



Gide Loyrette Nouel

# **PROTECTION DE LA VIE PRIVEE DANS LE CYBERESPACE**

Deuxième Université de la communication  
de l'Europe du Sud-Est

"Un grand pas en avant"

12-14 juin 2003  
Sarajevo, Bosnie-Herzegovine

## Sommaire

### *Liberté d'expression et protection de la vie privée : le difficile équilibre des droits fondamentaux*

*La liberté d'expression  
Le droit à la vie privée*

### *Internet : les nouveaux enjeux de la protection de la vie privée*

*Les enjeux humains  
Les enjeux techniques*

### *La réaction des organismes internationaux : définition des grands principes*

*OCDE  
Organisation Mondiale du Commerce  
Nations Unies  
Conseil de l'Europe  
Union Européenne*

### *Réglementation*

*L'adaptation du droit de la presse au réseau  
Le droit de l'informatique et des libertés  
L'autorégulation*

### *La mise en œuvre de la réglementation*

*Les technologies protectrices de la vie privée  
Les responsabilités*

Les juristes ont créé la catégorie des droits de la personnalité dont fait partie le droit à la vie privée. Aux Etats-Unis, dès 1870, le terme *privacy* a été défini comme le droit d'être laissé tranquille (the right to be left alone<sup>1</sup>). En Allemagne, le concept de « *Datenschutz* <sup>2</sup> », utilisé depuis la fin des années soixante, dissocie d'une part, la vie privée et les données personnelles, et, d'autre part, les personnes concernées. Ce sont les personnes qui sont protégées et non les données.

Pourtant très proches, il existe une distinction entre la notion de vie privée et les données personnelles. La vie privée concerne tous les éléments de la personnalité et englobe notamment les données personnelles :

*Vie privée*<sup>3</sup> : « les éléments qui ont trait à l'individu et à sa vie familiale entrent dans le cadre de la vie privée, en revanche, les informations relatives au patrimoine et à la vie professionnelle ne bénéficient pas de la même protection »

*Données personnelles*<sup>4</sup> : « toutes les informations concernant une personne physique identifiée et identifiable : 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, économique, culturelle ou sociale »

A ce jour, les questions soulevées par le droit fondamental que constitue le droit à la vie privée se résolvent dans la pratique par un mélange d'application du droit commun accompagnées de quelques adaptations, de réglementation spécifique, d'autodiscipline des acteurs ainsi que d'une mise en pratique technique et judiciaire.

## **Liberté d'expression et protection de la vie privée : le difficile équilibre des droits fondamentaux**

### **La liberté d'expression**

- La liberté d'expression est un principe fondamental de toute société démocratique. A ce titre, elle a été consacrée par la Déclaration universelle des droits de l'homme du 10 décembre 1948 :  
*" Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions "*
- Ce principe fondamental est entériné par le pacte international relatif aux droits civils et politiques de 1966 (pacte de 1966)<sup>5</sup>  
*" (la liberté d'expression) comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontière, sous une forme orale, écrite, imprimée ou artistique et par tout autre moyen de son choix (article 19) "*
- La Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 énonce que *" toute personne a droit à la liberté d'expression "*

---

<sup>1</sup> Revue de droit de Harvard, 1890. Le droit à la vie privée/

<sup>2</sup> Protection des données

<sup>3</sup> Source : Guy Braibant. Données personnelles et société de l'information. Rapport au premier ministre sur la transposition en droit français de la directive 95/46/CE. La Documentation Française, 1998, p. 19

<sup>4</sup> Définition posée par l'article 2.a de la directive numéro 95/46/CE

<sup>5</sup> Pacte international relatif aux droits civils et politiques adopté le 16 décembre 1966 par l'Assemblée générale des Nations Unies <http://www.hri.ca/partners/forob/f/docs/2.htm>

Ces textes de droit international sont souvent relayés par des textes nationaux :

- Le premier amendement de la Constitution américaine précise que *"le Congrès ne pourra faire aucune loi ... restreignant la liberté de la parole et de la presse". Chacun doit avoir le droit d'exprimer ses opinions sans être inquiété.*

La liberté d'expression est un principe fondateur du réseau Internet qui est lui-même, basé sur la libre circulation de l'information et des idées. Si la liberté d'expression est un droit fondamental, son exercice ne doit pas porter atteinte au respect de la personne d'autrui, à la dignité humaine, à l'ordre public ou encore au respect de la vie privée qui constitue également un droit fondamental de l'homme.

### **Le droit à la vie privée**

Le droit au respect de la vie privée constitue un droit reconnu au niveau international et national, il s'agit d'un droit fondamental de l'homme

- Article 12 de la Déclaration Universelle des droits de l'homme de 1948.

*" Nul ne fera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteinte à son honneur ou sa réputation ".*

- Article 8 de la Convention européenne des Droits de l'homme et des libertés fondamentales :

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

- Article 9 du code civil français:

En France, depuis 1970, le juge peut ... prescrire toute mesure ... propre à empêcher ou faire cesser une atteinte à l'intimité de la vie privée (Code civil, article 9-2). Le besoin de confidentialité et de respect de la vie privée est un droit profondément ancré dans nos sociétés.

*" Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé ".*

Les technologies de l'information et de la communication représentent un nouveau défi pour la protection de la vie privée. Transposé aux réseaux Internet, le nécessaire équilibre entre liberté d'expression et protection de la vie privée se trouve confronté à un support de communication dynamique, mondial, interactif et extrêmement rapide. C'est dans ce nouvel environnement que réside le nouvel enjeu de la protection de la vie privée.

## **Internet : les nouveaux enjeux de la protection de la vie privée**

Chaque individu est désormais fiché plusieurs centaines, voire plusieurs milliers de fois. «*Toute personne est en effet appréhendée par des traitements automatisés de données dans une très grande diversité de situations : comme écolier, étudiant, salarié, contribuable, candidat à un emploi, patient, assuré social, bénéficiaire de prestations sociales, électeur, abonné au téléphone, à l'électricité et au gaz, locataire, titulaire d'un compte en banque, voyageur sur une ligne aérienne, abonné à un journal, client d'une librairie ou d'un supermarché, personne nominativement sondée sur ses jugements ou ses habitudes de consommation...*»<sup>6</sup>

### **Les enjeux humains**

#### ***Internet grand public : la communication à l'échelle mondiale***

Le périmètre des acteurs et des utilisateurs d'Internet a diversifié la nature des usages et des contenus du réseau. Internet, réseau mondial, décentralisé et dématérialisé constitue un moyen de communication d'envergure mondiale.

#### ***Internet marchand : la facilité des échanges***

Lieu d'échange d'idées, Internet est également un espace d'échange de biens et services. Le commerce électronique crée de nouveaux défis pour le respect de la vie privée en générant la diffusion et la transmission de données personnelles notamment lors des transactions électronique. En effet, lorsqu'une personne effectue une transaction électronique, elle donne elle-même ses données personnelles.

#### ***Internet citoyen : la libre expression***

La dimension non marchande et citoyenne d'Internet est très importante. Internet est porteur d'enjeux culturels et démocratiques de dimension mondiale. Il multiplie les capacités d'expression et d'action des citoyens et de leurs associations.

Ainsi, Internet n'est pas en soi un vecteur de nouvelles atteintes aux droits de la personne, ni même de nouveaux délits, hormis les délits de piratage informatique. En revanche, les atteintes aux droits de la personne telles que les atteintes à la vie privée et à la confidentialité des données personnelles peuvent prendre de nouvelles formes, ou plutôt des formes exacerbées par le fait qu'Internet permet l'expression publique à tous.

### **Les enjeux techniques**

#### ***La collecte automatique de données***

Lorsqu'un utilisateur rend visite à un site Web, le logiciel du site enregistre automatiquement l'adresse Internet Protocol (IP) de l'ordinateur utilisé pour se brancher sur l'Internet. L'adresse IP est un chiffre unique attribué à chaque ordinateur branché sur l'Internet, elle joue le même rôle qu'une adresse postale. L'adresse IP ne révèle pas nécessairement l'identité du visiteur (il faudrait que la personne soit branchée directement sur l'Internet). Comme la plupart des gens se branchent chez eux par l'entremise d'un PSI, l'adresse IP identifie le PSI et non l'utilisateur. Dans ce cas, l'adresse IP sert simplement à suivre anonymement les actions du visiteur alors qu'il navigue sur le site Web.

Les sites Web recueillent automatiquement des renseignements personnels concernant le fureteur, le système d'exploitation et la plate-forme de l'utilisateur, la date et l'heure de la visite, le nom et l'adresse

---

<sup>6</sup> Guy Braibant, *Données personnelles et société de l'information*, rapport au Premier ministre. La Documentation Française, 1999.

URL de la page Web que l'utilisateur a consultée immédiatement avant d'avoir accédé à la page actuelle, tous les éléments de l'interrogation.

### ***Renseignements volontairement fournis par l'utilisateur***

Les sites qui offrent des services ou commercialisent des produits exigent que l'utilisateur complète au moins une partie de la formule d'inscription pour avoir accès au service ou effectuer des achats en ligne. Il en est de même pour les forums, les groupes et les options de personnalisation des sites Web personnels. Les transactions en ligne sont toujours subordonnées à l'obtention de données sur le client internaute.

### ***Les mouchards électroniques***

Un mouchard électronique est un petit fichier-texte renfermant un code d'identification unique qui est automatiquement placé dans le disque dur de l'utilisateur par l'ordinateur d'un site Web. Il sert à identifier les personnes qui rendent visite au site, à stocker des données les concernant, p. ex. leur mot de passe, à mettre en mémoire certains renseignements sur leurs activités au site ou encore les pages visitées. Ils peuvent également servir à stocker les données personnelles fournies en ligne dans le but de les regrouper et de les combiner à d'autres renseignements pour créer un profil de l'utilisateur qui servira, entre autres, à des programmes de marketing. Le profil de l'utilisateur peut également être vendu à des tierces parties à l'insu et sans le consentement de celui-ci.

