# La protection des données personnelles en France


## Cynthia CHASSIGNEUX (*)



***Lex Electronica*, vol. 6, n°2, Hiver / Winter 2001**



**Synopsis**

The notion of privacy, and more precisely the right to the protection of personal information, is recognized in provincial, national and international legislation, as well as in policies created by Web sites. It has been acknowledged that the unauthorized distribution of personal, identifying information, such as a person's name, phone number, bank card, social security number, or even Internet address or e-mail, can be regarded as breach to this person's right to privacy. Traditional methods which protect one's privacy, must adapt and extend their protection in the realm of cyberspace, since " computers (...) must not affect human identity, human rights, privacy or individual and public rights " (art. 1 of the French " Informatique et Libertés " January 6th 1978 law).

Although the importance of securing our privacy is agreed upon, it is necessary to question ourselves on the means that must be put forth to reach it. Shall we fall back on State legislation, on self-regulation or on co-regulation? This last notion « *is not, for say, a new form of regulation* », it simply draws from the collaboration of both the private and public sectors. This system of partnership attracted the attention of the French Government, and have influenced it's effort to adapt it's legislative framework to the information society, as is shown by the report « Du droit et des libertés sur l'Internet », recently handed to the Prime minister.

As a result, this article aims to illustrate the development of French legislation applied to the protection of privacy and, more precisely, to the personal information found on the World Wide Web. While keeping in consideration solutions put forth by the State or the private sector which have been utilized for the last two decades, we will study the first draft of the government's law concerning the protection of personal data, that aims to incorporate the European Directive européenne of October 24th 1995 into state legislation.

**Résumé**

La notion de vie privée, et plus précisément le droit à la protection des renseignements personnels, est reconnue aussi bien dans les textes provinciaux, régionaux, nationaux et internationaux, que dans les politiques mises en place par les sites Web. Il est admis que toutes informations identifiant ou permettant d'identifier une personne peut porter atteinte à sa vie privée, à savoir son nom, prénom, numéro de téléphone, de carte bancaire, de sécurité sociale, ou encore ses adresses électronique et Internet. Cette protection, admise dans le monde réel, doit aussi exister sur les inforoutes, étant entendu que « *l 'informatique*

*(…) ne doit porter atteinte ni à l ’identité humaine, ni aux droits de l ’homme, ni à la vie privée, ni aux libertés individuelles ou publiques* » (art. 1er de la Loi française dite « Informatique et Libertés » du 6 janvier 1978).

Ce principe étant admis, il est pertinent de s’interroger sur les moyens envisagés pour parvenir à le réaliser. Faut-il avoir recours à la réglementation étatique, à l’autoréglementation ou à la corégulation ? Cette dernière notion « *n’est pas à proprement parler une nouvelle forme de régulation* », mais elle préconise une collaboration entre les acteurs du secteur public et privé. L’idée de partenariat semble retenir l’attention du gouvernement français dans sa mission d’adaptation du cadre législatif à la société de l’information, comme nous le montre le rapport *Du droit et des libertés sur l’Internet* remis dernièrement au Premier ministre.

Par conséquent, cet article a pour objectif de dresser un tableau de la législation française, et de ses multiples rapports, applicables à la protection de la vie privée et, plus particulièrement, aux données personnelles sur le réseau des réseaux. En prenant en considération les solutions étatiques et non étatiques retenues depuis ces deux dernières décennies, nous envisagerons une étude de l’avant-projet de loi du Gouvernement visant à transposer en droit interne la Directive européenne du 24 octobre 1995 relative à la protection des données personnelles.

## Table des matières

**Introduction**

1. La Directive n° 95-46 du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Directive 95/46/CE) énonce en son article 32 § 1 que " *les Etats membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard à l'issue d'une période de trois ans à compter de son adoption* "[1], à savoir le 24 octobre 1998[2]. Toutefois, pratiquement deux ans après son entrée en vigueur, cinq Etats ne se sont pas encore conformés aux dispositions de la directive faisant ainsi l'objet de sanctions de la part de la Commission européenne[3].

2. Cette absence de transposition est remarquable car certains de ces Etats ont longtemps fait figure de pionniers en ce qui concerne la protection de la vie privée, et plus particulièrement des données personnelles. Ainsi, si nous prenons le cas de la France, nous pouvons dire que l'article 9 alinéa 1er du Code civil français, issu de l'article 22 de la loi n° 70-643 du 17 juillet 1970[4] et consacrant l'action prétorienne des juges se fondant jusqu'alors sur l'article 1382 du Code civil (responsabilité pour faute), stipule que " *chacun a droit au respect de sa vie privée* ". Par la suite, le législateur français tenant compte des critiques lancées à l'encontre des projets de l'administration[5] a adopté la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[6] disposant dans son article premier que " *l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ".

3. Cette loi qui encadre les dangers liés au développement de l'informatique tant dans le secteur public que privé est au centre des débats depuis l'entrée en vigueur de la Directive 95/46/CE. En effet, comment concilier les exigences nationales et communautaires, mais aussi internationales ? Comment concilier les solutions réglementaires avec l'élaboration de garanties complémentaires ? Comment parvenir à un accord entre les différents acteurs ? Même s'il est possible de multiplier à l'infini ces interrogations, il convient de préciser qu'elles ont toutes pour objectif d'assurer la protection des données personnelles quel que soit le support envisagé. Cette préoccupation est donc transposable à Internet. Elle est même accentuée du fait de la dimension transnationale du Réseau. Pour appréhender ce phénomène il suffit de parcourir l'actualité de ces dernières années pour comprendre comment l'utilisation des nouvelles technologies de l'information peut être source de dérives en ce qui concerne les données transitant sur Internet.

4. Ces atteintes loin d'être nouvelles (re)mettent cependant en cause la relation de confiance qui doit exister entre un commerçant et sa clientèle, entre un commerçant électronique et l'internaute-consommateur. Cette relation de confiance est nécessaire à tout échange de renseignements que ceux-ci soient professionnels ou comme en l'espèce personnels. En effet, les données personnelles qui, entre autres, regroupent non seulement les noms et prénoms, l'adresse postale, les numéros de téléphone, de carte bancaire, de sécurité sociale, la date de naissance, mais aussi les adresses électroniques et IP, font partie

intégrante de la notion de vie privée. Elles identifient ou permettent d'identifier, séparément ou collectivement, une personne, à son insu ou non.

5. Pour minimiser, voire faire cesser les risques d'atteintes relatives aux données personnelles, les notions de confiance et de sécurité sont souvent mises en avant dans les débats de la classe politique française, et internationale. Dès lors, prenant conscience que les solutions réglementaires, d'une part, et autoréglementaires, d'autre part, ne parviennent pas seules à garantir la sécurité des données personnelles compte tenu du caractère transnational, décentralisé et dématérialisé d'Internet, les autorités publiques préconisent l'adoption d'une nouvelle forme de régulation. Cette dernière faciliterait le dialogue entre les acteurs du secteur public et privé afin d'adapter le cadre législatif français à la société de l'information. On voit se mettre en place l'idée d'une co-régulation[7].

