La protection des données dans le cyberespace

Jean-Philippe Walter

Dr en droit, Préposé fédéral suppléant à la protection des données, Berne

Zusammenfassung:
Die geltenden nationalen Gesetzgebungen sowie die internationalen Richtlinien beantworten lediglich einen Teil der Fragen, die sich im Internet stellen. Auch wenn die Grundprinzipien des Datenschutzrechts ohne weiteres auch im Cyberspace Anwendung finden, sind neue Strategien zu entwickeln, um dem Recht mit datenschutzfreundlichen Technologien zum Durchbruch zu verhelfen. In einem Bereich, der Freiheit für alle bringt, ist es zur Vermeidung des Chaos notwendig, dass jeder gewisse Regeln beachtet.

I. Le village planétaire et les risques d'atteinte à la vie privée

La fin du 20e siècle est marquée par ce que d'aucuns qualifient de révolution informationnelle[1] et que nous décrirons plutôt comme une évolution irréversible due au couplage des techniques de l'informatique et des télécommunications débouchant sur le multimédia et le développement fulgurant de l'internet, prémisse à l'apparition de gigantesques inforoutes. Cette évolution contribue à la globalisation et à la virtualisation de la société. Elle engendre des espoirs, notamment du fait de la liberté qu'offre l'espace cybernétique. Elle suscite également des craintes d'anéantissement de la vie privée et d'émergence de l'homme transparent[2].

Sur l'internet, circulent d'innombrables données personnelles concernant non seulement les utilisateurs, mais aussi d'autres personnes au sujet desquelles des données sont traitées et communiquées. L'utilisation de l'internet engendre des données personnelles qui seront collectées, enregistrées et exploitées à différentes fins. Aujourd'hui, chaque utilisation d'internet laisse une trace et permet aisément aux intermédiaires, de bonne ou de mauvaise foi, d'utiliser ces informations. Le fournisseur de service peut déterminer qui utilise le réseau, à quel moment, quelles informations ont été appelées, ou avec qui des informations ont été échangées et sur cette base, peut dresser des profils d'utilisateurs.

L'internet ne crée pas de nouveaux risques d'atteinte à la personnalité ou aux droits fondamentaux des personnes concernées: il n'est pas nécessaire de recourir à l'internet pour intercepter un numéro de carte de crédit, cela peut se faire lors de l'utilisation courante dans un magasin ou un restaurant ou lors de la transmission par téléphone ou fax. L'internet cependant amplifie[3] les risques déjà identifiés du fait de mesures de sécurité encore insuffisantes, du fait du nombre d'utilisateurs et de par le caractère universel du réseau. Le risque augmente en fonction du volume de données enregistrées et du nombre de personnes qui peuvent avoir un accès aux données.

Il faut garder à l'esprit qu'aujourd'hui tous nos actes informatiques ou cybernétiques si anodins soient-ils, laissent des traces quasi indélébiles dans les réseaux télématiques. Ces traces sont une source d'informations précieuses pour une foule d'acteurs de notre société: autorités publiques, médias, banques, assurances, commerçants, voyagistes, spécialistes en marketing, sectes, etc. L'individu doit être conscient que lorsqu'il traite des données par le biais de l'internet, notamment en les communiquant à des tiers ou en les rendants accessibles, il court le risque que ces données soient accessibles à un grand nombre, qu'elles puissent être connectées à d'autres données ou fichiers et qu'il ne soit plus possible de savoir qui utilise ces données. Ces utilisateurs peuvent consulter ces données, les télédécharger, les traiter à d'autres fins ou les conserver. Il doit également être conscient que la connection de différents traitements de données personnelles, qui pris isolément,

1 Voir notamment De Rosnay J., La révolution informationnelle, dans internet, l'extase et l'effroi, Le Monde Diplomatique, Manière de voir, Hors série 1996.

2 Voir aussi Von Hinden M., Persönlichkeitsverletzungen im internet, Das anwendbare Recht, Tübingen 1999.

3 United States searches for a privacy policy to include internet and EU Directive, dans Privacy Laws & Business, 12/1996, p. 15

n'étaient pas problématiques, le deviennent notamment par la constitution de profils de la personnalité, de consommation ou de déplacement. Il devient en outre difficile d'obtenir la destruction des informations une fois sur le net.