Face à cette prolifération de moyens techniques dont l'utilisation est susceptible de porter atteinte au respect de la vie privée, il n'y a donc pas lieu de légiférer spécifiquement pour Internet, mais sans doute de modifier la procédure pénale ainsi que l'organisation judiciaire, afin de tenir compte des caractéristiques du réseau, ainsi que de ses usages.

### **Les éléments de la protection de la vie privée :**

- **Définition des grands principes**
- **Réglementation**
- **Autorégulation**
- **Technologies protectrices de la vie privée**
- **Sanctions**

## **La réaction des organismes internationaux : définition des grands principes**

### **OCDE**

La protection des données personnelles en ligne sur les réseaux informatiques fait l'objet de toutes les attentions du WPISP (Working Party on Information Security and Privacy), groupe de travail créé au sein de la Direction Science technologie et industrie de l'OCDE qui a notamment rédigé des Lignes directrices de l'OCDE régissant la protection des consommateurs dans l'e-business.

Les Lignes directrices de l'OCDE énoncent huit principes fondamentaux en la matière, à savoir :

- *limitation en matière de collecte* (paragraphe 7 Lignes directrices de l'OCDE), c'est-à-dire que les méthodes de collecte doivent être loyales et licites. Par voie de conséquence, la collecte n'est possible qu'après en avoir informé la personne concernée ou encore après avoir obtenu son consentement ;

· *qualité des données* (paragraphe 8 Lignes directrices de l'OCDE), c'est-à-dire que les données recueillies ne doivent pas dépasser les finalités du traitement. Ainsi, l'internaute ne doit pas avoir à donner son numéro de sécurité sociale pour accéder à un service gratuit de messagerie électronique ;

· *spécification des finalités* (paragraphe 9 Lignes directrices de l'OCDE), c'est-à-dire que les raisons de la collecte doivent être mentionnées avant que l'internaute ne saisisse ses données. De cette façon, il pourra consentir à la collecte en toute connaissance de cause ;

· *limitation de l'utilisation* (paragraphe 10 Lignes directrices de l'OCDE), c'est-à-dire que les données recueillies ne doivent pas être divulguées, utilisées à des fins autres que celles spécifiées au moment de la collecte, à moins que la personne concernée n'y consente ;

· *garanties de sécurité* (paragraphe 11 Lignes directrices de l'OCDE), c'est-à-dire protéger les données contre leur perte, accès, destruction, utilisation ou divulgation non autorisés.

· *transparence* (paragraphe 12 Lignes directrices de l'OCDE), c'est-à-dire que les engagements du maître du fichier doivent être exprimés de façon claire et facilement accessible à la clientèle ;

· *participation individuelle* (paragraphe 13 Lignes directrices de l'OCDE), c'est-à-dire que les personnes concernées doivent pouvoir obtenir copie des informations détenues sur lui par le maître du fichier et par toute autre personne. Ainsi il pourra soit les corriger, soit les compléter, voire demander leur destruction compte tenu du fait que les renseignements recueillis doivent faire l'objet de mises à jour pour éviter toute confusion ;

· *responsabilité* (paragraphe 14 Lignes directrices de l'OCDE), c'est-à-dire qu'en cas de non respect des principes énoncés ci-dessus, l'internaute pourra poursuivre le responsable d'un site Web donné pour atteinte à la vie privée.

### **Nations Unies**

Adoptées par l'Assemblée générale des Nations Unies<sup>7</sup>, les lignes directrices des Nations Unies établissent les garanties minimum de protection des droits de l'homme qui devraient figurer dans les législations nationales. Bien que dépourvues de valeur obligatoire, elles constituent un texte de référence. Elles se distinguent des lignes directrices de l'OCDE par la plus grande précision des garanties notamment en ce qui concerne les données sensibles. C'est en outre le premier instrument international à recommander la mise en place d'une autorité de contrôle (à la différence de la Convention n° 108 du Conseil de l'Europe). Les lignes directrices interdisent la collecte et le traitement de données selon des moyens déloyaux. Elles établissent les principes d'exactitude, d'adéquation, de finalité des données ainsi que les conditions d'exercice des droits d'accès et de rectification. Les seules exceptions sont celles nécessaires à la protection de la sécurité nationale, de l'ordre public, de la santé et de la moralité publiques ainsi que des droits et libertés des personnes (en particulier celles qui sont persécutées). Les données doivent circuler librement entre les Etats lorsque ceux-ci offrent des garanties comparables.

### **Organisation Mondiale du Commerce**

L'article 14 du traité du GATT du 15 avril 1994 concernant les échanges mondiaux de services admet la possibilité de dérogation au principe d'ouverture des marchés pour des motifs relevant du respect de la vie privée.

---

<sup>7</sup> Résolution numéro 45/95 du 14 décembre 1990

Les lignes directrices de l'OCDE, rédigées il y a plus de 20 ans servent de référence constante au plan international et constitue la base tant de la réglementation juridique que de l'autorégulation.