6. Cette co-régulation favorisera l'émergence d'un nouveau climat entre les pouvoirs publics et la régulation privée, climat qui aura des répercussions sur les relations entre les commerçants électroniques et les internautes-consommateurs. En effet, les internautes-consommateurs sont perdus face à la pluralité des protections s'offrant à eux en ce qui concerne la protection de leurs données personnelles sur Internet. Par conséquent, il est important, à l'heure où le législateur français entend transposer la Directive 95/46/CE en droit interne et réviser la *Loi Informatique et Libertés*, de dresser un état des protections accordées et reconnues. Ainsi, dans une première partie nous serons amenés à prendre en considération les règles nationales, communautaires et internationales pouvant garantir sur le territoire français la confidentialité des données personnelles de l'internaute (I). Cependant la référence à ces règles ne peut suffire à assurer la sécurité desdites données sur Internet, c'est pourquoi nous envisagerons, dans une seconde partie, le recours à des garanties complémentaires en tenant compte des enseignements étrangers (II).

## I. La protection réglementaire des données personnelles : une protection nécessaire mais non suffisante

7. Le caractère transnational, décentralisé et dématérialisé d'Internet favorise l'émergence de nouvelles règles remettant en cause le monopole normatif jusque là reconnu à l'État. Cette situation est, nous le reconnaissons, loin d'être nouvelle. Dans nos sociétés traditionnelles, aux côtés des normes étatiques, une dynamique sociale existe déjà faisant intervenir une multitude d'acteurs et de normes dans l'encadrement des relations et des comportements des individus. L'autorité étatique laisse ainsi entrouverte la porte à d'autres ordres normatifs qui peuvent être de nature sociale, éthique, déontologique, technique comme nous pourrons le constater dans la seconde partie de cet article.

8. Pour l'heure, nous devons nous intéresser aux protections réglementaires permettant de garantir la confidentialité des données personnelles sur Internet. Cette prise en compte peut s'expliquer non seulement par rapport à la relative nouveauté du Réseau, mais aussi eu égard au fait que " *le droit étatique demeure, à l'heure actuelle, la technique de réglementation la plus usuelle entourant les environnements électroniques* "[8].

9. Ainsi, à la veille de la transposition de la Directive 95/46/CE, il est possible de dire que l'internaute français peut s'attendre à ce que ses données personnelles soient protégées par les sites Web marchands qu'ils visitent en référence non seulement au droit national (A) et communautaire (B), mais aussi international (C).

**A. Le droit national**

10. La protection des données personnelles est principalement encadrée, en droit interne, par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après *Loi 1978* ou *Loi Informatique et Libertés*). Cette loi s'est inscrite dans un mouvement, venu d'Allemagne et de Suède[9], de protection des données personnelles face à l'informatisation grandissante de l'administration, mais aussi des entreprises privées. Dès lors, elle vise aussi bien le secteur public que privé (article 14*Loi 1978*), le premier étant soumis à un avis préalable (article 15 *Loi 1978*) alors que le second doit simplement déclarer ses intentions (article 16 *Loi 1978*) à la *Commission Nationale de l'Informatique et des Libertés* (CNIL)[10].

11. Cette distinction entre le secteur public et privé n'est plus de mise actuellement, le secteur privé cherchant lui aussi à connaître les moindres faits et gestes des internautes. *Big Brother* n'est plus seulement personnalisé par l'État, il a également le visage d'un commerçant électronique. C'est pourquoi la Directive 95/46/CE préconise que " *[…] le responsable du traitement, ou le cas échéant son représentant, doit adresser une notification à l'autorité de contrôle visée à l'article 28 préalablement à la mise en œuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées* " (article 18 Directive 95/46/CE) et, ce faisant " *[…] les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées* " devront faire l'objet d'un contrôle préalable de la part de l'autorité de contrôle (article 20 § 1 Directive 95/46/CE). Les secteurs public et privé seront donc soumis aux même exigences.

12. Une fois cette précision apportée, il convient de revenir sur l'essence même de la *Loi Informatique et Libertés* qui est de protéger les individus contre les risques liés aux traitements automatisés de leurs informations nominatives, c'est-à-dire des données " *[…] qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale* " (article 4 *Loi 1978*). Ainsi sont concernés " *tout ensemble d'opérations réalisées par les moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives* " (article 5 *Loi 1978*).

13. Dès lors, pour que la collecte des informations nominatives se fasse dans les meilleures conditions possibles, le responsable du site Web marchand doit respecter certaines

obligations et accorder des droits à l'internaute. Le respect de ces principes favorisera un climat de confiance nécessaire à toutes transactions en ligne.

14. Ainsi, le responsable du site Web marchand devra, préalablement à la collecte, demander le consentement de l'internaute et l'informer des finalités du traitement. Devrons donc être mentionnés les renseignements qu'il souhaite collecter étant entendu qu'il ne peut demander des données sans relation avec le traitement. Il devra également indiquer les méthodes utilisées pour y parvenir (formulaire d'inscription ou de commande ; sondage ; concours ; correspondance ; fichiers journaux ; fichiers témoins ; etc...) et les raisons de cette collecte (suivi de la commande ; envois d'informations et d'offres promotionnelles ; statistiques ; communication à des tiers ; etc.). L'ensemble de ces précisions, exprimées à l'article 6 § 1 de la Directive 95/46/CE, sont nécessaires dans le cadre du commerce électronique et de la protection des données personnelles. Le législateur lors de la transposition de la Directive 95/46/CE devra donc pour compléter l'article 27 de la *Loi Informatique et Libertés* s'inspirer des mentions contenues à l'article 6 § 1 de la Directive 95/46/CE :

*" Les Etats membres prévoient que les données à caractère personnel doivent être :*

*(...)*

*b) collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. (...) ;*

*c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ;*

*(...) "*

15. Cette information préalable est nécessaire, mais elle ne sera complète que si le responsable du site Web accorde à l'internaute un droit d'opposition et d'accès aux informations nominatives le concernant contenues dans les bases de données du site Web.

16. Le premier de ces droits, le droit d'opposition, est prescrit à l'article 26 de la *Loi Informatique et Libertés* : " *toute personne physique a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement* ". Ce droit doit pouvoir s'exercer non seulement au moment de la collecte, mais aussi postérieurement à celle-ci. Dans le premier cas, l'internaute peut refuser de communiquer ses informations dès qu'il est en présence d'un document électronique lui demandant de fournir des renseignements personnels. Le plus souvent il mettra alors fin à sa session sur le site Web. Il peut aussi accepter de donner ses informations mais s'opposer alors à leur divulgation auprès des tiers. Pour ce faire, il activera ou désactivera l'option qui lui est offerte par le responsable du site Web. On parle ici de la technique du *opt-in*.

17. Dans le second cas, l'internaute peut demander que cesse le traitement de ses informations nominatives pour les fins mentionnées lors de la collecte. On fait alors

référence à un droit de retrait ou encore à la technique du *opt-out*. Pour ce faire, l'internaute adressera sa requête par voie postale ou électronique selon les possibilités offertes par le responsable du site Web.

18. Le second de ces droits, le droit d'accès fait l'objet du " Chapitre V : Exercice du droit d'accès " de la *Loi Informatique et Liberté*. Les informations nominatives faisant partie des droits de la personnalité, il est important que les internautes puissent connaître quels sont les renseignements les concernant susceptibles d'être détenus par un commerçant électronique, voire par un tiers. Ainsi, " *toute personne justifiant de son identité a le droit d'interroger les services ou organismes chargés de mettre en œuvre les traitements automatisés dont la liste est accessible au public en application de l'article 22 ci-dessus en vue de savoir si ces traitements portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir communication* " (article 34 *Loi 1978*). Ce droit d'accès ne saurait être total si la loi n'accordait pas au titulaire du droit la possibilité de modifier les informations nominatives qu'un commerçant électronique détient dans sa base de données. Ce sont ces informations qui sont contenues dans le profil de l'internaute et qui seront communiquées à des tiers. Il est donc normal que l'internaute puisse " *[...] exiger que soient rectifiées, complétées, mises à jour ou effacées les informations le concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte ou l'utilisation, la communication ou la conservation est interdite* " (article 36 *Loi 1978*).