Ainsi, tout individu qui surfe sur internet pour consulter des banques de données, rechercher de l'information, effectuer des transactions commerciales ou dialoguer avec d'autres utilisateurs ou qui envoie des messages par le biais du courrier électronique, dépose des «pierres blanches» qui balisent sa route et permettent à des tiers de reconstituer son profil, de connaître ses habitudes de consommation, son mode de vie et ses goûts, de suivre ses déplacements, de calculer sa vitesse sur l'autoroute, de vérifier ses alibis, etc.[4].

Quelques exemples illustrent les risques inhérents à l'utilisation d'internet:

- Publication sur internet des profils de la personnalité des chômeurs en recherche d'emploi[5];
- Caméras opérant en direct sur le World Wide Web, rendant les images filmées accessibles dans le monde entier et permettant d'identifier les personnes passant dans le champ de la caméra, sans qu'elles en soient informées et qu'elles puissent s'y soustraire[6];
- Enregistrement des activités des utilisateurs accédant à internet[7];
- Publication des photos du personnel sans le consentement des personnes concernées[8].
- Divulgation de manière diffamatoire sur un site web qu'une jeune fille de 13 ans est une prostituée, tout en donnant les coordonnées précises de cette personne[9].
- Publication sur le site d'une entreprise de données personnelles comprenant le numéro de cartes de crédit, mot de passe, rendez-vous médicaux, adresse, nom et prénom, etc.
- Mise à disposition d'une banque de données de démonstration à des fins de renseignements de crédit comportant la majorité de la population suisse, y compris des enfants de moins de 10 ans et comprenant des doublons, des données fausses ou dépassées.
- Publication sur internet des coordonnées (y. c. photo) de personnes qui visiblement ne s'étaient pas acquittées de certaines factures.
- L'agence de marketing online «DoubleClick» gère une banque de données qui contient quelques 2 millions de profils de clients établis à partir des achats électroniques[10].

II. La législation sur la protection des données

Le traitement de données personnelles sur l'internet ne repose pas sur un vide juridique[11]. Il est en particulier soumis aux dispositions nationales et internationales régissant la protection des données personnelles. Toutefois ces règles se heurtent aux limites territoriales (souveraineté nationale). Il n'existe pas encore un accord global et universel régissant la protection des données dans le cyberespace. De ce fait, internet permet plus facilement de détourner les contraintes nationales et en se basant sur son assise universelle de publier des données qui ne pourraient pas l'être dans l'Etat d'où elles proviennent[12].

Pour ce qui est des acteurs agissant en Suisse, ils sont soumis à la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[13], ainsi qu'aux dispositions sectorielles et notamment celles touchant au secret et à la confidentialité. En outre, les communications (par exemple par la

Résumé: *Les législations nationales et les réglementations internationales en vigueur n'offrent qu'une réponse partielle aux problèmes d'un monde virtuel. Si les principes fondamentaux du droit de la protection des données sont sans autre applicables au cyberespace, il convient de développer de nouveaux schémas alliant droit et technologie de la vie privée. Un espace de liberté pour tous implique que chacun s'engage à respecter certaines règles pour éviter le chaos.*

4 Voir RAMONET I., Citoyens sous surveillance, dans le Monde Diplomatique, Manière de voir n° 27, août 1995.
5 Voir PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES, 5e Rapport d'activités, 1997/98, p. 173s (Rapport d'activités).
6 Voir 5e Rapport d'activités, p. 169s.
7 Voir 4e Rapport d'activités, 1996/97, p. 165s et 6e Rapport d'activités, 1998/99, p. 254.
8 Voir 6e Rapport d'activités, p. 247.
9 Le Matin du 5 avril 2000.
10 «Der gläserne Konsument nimmt Formen an», dans Heise Online, Meldung vom 26.02.2000, (http://www.heise.de/newsticker/data/hob-26.01.00-000/).
11 Voir OFFICE FÉDÉRAL DE LA JUSTICE, internet, Le Nouveau Média interroge le Droit, Berne 1996
12 Voir par exemple la polémique autour de la publication du livre de Claude Gubler, «le Grand Secret» relatant la maladie du président François Mitterand; voir aussi VON HINDEN M., op. cit., p. 1ss.
13 RS 235.1

voie du courrier électronique) sont également protégées par le secret des télécommunications et de la correspondance[14].