Les grands principes de la protection de la vie privée ont été confirmés tant par le Conseil de l'Europe que par l'Union Européenne

### **Conseil de l'Europe**

Le Conseil de l'Europe qui regroupe les pays européens entendu au sens large a adopté la Convention 108 qui établit des "Principes de base pour la protection des données". Ces principes, tout comme ceux des Lignes directrices de l'OCDE, reflètent les domaines qu'il convient de respecter dès que l'on veut collecter des renseignements personnels, à savoir par exemple :

- **la qualité des données** (article 5 Convention 108), cela signifie que la collecte doit être licite et loyale, pour des finalités spécifiées préalablement à la personne concernée, et l'utilisation de ces données ne doit pas contrevenir avec ce qui a été prévu à l'origine ;
- **la sécurité des données** (article 7 Convention 108), c'est-à-dire que tout risque de destruction, de perte, d'accès par des personnes non autorisées aux données personnelles recueillies doit être évité par l'adoption de mesures de sécurité ;
- **les garanties complémentaires pour la personne concernée** (article 8 Convention 108), c'est-à-dire que l'internaute doit avoir la possibilité d'accéder, de modifier, d'effacer sur simple demande les données le concernant. En cas de refus, celui-ci peut engager des poursuites contre le gestionnaire du site Web.

### **Union européenne**

La directive 2002/58/CE du Parlement et du Conseil concernant la protection des données personnelles dans le secteur des communications électroniques a été adoptée le 12 juillet 2002. Les Etats membres doivent se conformer à la directive avant le 31 octobre 2003.

En matière de protection de l'internaute, les députés européens ont choisi l'"opt-in", c'est-à-dire l'obligation de l'accord préalable de l'utilisateur contre l'envoi de messages commerciaux non sollicités (spamming).

L'utilisation de "cookies", ces petits logiciels espions utilisés sur Internet pour enregistrer l'activité et les habitudes de navigation des internautes, a été autorisée sous condition que les utilisateurs soient clairement informés de leur objet, et puissent les refuser.

La directive précise enfin que les données relatives aux abonnés "ne peuvent être stockées que dans la mesure où cela est nécessaire à la fourniture du service, aux fins de la facturation et des paiements pour interconnexion, et ce, pour une durée limitée".

## **La réglementation nationale**

Le modèle du cyberspace se distingue complètement du monde physique, sans frontières nationales ni juridiques, il ne comporte aucune hiérarchie. Pourtant, il doit s'accommoder des réalités des juridictions nationales et notamment les droits pré-existants, la réglementation "off-line" s'adaptant aux espaces "on-line".

### **L'adaptation du droit de la presse au réseau**

En France, la loi sur la presse de 1881 et celle du 30 septembre 1986 sur la communication audiovisuelle sanctionnent les délits commis par voie de la presse "ou par tout autre moyen de publication". Ces textes trouvent donc leur application dans le cadre de la diffusion du Internet à l'exception des messages de correspondance privée. Sont donc concernés les messages diffusés par un site web ou encore dans le cadre d'un forum, bien qu'il existe une distinction entre forum ouvert et forum fermé.

La loi de 1881 vise la diffamation, l'injure ainsi que les discriminations fondées sur la race, la religion, l'ethnie ou la nationalité.

### **Droit de l'informatique et des libertés : protection des données personnelles**

La notion de protection des renseignements personnels, est reconnue aussi bien dans les textes régionaux, nationaux et internationaux. Lorsque des données de tous types sont demandées, il est primordial de fournir des garanties et des informations spécifiques sur la manière dont elles seront utilisées. Garantir la protection des données personnelles dans l'environnement numérique c'est instaurer un climat de confiance en garantissant la protection de ces renseignements sous leur forme numérique.

Pendant les années 70, les pays d'Europe, les Etats-Unis et le Canada, adoptent une loi générale s'appliquant aux données personnelles.

- Suède, mai 1973, loi sur le traitement automatisé des informations nominatives
- Etats-Unis, janvier 1974, Privacy Act concernant les fichiers détenus par les administrations fédérales
- Allemagne, novembre 1976, loi fédérale sur le traitement automatisé des informations nominatives
- France, janvier 1978, loi informatique et libertés
- Norvège, 1978, loi sur les registres de données personnelles

### **Encadrement par le haut, contrôle par le bas**

Pour sauvegarder la vie privée, la plupart des législations « informatique et libertés » ont consacré une double approche de la protection des données :

- Un contrôle exercé, par le haut, par les autorités indépendantes : ce contrôle sur les fichiers et les traitements est exercé en amont (déclaration ou demande d'autorisation selon le statut, public ou privé de l'organisme selon la nature des données et des traitements eux-mêmes)

En France, la loi relative à l'informatique, aux fichiers et aux libertés de 1978 a créé la CNIL (Commission Nationale de l'Informatique et des Libertés) qui est une Autorité indépendante chargée de l'enregistrement des projets de traitement de données en conformité avec la loi nationale.