19. Nous venons de voir que le respect des principes relatifs à l'information préalable, aux droits d'opposition et d'accès est un élément clé de la relation de confiance devant s'instaurer entre le commerçant électronique et l'internaute-consommateur. Toutefois, il convient d'insister aussi sur le besoin de sécurité. En effet, pour pouvoir transmettre des informations nominatives, les internautes doivent avoir le sentiment qu'aucun danger n'est à craindre, que le gestionnaire du site Web protège les informations tant au niveau de leur communication lors de la collecte que de leur stockage dans les bases de données. Ainsi, il est important que le responsable du site Web " *[...] s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés* " (article 29 *Loi 1978*). Nous reviendrons sur les mesures de sécurité pouvant être adoptées dans la seconde partie de cet article.

20. « Information préalable », « droits d'opposition et d'accès » et « sécurité » sont les moteurs de la protection des données personnelles sur Internet comme nous l'a démontré l'étude de la *Loi Informatique et Liberté*. Ce souci ne se limite pas à la seule dimension nationale, il se retrouve également au niveau communautaire, comme nous avons déjà pu l'entrevoir, et international. De plus, Internet étant un réseau transnational, il est important de prendre en considération les instruments juridiques communautaires et internationaux pouvant s'appliquer à la protection des données personnelles sur le territoire français.

**B. Le droit communautaire**

21. L'Union européenne, dont la mission est de promouvoir un équilibre économique et social durable entre les États membres[11], a adopté le 24 octobre 1995 la Directive

95/46/CE[12]. Les directives sont des actes qui, d'une part, visent à harmoniser les législations et les réglementations nationales et, d'autre part, posent une obligation de résultat aux États membres.

22. La Directive 95/46/CE vise à concilier la protection des données à caractère personnel avec la libre circulation de celles-ci non seulement au sein de l'Union européenne, mais aussi en dehors des frontières, c'est-à-dire en direction de pays tiers. Cette libre circulation ne pourra se faire, selon les termes de l'article 25 § 1 de la Directive 95/46/CE[13], que si ces derniers offrent " *un niveau de protection adéquat* ". Nous reviendrons plus tard sur cette notion qui peut avoir des répercussions sur le transfert des données sur Internet.

23. Au préalable, il convient de préciser que la Directive 95/46/CE a vocation, nonobstant le défaut de transposition, à s'appliquer " *au traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* " (article 3 § 1 Directive 95/46/CE). Nous remarquons que la Directive 95/46/CE emploie l'expression " données à caractère personnel "[14], là où la *Loi Informatique et Liberté*utilise celle d'" informations nominatives ". Cette distinction, qui peut sembler anodine, est à l'origine de nombreux débats doctrinaux[15], la définition de la Directive 95/46/CE englobant un trop grand nombre de données et risquant, par conséquent, d'affaiblir la protection elle-même. Quoi qu'il en soit, ces deux notions ont pour vocation de protéger les renseignements identifiant ou permettant d'identifier une personne physique et, ce, quel que soit le support utilisé.

24. À partir de là, nous pouvons dire que les données traitées doivent être adaptées aux finalités poursuivies et ne pas concerner l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle, à moins que la personne n'ait donné son consentement (article 8 § 1 et 2a) Directive 95/46/CE), ce dernier étant d'ailleurs requis pour toute collecte (article 7a) Directive 95/46/CE). De plus, l'internaute qui fait l'objet d'un traitement doit être tenu informé de l'identité des personnes qui seront en possession de ses données personnelles (article 10 Directive 95/46/CE) et en mesure d'exercer ses droits d'opposition (article 14 Directive 95/46/CE) et d'accès (article 12 Directive 95/46/CE). Enfin, tout comme en droit interne, le responsable du traitement " *[…] doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute forme de traitement illicite* " (article 17 § 1 Directive 95/46/CE).

25. Toutes ces mesures ont pour but d'assurer un niveau de protection adéquat pour les données personnelles tant au sein de l'Union européenne qu'au regard des pays tiers. En effet, le développement de l'informatique a permis l'interconnexion des fichiers, le partage des données, la transmission des renseignements personnelles d'un pays à l'autre. Or, cela doit se faire dans le respect des droits reconnus aux personnes faisant l'objet d'un traitement automatisé. C'est pourquoi, la Directive 95/46/CE insiste sur l'existence d'un

niveau de protection adéquat dans le pays destinataire desdites informations[16], ce qui a donné lieu à de nombreuses discussions entre l'Union européenne et les États-Unis relativement au secteur privé principalement soumis à l'autorégulation.

26. Un accord " sphère de sécurité " ou " *Safe Harbour Principles* "[17] est finalement intervenu entre les deux parties au mois de juin 2000, mais n'a réellement été adopté qu'en août 2000 lorsque la Commission européenne[18] a décidé de passer outre les recommandations du Parlement[19]. L'accord repose sur l'idée que le ministère du commerce américain dressera une liste des entreprises qui adhéreront et s'engageront publiquement à respecter un ensemble de règles protégeant les données personnelles. Les entreprises devront adresser une lettre mentionnant les coordonnées, les activités et la politique adoptée en matière de protection des données personnelles. Par la suite, le ministère pourra procéder à toutes vérifications et, en cas de fausse déclaration ou de non respect, l'organisme fera non seulement l'objet de sanctions légales mais sera également retiré de la liste des entreprises assurant une protection adéquate aux dites données

27. Pour certains commentateurs, cet accord signifie " une victoire des positions américaines, qui font confiance à l'autorégulation des entreprises et à la justice "[20], l'adhésion des entreprises étant volontaire. Cet accord signifie donc que l'Union européenne et les États-Unis s'entendent sur le contenu, non sur le contenant, de la protection à accorder aux données personnelles. En effet, même si l'image est schématique, il est possible de dire que les premiers sont plutôt favorables à une protection de type réglementaire, alors que les seconds recourent davantage à l'autoréglementation du secteur privé.

28. Toutefois, cette dualité s'amenuise ces derniers temps si l'on en juge, d'une part, de l'adoption de l'accord " de sphère de sécurité " et, d'autre part, de l'émergence de l'idée de co-régulation comme mentionnée dans le rapport Christian Paul. En effet, " *la corégulation doit s'appliquer à permettre la rencontre difficile entre le temps de l'Internet et le temps des institutions* "[21], c'est-à-dire entre les différents acteurs du Réseau. Dès lors, cette coopération devra se faire dans un environnement international afin d'arriver à un consensus comme ce fut le cas au début des années quatre-vingt lors de l'adoption des règles de l'Organisation de Coopération et de Développement Économiques (OCDE) et du Conseil de l'Europe.