1. But de la protection des données

Dès le moment où des données relatives à des personnes (physiques ou morales) sont collectées, traitées et diffusées par le biais de l'internet, le droit de la protection des données s'applique. Le but du droit de la protection des données est de protéger la personnalité des personnes physiques ou morales et de garantir le respect des droits et libertés fondamentaux, notamment le droit à la vie privée[15], lors du traitement de données personnelles par des personnes privées ou des organes étatiques. Toute personne doit ainsi pouvoir exercer une certaine maîtrise sur l'information qui la concerne et restreindre le traitement de données personnelles par des tiers.

Pour atteindre cet objectif, la loi définit un certain nombre de règles matérielles régissant le traitement des données personnelles, détermine les obligations liant le responsable du traitement, énonce les droits des personnes concernées et met en place un système de surveillance (en particulier institution d'un préposé fédéral à la protection des données).

2. Règles matérielles de protection des données

Tout traitement de données personnelles doit intervenir dans le respect des règles matérielles de la LPD, à savoir les principes généraux du traitement et les règles matérielles proprement dites. Ces règles présupposent une constante mise en balance des intérêts de celui qui veut traiter des données avec le droit des personnes à la maîtrise des informations qui les concernent.

A. Principes généraux de traitement de données personnelles

Les articles 4 à 7 LPD énoncent ainsi sept principes fondamentaux de la protection des données.[16] Ces principes sont des normes de comportement et constituent en quelque sorte le noyau dur de la loi.

La **collecte de données doit être licite:** Ce principe énoncé à l'article 4, 1er alinéa LPD, exprime le principe général de loyauté non seulement quant au droit de collecter des données, mais également quant au mode de collecte. Il s'agit d'éviter que dès le début, le traitement de données ne soit entaché d'irrégularité. Ainsi, toute collecte effectuée par tromperie, menace ou de manière dissimulée est illicite.

Le deuxième principe énoncé à l'article 4, 2e alinéa LPD prévoit que le **traitement des données doit être conforme au principe de la bonne foi.** Ce principe définit l'attitude loyale que l'on est en droit d'attendre de toute personne ou organe intervenant dans la vie sociale. Avec le principe de licéité, il constitue un élément de la **transparence** et de la **prévisibilité** du traitement de données personnelles permettant aux personnes concernées d'adapter leur comportement. Il en découle en particulier qu'en règle générale la collecte de données doit avoir lieu auprès de la personne concernée ou du moins au su de celle-ci, et qu'elle ne doit en principe pas intervenir contre sa volonté. La transparence du traitement implique en particulier que la personne concernée soit informée des traitements soit directement, soit indirectement notamment par le biais du registre des fichiers publié par le préposé fédéral à la protection des données. Il serait ainsi souhaitable qu'à l'instar du droit européen[17], la personne concernée soit, au moment du premier traitement (collecte ou communication), informée de l'identité du responsable du traitement, des finalités du traitement, des catégories de données traitées, des destinataires des données et du caractère obligatoire ou fa-

14 Voir arrêt du Tribunal fédéral du 5 avril 2000 non encore publié (1A.104/1999).

15 Voir arrêt de la Cour européenne des droits de l'homme du 16 février 2000, dans la cause Ammann contre Suisse (http://www.dhdirhr.coe.fr/), aux termes duquel la notion de «vie privée» ne doit pas être interprétée de façon restrictive: «En particulier, le respect de la vie privée englobe le droit pour l'individu de nouer et de développer des relations avec ses semblables; de surcroît aucune raison ne permet d'exclure les activités professionnelles ou commerciales de la notion de 'vie privée'».

16 Voir Maurer U., dans Maurer/Vogt, Kommentar zum schweizerischen Datenschutzgesetz (1995), ad. art. 4 et ss.; Walter J.-Ph, Le droit public matériel, dans Gillard N. (édit.), La nouvelle loi fédérale sur la protection des données, Lausanne 1994, p. 41; Page G., Autoroutes de l'information et protection des données, dans Hilty R. M., Information Highway, Berne, 1996, p. 364ss.

cultatif de la collecte[18]. En outre, lorsque le traitement intervient dans un environnement peu sûr, il convient également d'informer la personne sur les risques inhérents au système[19].