En Allemagne, la loi fédérale du 21 janvier 1977 a créé une « Autorité de supervision », une procédure d'enregistrement et un Commissaire fédéral à la protection.

Les autorités publiques telle que la CNIL en France, ont vu leur champ d'action s'élargir naturellement au cyberspace, les institutions préexistantes ont du s'adapter au monde des réseaux.

- et en aval (contrôle *a posteriori*) un contrôle exercé, par le bas, par les personnes elles-mêmes : à travers les droits d'information et d'opposition, d'accès et de rectification et d'opposition, à travers les droits d'information, d'accès, de rectification et même d'opposition<sup>8</sup>.

### **Droit à l'information préalable**

Le contrôle par l'individu des données qui le concernent suppose de sa part la connaissance des fichiers dans lesquels il est recensé. Ce droit à l'information préalable conditionne l'exercice des autres droits tels que le droit d'accès ou d'opposition.

Il se manifeste par :

- une obligation d'information au moment de la collecte des données : lors du recueil de données nominatives, la personne doit être informée du caractère obligatoire ou facultatif des réponses, des conséquences d'un défaut de réponse, des destinataires des informations ainsi que de l'existence d'un droit d'accès.
- la transparence des traitements automatisés :

### **Le droit d'accès**

Le droit d'accès donne à toute personne la possibilité de connaître l'existence ou non de données la concernant dans un fichier automatisé ou manuel et, si elle le désire, d'en obtenir communication. L'exercice de ce droit permet à l'individu de contrôler l'exactitude des données stockées sur son compte et, au besoin, de les faire rectifier ou effacer. Le droit d'accès s'exerce directement par l'individu auprès de l'organisme détenteur d'informations le concernant<sup>9</sup>.

### **Droit de rectification**

Le droit de rectification constitue un complément du droit d'accès.

### **Droit d'opposition**

Toute personne peut décider elle-même de l'utilisation de données la concernant et a donc la possibilité de s'opposer à figurer dans certains fichiers ou de refuser la communication des informations qui la concernent à des tiers

Il existe différentes formes d'expression de ce droit d'opposition :

- le refus de répondre lors de la collecte non obligatoire de données ;
- la nécessité de donner son accord écrit pour le traitement de données sensibles telles que les opinions politiques ou les convictions religieuses
- la faculté de demander la radiation des données contenues dans les fichiers commerciaux ou de vente par correspondance ;
- la possibilité d'exiger la non-cession ou la non-commercialisation des informations.

Le droit d'opposition comporte deux limites :

- son exercice est subordonné à l'existence de raisons légitimes ;
- il n'existe pas pour de nombreux traitements du secteur public.

---

<sup>9</sup> La communication des données doit être fidèle au contenu des enregistrements et effectuée en langage clair. Une copie des enregistrements peut être obtenue à la demande moyennant l'acquittement d'une redevance (20 francs pour le secteur public et 30 francs pour le secteur privé) (arrêté du 23 septembre 1980).

Le non-respect de l'opposition pour raisons légitimes d'une personne à un fichage est sanctionné pénalement.

Ces droits d'accès, de rectification et d'opposition ont notamment été consacrés par la loi italienne sur la protection de la vie privée :

#### Italie

La version consolidée de la loi sur la protection de la vie privée du 31 décembre 1996, définitivement adoptée le 28 décembre 2001, est entrée en vigueur le 1er février 2002. Plusieurs des articles de cette loi, qui transpose en droit italien la directive européenne de 1995 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, renforcent la protection de la vie privée des consommateurs. Ainsi, les différents secteurs de l'industrie intervenant dans le secteur du commerce électronique doivent se conformer aux dispositions d'un code de conduite. Cette nouvelle loi repose principalement sur le respect de l'exercice par les intéressés du droit de contrôle, de correction et d'annulation d'informations sur la personne. Par ailleurs, leur consentement préalable est requis pour toute utilisation des données personnelles les concernant. Enfin, les pouvoirs du "Garante", la Commission italienne de protection des données, sont renforcés.

#### Albanie

Loi, numéro 8517 du 22 juillet 1999 prise en application des articles 35, 78 et 81.1 de La Constitution de la République d'Albanie, sur la protection des données et informations à caractère personnel. Cette loi interdit l'utilisation des données personnelle sans autorisation.

#### Macédoine

La Macédoine a adopté une loi sur la protection des données personnelles en 1994

#### Roumanie

La Roumanie a transposé la Directive 95/46/CE du Parlement européen et du Conseil le 24 octobre 1995 en adoptant une loi relative à la protection des données personnelles

Ainsi, les Etats ont créer de nouveaux cadres réglementaires ou adapté les cadres juridiques existants pour assurer le respect de la vie privée et la protection des données personnelles. Pourtant, ces droits nationaux rencontrent des limites pratiques d'application.

## **Les nouvelles formes de régulation**

Les processus d'autorégulation et de co-régulation ont pour fonction d'actualiser, d'adapter et de particulariser les règles de droit.