**C. Le droit international**

29. L'une des caractéristiques d'Internet est d'être un réseau mondial, opérant en dehors de toute référence territoriale, il convient donc de se demander comment les normes internationales peuvent s'appliquer sur les inforoutes. Pour ce faire, il faut partir de l'idée que les traités internationaux sont, en principe, opposables aux parties dès leur ratification par celles-ci. Dès lors, la France ayant ratifié, d'une part, les Lignes Directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel[22] adoptées le 23 septembre 1980 par l'OCDE (Lignes directrices de l'OCDE) et, d'autre part, la Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[23] adoptée le 28 janvier 1981 par

le Conseil de l'Europe (Convention 108), ces textes peuvent être invoqués par les internautes dès que le traitement des données les identifiant ou permettant de les identifier est contraire aux principes établis par ces instruments internationaux[24].

1. Les Lignes directrices de l'OCDE

30. Les textes de l'OCDE sont le reflet d'un dialogue entre les pays membres mais, parfois, ceux-ci peuvent donner lieu à des discussions avec des pays non-membres. Ces échanges permettent un rapprochement et la communication de différents points de vue. En effet, pour avoir une vision globale, l'OCDE est tenu de considérer les influences du monde entier. Dans le même ordre d'idées, l'OCDE doit suivre les évolutions technologiques susceptibles d'avoir des répercussions sur le commerce et sur la société en générale.

31. Dès lors, les Lignes directrices de l'OCDE visant à harmoniser les législations nationales des pays signataires concentrent leur objectif sur la protection des données à caractère personnel qui circulent au-delà des frontières. Pour ce faire, elles préconisent un ensemble de principes technologiquement neutres et couvrant aussi bien le secteur public que privé[25], ce qui en fait un modèle dans le cadre de la protection des données personnelles. Ainsi, les États signataires et les entreprises voulant œuvrer sur le territoire de ces derniers doivent respecter certains principes relatifs à la collecte, à l'utilisation et à la gestion des données personnelles collectées. En effet, 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.

Cette obligation de sécurité se retrouve également dans les Lignes directrices relatives à la sécurité des systèmes d'information adoptées le 26 novembre 1992 par l'OCDE[26]. En effet, la mise en place de moyens sécuritaires tels que la cryptographie pour l'échange d'informations personnelles, en ligne est nécessaire non seulement pour garantir la confidentialité desdites informations, mais aussi pour rencontrer la confiance des internautes. Cette garantie de sécurité est de mise en ce qui concerne la transmission des données, d'une part, et le stockage de celles-ci dans les bases de données, d'autre part ;

· **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.

32. Au lendemain de l'adoption des Lignes directrices de l'OCDE, le Conseil de l'Europe a mis en place la Convention 108 qui, contrairement aux Lignes directrices de l'OCDE qui ne sont que de simples recommandations, sont contraignantes pour les pays signataires.

**2. La Convention 108 du Conseil de l'Europe**

33. Le Conseil de l'Europe regroupe les pays européens entendu au sens large et non pas seulement les quinze pays membres de l'Union européenne. Il ne s'agit donc pas d'un club fermé, mais d'une organisation internationale qui, en dehors des invités spéciaux et des observateurs que sont par exemple le Canada, l'État d'Israël, le Japon, le Mexique et les Etats-Unis, rassemble 41 pays membres.

34. La mission du Conseil de l'Europe est de débattre sur des questions de société. C'est dans le cadre de cette mission que le Conseil de l'Europe a adopté la Convention 108[27] qui a pour but " *[...] de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant* " (article 1er Convention 108) et ce que le secteur soit public ou privé (article 3 § 1 Convention 108).

35. Pour arriver à cet objectif, la Convention 108 a établi 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.

36. Il est également précisé que certaines données ne peuvent pas faire l'objet d'un traitement, à moins que ce dernier ne soit prévu en droit interne. Par conséquent, sont considérées comme des données sensibles, aux termes de l'article 6 de la Convention 108, celles " *[...] révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle (...). Il en est de même des données à caractère personnel concernant des condamnations pénales* ".

37. Pour finir, il convient de préciser que le principe émis à l'article 25 de la Directive 95/46/CE figurait déjà au titre des recommandations de l'OCDE (paragraphe 15 et suivants Lignes directrices de l'OCDE) et du Conseil de l'Europe (article 12 Convention 108) relatives aux flux transfrontières de données. Toutefois, les débats qui se sont ouverts autour de cette question et les solutions élaborées démontrent que la protection réglementaire des données personnelles doit s'accompagner de garanties complémentaires.

## II. La protection complémentaire des données personnelles : une protection indispensable pouvant connaître des limites

38. Nous venons de voir que la protection réglementaire des données personnelles sur Internet était nécessaire, mais non suffisante au regard de la dimension internationale et décentralisée d'Internet. C'est pourquoi, il convient de reconnaître l'existence de garanties complémentaires. Cette idée n'est pas seulement le fait des pays qui ne connaissent pas d'encadrement juridique des données personnelles, elle se rencontre également dans les pays favorables à une protection réglementaire desdites données. En effet, si nous prenons l'exemple de la France, le rapport du Conseil d'État[28], d'une part, souligne l'importance des garanties complémentaires afin de parvenir à une meilleure protection des données personnelles et, le rapport Christian Paul[29], d'autre part, préconise la mise en place d'un organisme de co-régulation des réseaux, associant acteurs publics et privés.

39. Partant de là, il convient de s'intéresser aux protections complémentaires pouvant s'appliquer aux inforoutes. Ces garanties sont souvent qualifiées d'autoréglementaires car elles sont le fruit des acteurs eux-mêmes. En effet, " *l'autoréglementation fait référence aux normes volontairement développées et acceptées par ceux qui prennent part à une*

*activité. La nature première des règles autoréglementaires est d'être volontaires, c'est-à-dire de ne pas être obligatoire au sens où l'est la règle de droit édictée par l'État. L'assujettissement à l'autoréglementation est généralement consenti par le sujet. Elle est fondamentalement de nature contractuelle. Le plus souvent, on consent à adhérer à des normes autoréglementaires parce que cela présente plus d'avantages que d'inconvénients* "[30].

40. Au titre de ces normes autoréglementaires, il est possible de mettre en avant celles faisant appel à l'élaboration de politiques de protection des données personnelles (A), aux sceaux de certification (B) et aux standards visant à la normalisation de la technique (C). L'ensemble de ces approches ont pour but de sécuriser et de garantir la confidentialité des informations personnelles pouvant circuler sur les autoroutes de l'information tout en renforçant le climat de confiance devant préexister entre l'internaute et le responsable du site Web.

**A. Les politiques de protection des données personnelles**

41. Il existe un adage selon lequel " nul n'est censé ignorer la loi ". Cependant, la dimension internationale d'Internet rend complexe l'application effective de ce dernier. Cette constatation est valable aussi bien pour l'internaute que pour le commerçant électronique. Dès lors, pour parer à ce phénomène en ce qui a trait à la protection des données personnelles, la plupart des sites Web établissent des engagements qui seront contenus dans des politiques de confidentialité et autres *privacy policy*, *privacy statement*, *privacy*. Toutefois, il ne faut pas croire que ces différentes politiques exonèrent les sites Web de leurs obligations légales, elles ont pour objectif de formaliser les prétentions du site Web et de permettre aux internautes de découvrir l'existence d'un cadre juridique. En effet, le responsable du site Web fera le plus souvent mention de la législation à laquelle le site Web est assujetti eu égard à son lieu physique d'enregistrement.

42. Par conséquent, l'établissement de politiques de protection des données personnelles n'est pas incompatible avec l'existence de législation nationale, régionale ou provinciale et internationale en ce domaine. Elles permettent au contraire de mettre au grand jour ce type de réglementation tout en informant les internautes sur les engagements du site Web. Elles ont donc un rôle éducatif.