Le troisième principe est celui de la **proportionnalité** (art. 4, 2e al. LPD) selon lequel le traitement de données personnelles doit être propre et nécessaire à atteindre le but pour lequel des données doivent être traitées tout en veillant à préserver les droits des personnes concernées. Le traitement de données personnelles suppose qu'il existe un rapport raisonnable entre le résultat recherché et le moyen utilisé. Ce principe touche au mode de traitement, ainsi qu'à l'étendue et aux catégories de données personnelles utilisées. Seules les données vraiment nécessaires doivent être collectées. Ainsi, dans le cadre de transactions commerciales par l'intermédiaire des nouvelles technologies (internet, carte à puce), chaque acteur ne devrait traiter que les données personnelles dont il a besoin pour l'opération qu'il est habilité à effectuer[20]. Il n'est par exemple pas nécessaire de collecter des données lorsque l'accès au service est gratuit, notamment la consultation d'un journal ou d'un site informatif, qui n'implique pas de dialogue avec l'utilisateur.

Le quatrième principe est celui de la **finalité**. Il est énoncé à l'article 4, 3e alinéa de la LPD: «Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances.» Ce principe comporte deux volets: l'obligation de déterminer une finalité préalable au traitement, et l'obligation d'utiliser les données uniquement en fonction de cette finalité ou du moins pour une finalité compatible avec la finalité initiale. Egalement élément de la transparence, il permet aux personnes concernées de savoir à quelles fins les données sont collectées et traitées. Ainsi, une collecte illimitée de données pour des finalités ou des applications indéterminées (collecte «en prévision de») ou la création de banques de données à multiusages non définis transgresse le principe de finalité et est illicite.

Le cinquième principe est celui de **l'exactitude des données** énoncée à l'article 5. Celui qui traite des données doit s'assurer que celles-ci sont correctes. Le non respect de ce principe peut avoir des conséquences graves pour la personne concernée, suivant le contexte et la finalité pour laquelle les données sont traitées. Ce principe n'est cependant pas absolu et doit être pondéré en fonction de la finalité et des circonstances concrètes du traitement de données personnelles.

Le sixième principe a trait à la **communication de données à l'étranger** (art. 6, 1er al. LPD). La communication n'est possible que dans la mesure où elle n'entraîne pas une menace grave pour la personnalité des personnes concernées, notamment du fait que le destinataire des données n'est pas soumis à une protection des données équivalente à celle qui est garantie en Suisse. Ainsi, on devrait s'abstenir de communiquer des données personnelles vers des Etats qui n'ont pas de loi sur la protection des données, sauf si l'équivalence peut être garantie par d'autres dispositions légales, statutaires ou contractuelles. Cette disposition n'est pas adaptée à la dimension de l'internet et elle risque rapidement de devenir lettre morte, si elle n'est pas accompagnée d'autres mesures permettant de respecter les droits des personnes concernées.

Le septième principe est celui de la **sécurité des données** selon lequel «les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures techniques et organisationnelles appropriées» (art. 7 LPD). La nécessité d'assurer la sécurité des données et des systèmes de traitement de l'information, notamment pour garantir leur confidentialité, leur disponibilité et leur intégrité est indispensable pour rendre effectives les

17 Voir les articles 10 et 11 de la Directive 95/46/CE 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, Journal officiel des Communautés européennes du 23 novembre 1995, p. 31.

18 Voir aussi Recommandation du Conseil de l'Europe N° R (99) 5 sur la protection de la vie privée sur internet, du 23 février 1999 (http://www.coe.fr/dataprotection/fdocs.htm).

19 Voir le principe 7.20 de la Recommandation du Conseil de l'Europe n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, du 7 février 1995, qui prévoit un tel devoir d'information dans le domaine de la téléphonie mobile.

autres exigences de la protection des données et éviter notamment que des personnes non autorisées aient accès aux informations, que les données soient diffusées de manière illicite ou utilisées pour des finalités non autorisées. Cela implique notamment que les systèmes soient conçus pour effectuer uniquement les traitements nécessaires à l'accomplissement des tâches pour lesquelles les données ont été collectées. Les mesures à prendre doivent être différenciées en fonction des finalités du traitement, de la nature des données traitées, de l'étendue du traitement et du risque encouru par les personnes concernées. On tiendra également compte du développement de la technique. Les mesures prises devront faire l'objet d'une réévaluation régulière. Ces mesures touchent notamment le personnel, le matériel, l'accès aux locaux, le logiciel et l'organisation de l'entreprise[21]. Ainsi, l'utilisation commerciale de l'internet n'est pas envisageable sans la présence de mécanismes de sécurité très poussés, notamment de cryptage des données, d'authentification des utilisateurs et des messages, ou de protection des banques de données.