### **L'auto-régulation**

Le réseau Internet mondial est un espace dans lequel les règles sont particulièrement souples et son bon fonctionnement repose essentiellement sur la responsabilité des acteurs (entreprise, gouvernements, consommateurs). L'auto-régulation, généralement élaborée et mise en œuvre plus rapidement que les lois conventionnelles est aussi plus souple ce qui lui permet d'évoluer de paire avec les technologies.

Le modèle américain s'appuie sur des méthodes inspirées par la logique du marché et plus généralement de l'initiative privée dont fait partie l'auto-régulation (privacy policies). L'opposition entre le système européen et le système américain a été exacerbé par l'article 25 de la directive européenne de 1995, qui dispose qu'à défaut de protection adéquate, les données personnelles collectées en Europe ne pouvaient être exploitées commercialement en dehors de l'Union. Le conflit a

été conclu par l'adoption par les deux parties du concept de *safe harbour*. Il s'agissait pour l'Europe et les Etats-Unis de s'accorder sur un système de label donné par un organe certificateur.

Pourtant, même aux Etats-Unis, adeptes de la pure autorégulation, l'intervention publique pour la protection de la vie privée a été nécessaire avec notamment la création de la Federal Data Protection Agency. De même, le Canada a adopté le 13 avril 2000 une nouvelle loi sur la protection des informations personnelles et les documents électroniques destinée à entrer en vigueur au 1er janvier 2001<sup>10</sup>.

### **La co-régulation**

La co-régulation, ou régulation coopérative, se base sur un accord entre les entreprises, les consommateurs, les professionnels, les administrations publiques ou encore la société civile. La co-régulation peut limiter les pratiques contestables par une intervention complémentaire à la mise en œuvre du dispositif législatif et réglementaire

La co-régulation en matière de protection de la vie privée sur Internet est mise en œuvre à titre d'exemples par :

- l'élaboration de codes de bonnes conduites, notamment dans les pratiques commerciales
- la définition de codes déontologiques
- la mise en œuvre de codes de bonnes pratiques dans le domaine de la protection des données personnelles

En janvier 1998, l'AFA (Association des fournisseurs d'accès et de services internet) a publié des « Pratiques et usages »<sup>11</sup> afin de « préciser le cadre dans lequel ses membres exercent leurs activités, décrire les usages qui sont les leurs, et attester de la relation de confiance qu'ils entretiennent avec leurs utilisateurs ». Parmi les principes communs à ses membres, outre les règles de la netiquette, elle a posé notamment des principes de confidentialité (respect de la correspondance privée) et de protection des mineurs.

### **La mise en œuvre effective du droit à la vie privée**

Toute opération sur Internet laisse des traces informatiques, qui permettent si elles sont exploitées de constituer des banques de données très riches en données personnelles.

### **Technologies protectrices de la vie privée**

Les technologies protectrices de la vie privée sont perçues comme une méthode pour rendre effectif le droit à la vie privée. Pour les juristes américains, il s'agit d'une incorporation du droit dans la technologie (la technologie rendant exécutoire la loi).

#### **Les technologies protectrices de vie privée**

- Progiciels de chiffrement des méls et des documents joints ;
- Cryptologie
- Stéganographie : technique qui consiste à dissimuler un message à l'intérieur d'un autre fichier;
- Génération de méls temporaires. Le texte des courriers n'est plus lisible passé un certain laps de temps ;
- Génération de méls non rediffusables. Le destinataire du message ne peut pas le faire suivre à d'autres destinataires.

<sup>10</sup> Cf. <http://e-com.ic.gc.ca/>

<sup>11</sup> Cf. [http://www.afa-france.com/html/action/index\\_usages.htm](http://www.afa-france.com/html/action/index_usages.htm)

- Services d'anonymisation de la navigation. Pour visiter les sites web sans laisser de traces susceptibles de faciliter l'identification du visiteur;
- *Remailer* (re-achemineur), service qui permet d'envoyer des messages sans que le destinataire puisse identifier l'émetteur;
- Services d'anonymisation des interventions sur les forums de discussion;
- Les gestionnaires d'identité virtuelle. Approche qui consiste à créer des personnalités virtuelles qui ne peuvent être rattachées à l'identité réelle de l'auteur. Ces personnes virtuelles peuvent alors consommer et communiquer sous un pseudonyme ;
- Cryptage des conversations en messagerie instantanée (*chat*) ;
- *Firewall* (logiciel pare-feu) personnel pour micro-ordinateur pour identifier la présence de *cookies* ou des *spywares*, voire pour en interdire l'accès;
- Progiciels de suppression des « traces » présentes sur l'ordinateur, par exemple les *cookies* ou le cache ;
- Progiciel de cryptage d'informations figurant sur le PC, par exemple les « favoris » ;
- Externalisation des données personnelles sur un disque dur distant ;
- Progiciels *anti-spam*, pour filtrer les courriers électroniques non sollicités.