43. En effet, si nous regardons de plus près ces politiques nous constatons que la majorité d'entre elles reprennent implicitement les principes émis dans les instruments internationaux ou encore font directement référence à la législation nationale applicable. Ainsi, les politiques de protection des données personnelles devant être claires, compréhensibles et facilement accessibles sur le site Web mettent généralement l'accent sur les points suivants :

· l'engagement général du site Web en matière de vie privée et de protection des données personnelles ;

· les informations collectées ;

· l'utilisation faite des informations ;

· le partage éventuel des informations avec des tiers ;

· l'utilisation de fichiers journaux (*log file*)[31] et/ou de fichiers témoins (*cookies*)[32] et leur finalité ;

· l'existence d'un droit d'opposition et de retrait quant à l'utilisation des renseignements collectés et la manière de l'exercer ;

· l'existence d'un droit d'accès et la manière de l'exercer ;

· la sécurité du site Web ;

· les mentions légales, c'est-à-dire la législation à laquelle le site Web est assujetti.

44. En plus de ces précisions, les politiques de protection des données personnelles peuvent faire état des codes de bonne conduite et de déontologie auxquels le site Web adhère. Il n'est généralement pas fait de distinction entre ces deux types de normes mais il est possible de dire que les codes de bonne conduite sont le fait des internautes eux-mêmes[33], alors que les codes de déontologie sont principalement mis en place par des organismes à l'intention de leurs membres. À ce sujet, nous pouvons citer la charte mise en place par l'*Association des Fournisseurs d'Accès et de Services Internet* (AFA)[34] qui a pour mission 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 (abonnés ou utilisateurs occasionnels)* "[35]. Pour y parvenir, l'AFA a élaboré en octobre 1998 " *Les pratiques des membres de l'AFA en matière de données personnelles et droit d'auteur* "[36]. Ou encore le Code de déontologie des professionnels du marketing direct vis-à-vis de la protection des données à caractère personnel[37] adopté le 7 décembre 1993 par la *Fédération des Entreprises de Ventes À Distance* (FEVAD)[38] ou, pour finir, l'Association *Panoranet*[39] qui, par son initiative Votre Vie Privée (VVP), entend " *sensibiliser les acteurs et usagers d'Internet à la protection de la vie rivée et des données personnelles* "[40].

45. Parallèlement, pour gagner davantage la confiance des internautes, les sites Web ont recours à des sceaux de certification.

B. Les sceaux de certification

46. La présence d'un logo, d'une griffe, d'un sceau fournit aux internautes l'assurance que le responsable du site Web à soumis ses engagements à l'autorité d'un tiers en ce qui concerne le respect de certaines conditions comme par exemple la protection des données personnelles et la sécurité des transactions.

47. L'obtention d'un sceau se fait sur une base volontaire. Rien n'oblige le responsable du site Web à certifier ses pratiques en matière de protection des données personnelles.

Toutefois, le recours à un label favorise l'établissement du rapport de confiance nécessaire à l'échange de données personnelles. En effet, " *la labellisation est le résultat de la combinaison de la technologie et de l'audit. Elle poursuit essentiellement l'objectif de donner une meilleure visibilité à un site Web et aux pratiques que le site applique dans les relations avec ses clients. Elle représente un argument commercial visant à faire mieux vendre les produits et les services offerts par le site. De surcroît, la labellisation atteste la volonté du site de s'engager, vis-à-vis de ses clients, à respecter certains critères et à prendre en compte leurs intérêts* "[41].

48. Ainsi, lorsqu'un site Web veut obtenir un sceau de certification, il doit se soumettre à certaines règles. Par exemple, pour obtenir le sceau de *TRUSTe[42]* le responsable du site Web doit suivre trois étapes.

49. Tout d'abord, il doit soumettre ses engagements en matière de protection des données personnelles. Il peut soir déposer une politique existante, soit suivre le modèle établit par *TRUSTe*. Les règles mises en place doivent tenir compte d'un certain nombre de points, à savoir :

· quels sont les renseignements collectés sur le site Web ;

· pour qui les renseignements sont-ils collectés ;

· comment les renseignements sont-ils, et seront-ils, utilisées ;

· avec qui les renseignements seront-ils partagées ;

· le choix de l'internaute en ce qui concerne la collecte, l'usage et l'échange des ses renseignements ;

· quels sont les moyens envisagés pour garantir la sécurité des renseignements ;

· le droit pour l'internaute de consulter, corriger, radier les renseignements détenus par le site Web.

50. Si la politique répond aux exigences de *TRUSTe*, le responsable du site Web doit ensuite faire parvenir à l'organisme une copie signée par laquelle il accepte les conditions d'adhésion au programme, ainsi que sa cotisation annuelle. Une fois les formalités et vérifications accomplies, *TRUSTe* délivre au responsable du site Web une licence. Cette dernière certifie que le site Web est membre de *TRUSTe* comme le prouve le sceau qui devra être apposé sur ledit site. Concrètement, pour savoir si un site Web marchand est sous licence avec *TRUSTe*, il suffit de cliquer sur le sceau qui conduira à une page contenant des informations relatives au site Web.

51. La référence au certificateur *TRUSTe* peut surprendre dans le cadres de cet article visant à faire état de la vision française en matière de protection des données personnelles et ce d'autant plus que l'impartialité de cet organisme est remis en cause suite aux

affaires *RealNetwork*[43] et *Toysmart*[44]. Cependant, elle peut se comprendre car, d'une part, il s'agit d'un des premiers organismes à avoir mis l'accent sur la nécessité d'encadrer les pratiques des sites Web en ce qui concerne le traitement des données personnelles et, d'autre part, la navigation sur Internet ne se limitant pas aux seuls sites Web nationaux, l'internaute français est souvent mis en présence du label *TRUSTe*. Il nous apparaissait donc utile d'expliquer la procédure de certification de cet organisme mais cela ne doit pas faire oublier l'existence des labels comme *BBBOnLine Privacy*[45], *WebTrust*[46], *BetterWeb*[47] et autres *L@belsite*[48].

52. Ainsi, en recourant aux politiques de protection des données personnelles et aux sceaux de certification les sites Web entendent faire preuve de transparence à l'égard de leur clientèle. Cette attitude doit cependant s'accompagner de mesures de sécurité, tant au niveau des transmission que des bases de données, comme cela est prescrit dans les différents textes que nous avons envisagés dans la première partie de cet article. En effet, la confiance et la sécurité sont indispensables dans le cadre de la protection des données personnelles.

### C. Le recours à la technique

53. Outre son aspect international, Internet est également caractérisé par sa nature technique. Il est donc normal de prendre en considération les standards techniques comme outils de protection des données personnelles[49]. Cependant, pour éviter qu'Internet ne soit régit que par la technique et ne devienne un domaine de non-droit, une collaboration est nécessaire entre les informaticiens et les juristes[50]. On voit ici encore poindre l'idée de co-régulation.

54. Pour l'heure, les mesures de sécurité les plus fréquemment rencontrées et pouvant être utilisées par l'internaute français sont la cryptographie (1) mais aussi l'utilisation de standards comme celui mis en place par le *World Wide Web Consortium* (W3C)[51], à savoir le *Platform for Privacy Preference Project* (P3P) (2).

