE CONTEXTE DU DEVELOPPEMENT DE LA “SOCIETE DE L'INFORMATION” 395

Valérie CASTILLE 395

1. Le principe de la territorialité de la protection par le droit d’auteur 396
1.1 Le principe de territorialité 396
1.2 Nécessité d'harmonisation internationale du droit d'auteur au-delà des frontières nationales 396
1.3 Nécessité d'harmonisation européenne du droit d'auteur au-delà des frontières nationales 397
1.4 Nécessité d'harmonisation accrue du droit d'auteur dans le cadre du développement de la “Société de l'Information” 398

1.5 “Droit d'auteur” versus “copyright” ? 399
2. Principes généraux de la loi relative au droit d’auteur 400
2.1 Introduction 400
2.2 Objet de la protection par le droit d'auteur 401
2.3 Le sujet du droit d'auteur 406
2.4 Aperçu des droits d’auteur 409
2.5 Le droit moral. 421
3. Nécessité d'introduction de nouveaux droits d'auteur (exclusifs, à rémunération) ? 423
3.1 Le droit de transmission / diffusion numérique 424
3.2 Le droit exclusif de radiodiffusion numérique 424
3.3 Les contrats d’exploitation 424
3.4 Le maintien du droit d’auteur et des droits voisins 427
3.5 L’exploitation des droits d’auteur et des droits voisins 428
4. Conclusion 430

NOUVELLES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION OU SOCIETE DE L'INFORMATION ? 433

Emmanuel Belin 433

1. Tentative de formalisation 433
2. Quelques remarques 436
2.1 La question du bon et du mauvais 437
2.2 La question des usages 438
2.3 Des questions plus larges 441

**TABLE DES MATIERES** **447**

With over thirty Internet sites online, the DAD team has a proven record of creative, sophisticated solutions for all types of online communication challenges. From design to databases, applets to e-zines, our staff have seen it, practised it, and mastered it. Our combined staff has published four best-selling books and dozens of articles on the Internet, its role in Belgium, and its implications for law and business. Our references speak for themselves. Toyota Europe, Thalys, Sony Belgium, Sony Music, and Sarma top a long and distinguished list of companies that have devoted their Internet development to DAD.

---

Impression Ciaco