(Source : ePrivacy, Arnaud Belleil, Dunod, 2001)

## **Les responsabilités des acteurs**

La chaîne qui va de l'émetteur d'une information jusqu'au récepteur final comporte un certain nombre d'intermédiaires techniques, variable en fonction du service Internet impliqué : les fournisseurs de contenus<sup>12</sup>, les fournisseurs d'accès<sup>13</sup>, les fournisseurs d'hébergement, les opérateurs... Ces intermédiaires assurent en particulier le transport et le stockage d'informations. Qu'en est-il de leur responsabilité face aux atteintes à la protection des données personnelles et de la vie privée ?

### **Union Européenne**

La directive sur le commerce électronique en date du 8 juin 2000 exonère de toute responsabilité les intermédiaires qui jouent un rôle technique en assurant le "simple transport" d'informations provenant de tiers (fournisseurs d'infrastructure et d'accès) et limite la responsabilité des prestataires de services pour les activités de stockage d'information (fournisseurs d'hébergement). Ces derniers sont exonérés de toute responsabilité pour les informations stockées sur leurs serveurs à condition :

a) qu'ils n'aient pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages-intérêts, qu'ils n'aient pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente ; ou

b) dès le moment où ils ont de telles connaissances, qu'ils agissent promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

---

<sup>12</sup> Les fournisseurs de services internet ("ISP", pour *Internet Service Providers*), qui mettent à disposition les outils et services permettant de construire un site Web et s'occupent de l'exploitation technique du serveur, bien souvent en louant un espace sur des machines qu'ils possèdent.

<sup>13</sup> Les fournisseurs d'accès Internet permettent aux utilisateurs (particuliers) et entreprises de se connecter au réseau. On distingue généralement trois niveaux de fournisseurs d'accès internet (FAI) : les détaillants (abonnés individuels ou très petits établissements), les grossistes (connexions d'entreprises) et les "colonnes vertébrales" (*backbones*) dont les clients sont pour l'essentiel les fournisseurs d'accès des deux autres catégories.

La Directive précise que les Etats membres ne doivent pas imposer aux prestataires une obligation générale de surveiller les informations qu'ils transmettent ou stockent.

### **France**

En France, le projet de loi pour la confiance dans l'économie numérique en cours d'adoption précise ou modifie les obligations et le régime de responsabilité actuellement prévus par la loi du 1er août 2000 modifiant la loi du 30 septembre 1986 relative à la liberté de communication.

Le projet de loi met en place un régime dérogatoire de responsabilité pour ces prestataires :

- Il précise que les *prestataires qui se bornent strictement à assurer la transmission* d'une communication sans aucune intervention sur le contenu, et notamment les fournisseurs d'accès, ne peuvent voir leur responsabilité engagée en raison des contenus qu'ils transmettent ou auxquels ils donnent accès.
- De même, les prestataires qui, de manière neutre et légitime, *stockent temporairement, automatiquement et à titre intermédiaire des contenus* en vue de rendre plus efficace leur transmission ne peuvent voir leur responsabilité engagée à ce titre. En revanche, leur responsabilité pourra être engagée s'ils n'ont pas agi promptement pour retirer du réseau les contenus qu'ils stockent ou pour en rendre l'accès impossible dès qu'ils ont eu effectivement connaissance que ces contenus doivent être retirés du réseau.
- Par ailleurs, le projet de loi consacre le principe en vertu duquel *les fournisseurs d'accès et d'hébergement* "ne sont pas soumis à une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites". Cette précision est conforme à la directive sur le commerce électronique, met définitivement.

Néanmoins, bien que dégagés de cette obligation générale de surveillance a priori, les fournisseurs d'hébergement n'en restent pas moins soumis à une obligation d'appréciation a posteriori de la licéité des contenus qu'ils hébergent.

Le projet de loi étend les obligations pour les hébergeurs d'apprécier a posteriori la licéité des contenus

- de la responsabilité civile des hébergeurs aux cas où, "dès le moment où ils ont eu la connaissance effective de leur caractère illicite, ou de faits et circonstances faisant apparaître ce caractère illicite, ils n'ont pas agi avec promptitude pour retirer ces données ou rendre l'accès à celles-ci impossible" ;
- de la responsabilité pénale des hébergeurs aux cas où "en connaissance de cause, ils n'ont pas agi avec promptitude pour faire cesser la diffusion d'une information ou d'une activité dont ils ne pouvaient ignorer le caractère illicite".

### ***Doit-on appliquer à Internet une règle de responsabilité en cascade ?***

Est-ce que les règles établissant une responsabilité en cascade dans les médias traditionnels s'appliquent à Internet ?

En France, la loi sur la liberté de la presse de 1881 prévoit un système de responsabilité en cascade. Les directeurs de publication ou éditeurs sont responsables et à défaut, les auteurs, à défaut des auteurs, les imprimeurs, à défaut des imprimeurs les vendeurs, les distributeurs et la afficheurs. L'assimilation des sites web à des services de communication audiovisuelle a conduit les tribunaux, à plusieurs reprises, à faire application du système de responsabilité en cascade.

Aux Pays-Bas, les articles 53 et 54 du Code pénal créent une forme de responsabilité en cascade pour le domaine de l'écrit qui exonèrent l'éditeur ou l'imprimeur.