#### 1. La cryptographie

55. La cryptographie[52], ou chiffrement, peut se définir comme étant un ensemble de techniques qui permettent de protéger des informations grâce à un code secret. Il s'agit d'une méthode qui permet de chiffrer et, par la suite, de déchiffrer l'information transmise par le biais d'une clé soit privée soit publique, empêchant ainsi les personnes non autorisées à accéder au message.

56. Avec le système de la clé privée ou cryptographie symétrique, les deux intervenants utilisent la même clé pour chiffrer et déchiffrer les messages transmis entre eux. Cette méthode a ses propres limites. En effet, elle ne peut se concevoir qu'entre personne se connaissant et pouvant s'échanger en toute sécurité la clé unique par un autre moyen que par le Réseau afin d'éviter toute interception de ladite clé.

57. Selon le système de la clé publique ou cryptographie asymétrique[53], chaque intervenant possède sa propre paire de clés, publique et privée. Avec cette technique, l'expéditeur d'un message utilise sa clé privée, qui doit rester confidentielle, pour signer et chiffrer le contenu de son document. De son côté, le destinataire utilisera la clé publique de l'expéditeur. Cette clé peut être librement divulguée. Ainsi, le destinataire pourra décoder la signature et le contenu du message envoyé. Par conséquent, il est possible de dire qu'il existe une complémentarité entre les clés, à une clé privée correspond une clé publique permettant de chiffrer et de déchiffrer un message en toute sécurité. Dès lors, la cryptographie asymétrique garantit non seulement l'identité de la personne mais, également, l'intégrité du message.

58. Compte tenu de ces possibilités, la cryptographie a pendant longtemps été considérée comme une arme de guerre pouvant aller à l'encontre de la sécurité publique. La France a toutefois modifié sa position en 1999[54] en libéralisant l'utilisation et l'importation de logiciels de cryptographie destinés à des fins de confidentialité et d'usage privé des personnes physiques[55].

59. Cependant, même si la cryptographie apparaît comme étant le système le plus répandu pour garantir la transmission et la confidentialité des données circulant sur le Web, les internautes peuvent vouloir aller plus loin dans la protection de leur données personnelles en ayant recours à des logiciels d'anonymisation[56].

60. Or, le commerçant, que ce soit dans le monde physique ou sur Internet, a besoin d'obtenir des renseignements sur son cocontractant. Pour établir un bon de commande ou une réservation, il doit demander l'identité de l'acheteur. Il doit notamment prendre connaissance des coordonnées postale et/ou électronique pour pouvoir effectuer une livraison et obtenir le numéro de carte de crédit pour paiement. C'est pourquoi le recours à des logiciels d'anonymisation peut connaître ses propres limites dans le cadre du commerce électronique.

61. Outre le cryptage des données transmises lors d'une transaction, responsables de sites Web et internautes peuvent vouloir établir un dialogue préalable à toute connexion. Pour ce faire, ils pourront employer le *Platform for Privacy Preferences Project.*

**2. Platform for Privacy Preferences Project (P3P)**

62. Le standard P3P, développé par le *World Wide Web Consortium*, permet l'établissement d'un dialogue entre le site Web et les internautes relativement à la vie privée. En effet, comme nous avons déjà pu le mentionner, les internautes doivent avoir confiance dans les pratiques du site Web marchand pour communiquer leurs renseignements personnels.

63. À l'heure actuelle, pour connaître les prétentions des sites Web, les internautes doivent se référer aux énoncés contenus dans leurs politiques de protection des données personnelles. Le projet P3P vise à rendre les intentions du site Web accessibles dès que l'internaute saisi l'URL dudit site.

64. En effet, P3P permet aux responsables de sites Web de préciser leurs pratiques en matière de traitement des données personnelles. Ces spécifications seront formulées selon certaines caractéristiques et pourront être interprétées automatiquement par les navigateurs des internautes. Auparavant, les internautes auront pris soin d'indiquer à leur fureteur, compatible P3P, leurs préférences en matière de données personnelles.

65. Ainsi, si le site Web répond, en matière de collecte et d'utilisation des renseignements personnelles, aux attentes de l'internaute, ce dernier pourra y accéder. Dans le cas contraire, l'internaute serait informé des pratiques envisagées par le site Web. Il aura donc le choix entre négocier le traitement de ses données, naviguer sur le site Web en toute connaissance de cause ou, encore, mettre fin à sa session sur ce site en question.

66. L'efficacité de P3P repose sur l'établissement d'un dialogue entre le navigateur et le serveur. Ce dialogue sera basé sur l'une ou toutes les catégories de données susceptibles de faire l'objet d'un traitement, à savoir :

· des informations permettant une prise de contact physique, comme le numéro de téléphone ou l'adresse postale ;

· des informations permettant une prise de contact électronique, comme le courriel ;

· des informations relatives à un identifiant unique, comme le numéro de sécurité sociale, d'assurance maladie ;

· des informations relatives à un identifiant financier, comme le numéro de carte de crédit, le numéro de compte bancaire ;

· des informations informatiques, comme l'adresse IP, le nom de domaine, le système d'exploitation utilisé ;

· des informations relatives à la navigation sur Internet, c'est-à-dire les pages précédemment consultées et la durée de cette visite ;

· des informations relatives à l'activité en ligne, c'est-à-dire les achats, les recherches effectuées;

· des informations démographiques et socio-économiques, comme l'âge, le revenu ;

· des informations relatives aux préférences personnelles, comme les goûts musicaux ;

· des informations de communication, comme les expressions utilisées lors de vos échanges par courriel ou dans un groupe de discussion.

67. En utilisant P3P, les commerçants électroniques et les internautes pourront commercer sur la base d'un terrain d'entente en matière de traitement des données personnelles. Il est donc important que les sites Web marchands, mais aussi les internautes, prennent en

considération ce projet qui favorise une interaction entre les parties au contrat : le commerçant et l'internaute.

68. Ainsi, quelle que soit la protection retenue par les acteurs, c'est-à-dire qu'elle soit réglementaire, complémentaire ou co-régulatrice, ce qui importe le plus c'est que cette protection réponde aux besoins de confiance et de sécurité des internautes, avertis ou novices. En effet, il ne suffit pas d'énoncer ses obligations légales ou contractuelles, encore faut-il les respecter. Sans cette volonté, les actions visant à la protection des données personnelles resteront lettres mortes et les atteintes seront toujours de mises sur le Réseau, ce qui se traduirait par une baisse de confiance des internautes et donc des connexions.

**Notes**

* Doctorante à la Faculté de droit de l'Université de Montréal et à l'Université Panthéon-Assas, Assistante de recherche au Centre de recherche en droit public de l'Université de Montréal (Canada - Qc). Email : cynthia.chassigneux@UMontreal.CA.

[1] Le texte de la Directive 95/46/CE est disponible à l'adresse <http://europa.eu.int/eur-lex/fr/lif/dat/1995/fr_395L0046.html>.

[2] " La directive concernant la protection de données à caractère personnel entre en vigueur ", Commission européenne, Direction Générale du Marché Intérieur, Section " Protection des données ", 23 octobre 1998, <http://europa.eu.int/comm/internal_market/fr/media/dataprot/news/925.htm>.

[3] " La Commission décide d'adresser un avis motivé à neuf Etats membres ", Commission européenne, Direction Générale du Marché Intérieur, Section " Protection des données ", 29 juillet 1999, <http://europa.eu.int/comm/internal_market/fr/media/dataprot/news/99-592.htm> et " La Commission engage une action en justice contre cinq Etats membres " Commission européenne, Direction Générale du Marché Intérieur, Section " Protection des données ", 11 janvier 2000, <http://europa.eu.int/comm/internal_market/fr/media/dataprot/news/2k-10.htm>. Il s'agit de l'Allemagne, de la France, de la Hollande, du Luxembourg et des Pays-Bas.