B. Traitement de données personnelles par des personnes privées

Dans le secteur privé, le traitement des données personnelles n'est possible que si le traitement ne porte pas une atteinte illicite à la personnalité des personnes concernées[22]. Aux termes de l'article 13, 1er alinéa LPD, une atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la personne concernée, un intérêt prépondérant privé ou public, ou par la loi. Trois conditions pour que la violation de la loi soit consommée:

- Un **droit de la personnalité** est en cause. Généralement le traitement de données personnelles met en jeu la personnalité des personnes concernées.
- Ce droit de la personnalité est **atteint**. Si nous admettons que tout traitement de données personnelles touche la personnalité des personnes concernées, il n'en résulte pas automatiquement et en tous les cas une atteinte. Cela dépendra en particulier de la nature des données traitées, des finalités et des circonstances du traitement, du domaine d'activité ou de l'organisation du système d'information. Ainsi la loi précise qu'en règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement (art. 12, 3e al. LPD). Dans un tel cas, il faut que ce soit la personne concernée elle-même qui rende ses données accessibles, soit en les diffusant, soit en consentant à leur diffusion par des tiers. Ainsi, tel n'est pas le cas lors de la publication d'un annuaire, téléphonique ou autre, effectuée sans que la personne y ait consenti ou ait le droit de s'y opposer. Face à la diffusion de données au travers des inforoutes, une certaine prudence est de mise. Ainsi, on ne peut déduire du fait qu'une personne rende accessible des données la concernant, qu'elle accepte sans autre leur rediffusion sur des réseaux électroniques. Dans ce cas, un consentement explicite et informé est nécessaire[23].
- Enfin, **l'atteinte est illicite**. En principe toute atteinte est illicite, sauf si elle est justifiée par le consentement de la personne concernée, par la loi ou par un intérêt public ou privé prépondérant.

La LPD définit, à titre exemplatif, trois cas dans lesquels le traitement de données personnelles porte une atteinte illicite à la personnalité des personnes concernées (art. 12, 2e al. LPD):

- Il s'agit de traitements de données personnelles qui **interviennent en violation de l'un des principes fondamentaux** définis aux articles 4 et suivants de la loi, et que nous avons examiné auparavant;
- Il y a également atteinte illicite lorsque le traitement s'effectue **contre la volon-**

20 Voir les principes 3.3 à 3.7 de la recommandation du Conseil de l'Europe n° R (90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes, du 13 septembre 1990.

21 Voir également les articles 8 à 12 de l'ordonnance du Conseil fédéral du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD, RS 235.11).

22 Voir Steinauer P.H., Le droit privé matériel, dans Gillard N. (édit.), La nouvelle loi fédérale sur la protection des données, Lausanne 1994, p. 85, Die Verletzung durch private Datenbearbeitung und die allfällige Rechtfertigung einer Verletzung: Einzelheiten der gesetzlichen Regelung, dans Schweizer R.J. (Hrsg), Das neue Datenschutzgesetz des Bundes, Zurich 1993, p. 43; Hünig, M. dans Maurer/Vogt, Kommentar zum schweizerischen Datenschutzgesetz, ad art. 12 et 13.

23 Du même avis, Page G., op. cit., p. 367.

té expresse de la personne concernée;
- Il s'agit enfin de la **communication** à des tiers de **données sensibles** ou de **profils de la personnalité**.

Dans ces trois cas, l'**illicéité** de l'atteinte peut être levée si le responsable du traitement parvient à démontrer qu'il est au bénéfice d'un motif justifiant le traitement des données.

La loi énonce trois motifs généraux justifiant une atteinte à la personnalité (art. 13, 1er al. LPD): le **consentement de la personne concernée**, qui peut être exprès ou tacite, mais qui doit être libre, spécifique, éclairé et révocable, la **loi** ou **l'intérêt public ou privé prépondérant**. Selon la jurisprudence du Tribunal fédéral[24], seul un intérêt particulièrement important à traiter les données peut l'emporter sur le droit à la vie privée exempte de troubles. Il s'agit en fait de procéder à une pesée des intérêts en présence et d'apprécier de cas en cas si l'intérêt au traitement l'emporte sur l'intérêt de la personne concernée à conserver la maîtrise sur ses données, et donc sur sa vie privée. La loi énonce également à titre exemplatif, six situations où, en principe, un intérêt prépondérant de celui qui traite des données entre en considération (art. 13, 2e al. LPD). Cela doit notamment permettre au juge de pondérer les intérêts en présence en cas de conflit.