En Belgique, la règle de la responsabilité en cascade (article 25, alinéa 2 de la Constitution) vaut uniquement pour le domaine de l'écrit. Cette règle oblige d'assigner d'abord l'auteur s'il est connu et domicilié en Belgique. Ce n'est qu'à défaut que l'on peut se retourner contre l'éditeur, l'imprimeur puis le distributeur.

## Liens

### Textes législatifs

- OECD Working Party on Information Security and Privacy : Privacy Online - Policy and practical Guidance, 21 January 2003 - DSTI/ICCP/REG(2002)3/FINAL - [http://www.oelis.oecd.org/olis/2002doc.nsf/43bb6130e5e86e5fc12569fa005d004c/942914d87a941e54c1256cad004ed52a/\\$FILE/JT00137976.PDF](http://www.oelis.oecd.org/olis/2002doc.nsf/43bb6130e5e86e5fc12569fa005d004c/942914d87a941e54c1256cad004ed52a/$FILE/JT00137976.PDF)
- OCDE Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptées le 23 septembre 1980 - <http://www.oecd.org/FR/longabstract/0,,FR-longabstract-0-nodirectorate-no-24-11159-0,00.html>
- OCDE Déclaration sur les flux transfrontières de données, 11 avril 1985 <http://www.oecd.org/EN/document/0,,EN-document-0-nodirectorate-no-4-22734-0,00.html>
- Recommandations de l'ONU. Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel. Adoptés le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990 [http://www.unhchr.ch/french/html/menu3/b/71\\_fr.htm](http://www.unhchr.ch/french/html/menu3/b/71_fr.htm)
- Déclaration d'Ottawa relative à la protection de la vie privée sur les réseaux, 1998 – [http://appli1.oecd.org/olis/1998doc.nsf/4cf568b5b90dad994125671b004bed59/61c1c8c0a31f9457c12566de00506c13/\\$FILE/12F81014.DOC](http://appli1.oecd.org/olis/1998doc.nsf/4cf568b5b90dad994125671b004bed59/61c1c8c0a31f9457c12566de00506c13/$FILE/12F81014.DOC)
- Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) - [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FR&numdoc=32002L0058&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FR&numdoc=32002L0058&model=guichett) et [http://www.europa.eu.int/eur-lex/fr/dat/2002/l\\_201/l\\_20120020731fr00370047.pdf](http://www.europa.eu.int/eur-lex/fr/dat/2002/l_201/l_20120020731fr00370047.pdf)
- Italie - Loi n° 675/96 du 31 décembre 1996 : [http://www.angap.it/legge/l67596\\_idx.htm](http://www.angap.it/legge/l67596_idx.htm)
- Document de la CNIL recensant les textes législatifs à travers le monde concernant la protection des données personnelles. Mis à jour en avril 2002. <http://www.cnil.fr/thematic/docs/international/intmontabl.pdf>

### Rapports

Guy Braibant. Données personnelles et société de l'information. Rapport au premier ministre sur la transposition en droit français de la directive 95/46/CE. La Documentation Française, 1998 <http://www.ladocumentationfrancaise.fr/BRP/984000836/0000.pdf>

Privacy online : Policy and practical guidance/OCDE, 21 janvier 2003 [http://www.oelis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-iccp-reg\(2002\)3-final](http://www.oelis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-iccp-reg(2002)3-final)

L'exercice de la liberté d'expression dans le cyberspace : le défi d'assurer l'application effective des droits proclamés/Pierre Trudel, 2002 [http://www.unesco.org/comnat/france/Colloque\\_liberte\\_expression\\_2002/P\\_Trudel.pdf](http://www.unesco.org/comnat/france/Colloque_liberte_expression_2002/P_Trudel.pdf)

### Articles

Internet et vie privée entre risques et espoirs/Yves Poulet. Le Journal des Tribunaux, 17 février 2001, numéro 6000

[http://www.droit-technologie.org/dossiers/JT6000\\_internet\\_et\\_vie\\_privée.pdf](http://www.droit-technologie.org/dossiers/JT6000_internet_et_vie_privée.pdf)

Libertés individuelles et libertés publiques/IRIS, octobre 1997

<http://www.iris.sgdg.org/documents/rapport-ce/html-css.html>

Protection de la vie privée sur Internet/Yves Deswarte

<http://www.urec.cnrs.fr/securite/CNRS/vCARS/DOCUMENTS/Deswarte-int2.pdf>

Comparaison des différentes législations sur la protection des données personnelles, par Gavina Gallier. Legalbiznext, mai 2002

<http://www.legalbiznext.com/cgi-bin/news/viewnews.cgi?category=8&id=1022661448>

Société d'information et vie privée/Groupe de travail coordonné par M. Pierre Tabatoni, membre de l'Académie, dans le cadre d'ALLEA (All European Academies)

<http://www.asmp.fr/sommair6/gpw/internetvieprivée/accueil.html>

<http://www.internet.gouv.fr/francais/textesref/pagsi2/lsi/rapportcpaul/sommaire.htm>