[4] Journal Officiel du 19 juillet 1970.

[5] Il est possible de faire ici mention du projet *Safari* (Système automatisé pour les fichiers administratifs et le répertoire des individus) de 1974 visant à l'interconnexion des fichiers de l'administration grâce à un numéro d'identification unique. L'abandon de ce projet a conduit le gouvernement français à adopter la loi n° 78-17 du 6 janvier 1978 relative à

l'informatique, aux fichiers et aux libertés et à créer la Commission Nationale de l'Informatique et des Libertés.

[6] Journal Officiel du 25 janvier 1978.

[7] Christian Paul, *Du droit et des libertés sur l'Internet. La co-régulation, contribution française pour une régulation mondiale*, Rapport remis au Premier ministre, mai 2000, accessible en format .doc et .pdf à l'adresse <http://www.internet.gouv.fr/francais/textesref/pagsi2/lsi/rapportcpaul>.

[8] Pierre Trudel, France Abran, Karim Benyekhlef et Sophie Hein, *Droit du cyberespace*, Montréal, Thémis, 1997, p. 3-13.

[9] L'Allemagne a été le premier pays européen à protéger les informations personnelles contre les traitements automatisés de données. C'est ainsi qu'une loi fédérale a été adoptée en 1977 suivant l'exemple du Land de Hesse qui s'était doté d'une telle législation dès 1970. La Suède a suivi la même direction en 1973.

[10] Les dispositions relatives à cette autorité administrative indépendante sont contenues aux articles 6 et suivants de la loi de 1978.

[11] Les États membres de l'Union européenne sont l'Allemagne, l'Autriche, la Belgique, le Danemark, l'Espagne, la Finlande, la France, la Grèce, l'Irlande, l'Italie, le Luxembourg, les Pays-Bas, le Portugal, le Royaume-Uni et la Suède.

[12] Dans le cadre de cet article nous n'examinerons que la Directive 95/46/CE. Cependant il convient de préciser que d'autres directives, plus sectorielles, ont vocation à s'appliquer à la protection des données personnelles sur Internet, comme par exemple la Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications disponible à l'adresse <http://europa.eu.int/eur-lex/fr/lif/dat/1997/fr_397L0066.html> ou, encore, la Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique dans le marché intérieur disponible en format .pdf à l'adresse <http://europa.eu.int/comm/internal_market/fr/media/eleccomm/index.htm>.

[13] Article 25 § 1 Directive 95/46/CE " Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat ".

[14] Article 2a) Directive 95/46/CE " *[…] " données à caractère personnel " : toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputés 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* ".

[15] Nathalie Mallet-Poujol, " La réforme de la loi " Informatique et Libertés " ", *La protection des données personnelles, Revue française d'administration publique*, Institut International d'Administration Publique, janvier-mars 1999, n°89, p.49 ; M. Briat et Ch. M. Pitrat, " Urgent : Concepts à clarifier ", *Droit de l'Informatique et des Télécoms*, rubrique " Informatique et Libertés ", <http://www.dit.presse.fr>.

[16] Le principe émis à l'article 25 de la Directive 95/46/CE est également mentionné à l'article 24 de la loi de 1978 stipulant que " *[…] sur proposition ou après avis de la commission, la transmission entre le territoire français et l'étranger, sous quelque forme que ce soit, d'informations nominatives faisant l'objet de traitements automatisés régis par l'article 16 ci-dessus peut être soumise à autorisation préalable ou réglementée selon des modalités fixées par décret en Conseil d'État en vue d'assurer le respect des principes posés par la présente loi* ".

[17] Il est possible de suivre l'évolution des discussions entre l'Union européenne et les États-Unis entre autres sur les sites de la Direction Générales du Marché Intérieur, Section " Protection des données " aux rubriques " Nouvelles ", " Documents adoptés par le Groupe de Travail " à l'adresse <http://europa.eu.int/comm/internal_market/fr/media/dataprot/index.htm> ou *Droit et Nouvelles Technologies*, section " Actualités " et " Dossiers " à l'adresse <http://www.droit-technologie.org/> ou, encore,*Multimédium* <http://www.mmedium.com/> et *ZDNet France* <http://www.zdnet.fr/>. Voir également Yves Poullet, « Les Safe Habor Principles Une protection adéquate ? », *Juriscom.net*, Doctrine, 17 juin 2000, <http://www.juriscom.net/uni/doc/20000617.htm>.

[18] Pour plus de renseignements, il est possible de lire les articles suivants : AFP, " Bruxelles considère suffisante la protection américaine dans les transactions électroniques ", *Multimédium*, 27 juillet 2000, <http://www.mmedium.com/cgi-bin/nouvelles.cgi?Id=4011> ; Etienne Wery, " Safe Harbour Principles : décision finale de la Commission européenne ", *Droit et Nouvelles Technologies*, 1 août 2000, <http://www.droit-technologie.org/fr/1_2.asp?actu_id=-1143539713>.

[19] Pour plus de renseignements, il est possible de lire les articles suivants : Jérôme Thorel, " Vie privée : le Parlement européen prêt à torpiller le Safe Harbor ", *ZDNet France*, 10 juin 2000, <http://www.zdnet.fr/actu/soci/a0014633.html> ; Robert MacMillan, " EU Nixes Net Privacy Deal ", *E-commerce Times*, 5 juillet 2000, <http://www.ecommercetimes.com/news/articles2000/000705-nb1.shtml> ; AFP, " Le Parlement européen contre un accord bilatéral sur la protection des données personnelles en ligne " *Multimédium*, 6 juillet 2000, <http://www.mmedium.com/cgi-bin/nouvelles.cgi?Id=3920>; Jérôme Thorel, " Données personnelles : Strasbourg contre

Safe Harbor ", *ZDNet France*, 7 juillet 2000, <http://www.zdnet.fr/cgi-bin/a_actu.pl?File_ini=a_actu.zd&ID=15022&Rub=&Dat=200007072359>.

[20] Francis Pisani, " Vie privée : les dangers de l'accord États-Unis/Europe ", *Le Monde, Édition électronique*, 14 mars 2000.

[21] *Op. cit.*, note 7, p.17.

[22] <http://www.oecd.org/dsti/sti/it/secur/prod/priv-fr.html>.

[23] <http://www.coe.fr/fr/txtjur/108fr.htm>.

[24] Dans le cadre de cet article nous ne traiterons que de ces deux textes internationaux. Il convient toutefois de préciser que d'autres instruments internationaux peuvent s'appliquer sur le territoire français afin de protéger les données personnelles des internautes. On peut citer les accords de Schengen, les lignes directrices des Nations unies, les dispositions de l'Organisation mondiale du commerce et de l'Organisation internationale du travail. Pour une vue d'ensemble de ces textes, voir notamment Marie-Pierre Fenoll-Trousseau et Gérard Hass, *Internet et la protection des données personnelles*, Paris, Litec, 2000, p.38 et suivantes.

[25] Paragraphe 2 Lignes directrices de l'OCDE " *Les présentes Lignes directrices s'appliquent aux données de caractère personnel, dans les secteurs public et privé, qui, compte tenu de leur mode de traitement, de leur nature ou du contexte dans lequel elles sont utilisées, comportent un danger pour la vie privée et les libertés individuelles* ".