III. Garantir la protection des données dans le cyberespace?

La loi fédérale sur la protection des données offre ainsi certaines garanties aux personnes concernées afin que leur personnalité ne soit pas illicitement violée lors du traitement de données à caractère personnel. Toutefois, l'application de ces dispositions est limitée aux territoires nationaux, et avec la globalisation des échanges d'informations, notamment via l'internet, il devient difficile de contrôler ou d'empêcher des activités indésirables. Pour les différents acteurs d'internet se pose en particulier un véritable casse-tête: ils sont confrontés à une multiplicité de règles existantes qui ont vocation à s'appliquer concurremment. Souvent l'utilisateur ne sait pas dans quel pays les données qu'il consulte ou qu'il transmet sont enregistrées et traitées. Il y a donc un risque accru que des données aboutissent chez des personnes qui ne sont pas soumises aux mêmes exigences de protection des données qu'en Suisse. Il est dès lors nécessaire de trouver un dénominateur commun et de dégager des règles communes aux internautes. Une coordination et une collaboration internationale sont indispensables. En attendant une législation internationale sur l'internet, définissant notamment des standards minimaux élevés et des procédures de contrôle et d'entraide internationale, il est souhaitable que les différents acteurs participant au processus de communication internet se dotent d'une autoréglementation (code de bonne conduite) les engageant à respecter des normes minimales de protection des données équivalentes aux dispositions des lois européennes, notamment de la Convention du Conseil de l'Europe[25] et de la Directive européenne sur la protection des données[26]. Un premier pas a été réalisé avec la Recommandation du Conseil de l'Europe R (99) 5 sur la protection de la vie privée sur internet[27] qui contient des lignes directrices à l'adresse des utilisateurs des inforoutes et aux fournisseurs de services et avec le Générateur de l'OCDE «de politique de protection de la vie privée»[28] qui tend à promouvoir des mesures de protection de la vie privée et leur affichage sur les sites.

Il convient également d'encourager d'autres solutions qui passent par l'autoréglementation[29], et la définition de politiques de la vie privée à afficher sur les sites. Les sites qui respecteraient ainsi les principes fondamentaux de la protection des données issus de la Convention 108, de la Directive européenne et des législations nationales (telle la loi fédérale) pourraient faire l'objet d'une certification par un organisme neutre et indépendant.

24 Voir en particulier, ATF 97 II 97
25 Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, FF 1997 I 701.
26 Directive 95/46/CE 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, Journal officiel des Communautés européennes du 23 novembre 1995, p. 31.
27 http://www.coe.fr/dataprotection/fdocs.htm
28 http://www.oecd.org/dsti/sti/it/secur/prod/generator-f.pdf
29 Comme cela est prévu à l'article 27 de la Directive européenne 95/46/CE.

L'utilisateur et les différents prestataires de service (fournisseur de services, fournisseur de contenu, fournisseur de serveurs, fournisseur d'accès ou transporteur) peuvent aussi contribuer à améliorer la protection des données, notamment en s'inspirant des recommandations[30] suivantes:

1. Information des utilisateurs

Tout prestataire de services informe de façon non équivoque chaque utilisateur des risques concernant le respect des droits et libertés fondamentales et notamment la vie privée. En particulier, il faut attirer l'attention sur:

- les lacunes de sécurité du réseau qui peuvent engendrer des risques pour le respect de la protection des données et de la vie privée, et notamment pour l'authenticité, l'intégrité et la confidentialité des messages;
- le caractère universel du réseau et le fait que l'information peut transiter ou être appréhendée dans des Etats qui ne sont pas soumis à des dispositions équivalentes de protection des données;
- les réseaux sur lesquels les informations seront disponibles;
- la finalité du traitement;
- les catégories de données enregistrées;
- la possibilité de s'opposer au traitement, de corriger les données ou de révoquer un consentement;
- la possibilité de surfer de manière anonyme ou en utilisant un pseudonyme;
- les mesures qui peuvent être prises pour assurer la confidentialité, l'intégrité et l'authenticité des messages.