[26] Document accessible sur le site de l'OCDE en format .pdf à l'adresse <http://www.oecd.org/dsti/sti/it/secur>.

[27] La Convention 108 a été ratifiée par la France en 1983.

[28] Conseil d'État, *Internet et les réseaux numériques*, Paris, La Documentation française, 1998 ou à l'adresse suivante <http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm>.

[29] *Op. cit.*, note 7.

[30] *Op. cit.*, note 8, p. 3-34 ; Pierre Trudel, " Les effets juridiques de l'autoréglementation ", (1989) 19 *R.D.U.S.* 247.

[31] Pour une vision synthétique de ces fichiers, il est possible de se référer à l'ouvrage de M.-P. Fenoll-Trousseau et G. Hass, *op. cit.*, note 24, p.132 et suivantes. Les auteurs font référence à la définition donnée en la matière dans le rapport du Conseil d'État : " *ces données sont liées aux techniques utilisées sur internet pour établir la communication entre ordinateurs distants (le protocole TCP/IP) et à l'utilisation faite du réseau par l'individu ; elles concernent d'une part les adresses des machines du réseau, dites adresses IP, et en*

*particulier celles de l'émetteur d'un message et de son destinataire, adresses auxquelles sont associées la date et l'heure de la connexion, des informations techniques caractérisant le type d'usage (accès au Web, messagerie ...) d'autre part, la requête (page du site que l'utilisateur veut visiter...) ou le message proprement dit. Ces données sont collectées automatiquement par les fournisseurs d'accès et consignées dans un fichier dénommé fichier log. Ces éléments sont des outils d'identification et de traçabilité des individus extrêmement puissants qu'il convient d'analyser* ".

[32] Selon la CNIL, les fichiers témoins correspondent à " *[...] un enregistrement d'informations par le serveur dans un fichier-texte situé sur l'ordinateur client (le vôtre), informations que ce même serveur (et lui seul) peut aller relire et modifier ultérieurement* ". À ce titre, la CNIL a mis en place une démonstration dressant un profil de l'internaute lors de ses déplacements sur le site Web de la CNIL. Pour une vision synthétique de ces fichiers, voir M.-P. Fenoll-Trousseau et G. Hass, *idem*, p.135 et suivantes.

[33] À ce sujet, voir Etienne Wery, " Les associations de consommateurs se lancent dans la labellisation des sites ", *Droit et Nouvelles Technologies*, 21 février 2000, <http://www.droit-technologie.org/2_1.asp?actu_id=951142276&month=2&year=2000>.

[34] <http://www.afa-france.com>.

[35] AFA, " Pratiques et Usages ", janvier 1998, <http://www.afa-france.com/html/action/usages.htm>.

[36] AFA, " Les pratiques des membres de l'AFA en matière de données personnelles et droit d'auteur ", octobre 1998, <http://www.afa-france.com/html/action/droit_auteur.htm>.

[37] <http://www.fevad.com/generale/re.htm>.

[38] <http://www.fevad.com>.

[39] <http://www.panoranet.org/index.htm>.

[40] <http://www.panoranet.org/vvp>.

[41] Didier Gobert et Anne Salaün, " La labellisation des sites Web : classification, stratégies et recommandations ", *Droit et Nouvelles Technologies*, février 2000, <http://www.droit-technologie.org/5_12.asp>. Voir également Vincent Gautrais, " La certification de qualités des sites Internet : un sésame voué à la sécurité du consommateur ", (1999) 3 Ubiquité ; Didier Gobert et Anne Salaün, " La labellisation des sites Web : inventaire des initiatives existantes ", *Droit et Nouvelles Technologies*, février 2000, <http://www.droit-technologie.org/5_11.asp>.

[42] <http://www.truste.net>.

[43] En ce qui concerne l'affaire *RealNetworks*, on peut consulter entre autres les articles parus sur les sites suivants : *Multimédium* <http://www.mmedium.com> ; *E-commerce Times* <http://www.ecommercetimes.com> ; *ZDNet France*<http://www.zdnet.fr> ; *Libération* <http://www.liberation.com> et, également, le site de l'Association *JunkBuster* <http://www.junkbusters.com>.

[44] En ce qui concerne l'affaire *Toysmart*, voir, entre autres, les articles parus sur les sites suivants : *Multimédium* <http://www.mmedium.com> ; *E-commerce Times* <http://www.ecommercetimes.com>, *ZDNet France* <http://www.zdnet.fr>, *Libération* <http://www.liberation.com> ; *Droit et Nouvelles technologies* <http://www.droit-technologie.org> ; *New York Times* <http://www.nytimes.com>. Mais aussi le site du *Federal Trade Commission* <http://www.ftc.gov>.

[45] <http://www.bbbonline.org>.

[46] <http://www.webtrust.net>.

[47] <http://wwwpwcbetterweb/betterweb>.

[48] <http://www.labelsite.org>.

[49] " *les problèmes qu'elle a introduit, la technologie peut également contribuer à les réduire ou à les éliminer* ", *op. cit.*, note 8, p. 3-64.

[50] Pierre Kayser, *La protection de la vie privée par le droit. Protection du secret de la vie privée*, 3ème éd., Paris, Economica, 1995, p. 21.

[51] <http://www.w3.org>.

[52] *Op. cit.*, note 24, p. 78 et suivantes. Et, Serge Guinchard, Michèle Harichaux et Renaud de Tourdonnet, *Internet pour le droit*, Paris, Montchrétien, 1999, p. 165 et suivantes.

[53] Jean-Paul Delahaye, " La cryptographie RSA vingt ans après ", *Pour la science*, juin 1999, <http://www.pourlascience.com/numeros/pls-267/logique.htm>.

[54] La législation française en matière de cryptographie fait non seulement référence à la loi n°90-1170 du 29 décembre 1990, modifiée par la loi n°91-648 du 11 juillet 1991 et la loi n°96-659 du 26 juillet 1996, mais aussi au décret d'application n°99-199 du 17 mars 1999, J.O. 19 mars 1999.

[55] On peut lire à ce sujet les articles suivants : Comité interministériel pour la société de l'information (CISI), " Bâtir un cadre législatif protecteur des échanges et de la vie privée ", <http://www.internet.gouv.fr/francais/textesref/cisi190199/decis1.htm> ; Ronald Rivest, " Pour la libéralisation de la cryptographie ", *Pour la science*, juin 1999, <http://www.pourlascience.com/numeros/pls-260/art-4.htm> ; Rémy Fière, Laurent

Mauriac et Florent Latrive, " Le plan du gouvernement français pour faire place au Net ", *Libération*, rubrique Multimédia, 20 janvier 2000, <http://www.liberation.com/multi/actu/semaine990118/art990120a.html> ; Jérôme Thorel, " Le nouveau PGP enfin disponible en français ", *ZDNet France*, 18 janvier 2000, <http://www.zdnet.fr/actu/tech/a0012601.html> ; Christian Aubry, " Vive la cryptologie française libre ! ", *Multimédium*, 20 janvier 1999, <http://www.multimedium.com/cgi-bin/nouvelles.cgi?Id=2156>.

[56] À ce titre, il est possible de citer les exemples de *Freedom* de la société montréalaise *Zeroknowledge* <http://www.zeroknowledge.com> et de *FlowProtector* de la société française *CheckFlow* <http://www.checkflow.net/corp>.


**ISSN 1480-1787**