Cette information pourrait se faire par le biais d'un message à l'écran avant que les données ne soient communiquées. Ce qui permettrait à l'utilisateur d'intervenir et d'empêcher la communication. Lorsque des données personnelles sont publiées, notamment l'adresse des collaborateurs/trices ou des membres d'une entreprise, d'une association ou de tout autre entité, le consentement libre, explicite et informé des personnes concernées devrait être préalablement requis.

2. Mesures techniques

Il convient de développer des moyens techniques pour améliorer la protection des données des utilisateurs qui utilisent le Net ou des personnes dont les données sont transmises sur le Net. L'utilisateur doit pouvoir contrôler l'utilisation des données qui le concernent et en obtenir la communication en retour. Il doit également pouvoir accéder à l'internet sans avoir à révéler son identité lorsque les données personnelles ne sont pas nécessaires à la prestation d'un service (droit de toute personne à utiliser l'inforoute sans être observée ni identifiée). Il est ainsi possible de développer des procédures et des techniques garantissant le respect de l'anonymat[31] par exemple en recourant à l'utilisation de protecteurs d'identité, de pseudonymes ou de cartes à prépaiement. Les exceptions au principe de l'anonymat et la levée de ce dernier doivent être précisément définies et limitées à ce qui est strictement nécessaire à la sauvegarde d'intérêts supérieurs (poursuite des abus et des fraudes, lutte contre la criminalité). Ces mesures doivent également permettre d'effectuer la collecte et le traitement de données personnelles de manière différenciée en fonction des tâches variées incombant aux différents partenaires ou intervenants dans la transaction. Par exemple, lors d'un achat, le vendeur n'a pas nécessairement besoin de connaître l'identité de la banque et/ou de l'acheteur; la banque n'a pas besoin de connaître l'identité du vendeur et le type d'achat effectué. Ce qui est important c'est que l'acheteur puisse acheter, que le vendeur soit payé et que la banque soit légitimée à débiter le compte de l'acheteur. En outre, les données personnelles, lorsqu'elles sont collectées, ne doivent pas être conservées au-delà de ce qui est nécessaire.

A. Cryptage des données

Des moyens techniques doivent aussi être mis en oeuvre pour protéger la confidentialité, l'intégrité et l'authenticité des messages et des données véhiculés. Il con-

30 Voir internet, Le nouveau média interroge le droit, op. cit.; Rapport et lignes directrices du Groupe de travail international sur la protection des données dans les télécommunications, La protection des données et le secret sur internet, Budapest/Berlin 1996; Recommandation du Conseil de l'Europe N° R (99) 5, op. cit.

31 Voir par exemple Petersen H., Anonymes elektronisches Geld, dans DuD 21 (1997) 7, p 403ss.

vient notamment de favoriser le recours à des méthodes sûres de cryptage, en particulier lors de la transmission de données sensibles ou de profils de la personnalité. La commercialisation de l'internet et le développement des transactions commerciales ou bancaires sur le Net nécessitent également un environnement sûr basé sur le cryptage des données. Ces mesures doivent être constamment réévaluées et perfectionnées pour faire face aux risques de déchiffrement. L'utilisateur doit pouvoir également lui-même chiffrer les messages ou les données qu'il transmet.

B. Protecteur d'identité[32]

Toute personne doit pouvoir préserver son identité et décider à qui elle souhaite la communiquer. Il n'est en effet pas nécessaire que toute relation se fasse en connaissant l'identité de son partenaire. Il est, par exemple, inutile de connaître l'identité de l'acheteur d'un journal dans la mesure où il s'acquitte correctement du prix. Et pourtant la société d'information, telle que nous la connaissons, tend vers une limitation du droit à l'anonymat. Chaque communication identifiée ne se limite pas à la simple connaissance de l'identité de la personne, mais comporte d'autres informations la concernant, notamment sur ses qualités et ses comportements, ce qui permet de dresser des profils de la personnalité.

Les technologies de l'information et de la communication permettent aujourd'hui d'augmenter l'efficience, d'améliorer la qualité, de développer de nouveaux produits et services, d'améliorer la sécurité ou encore de lutter contre des activités répréhensibles, tant dans l'accomplissement des tâches publiques/étatiques que dans les activités privées et commerciales. Toutefois, la technique nous offre aujourd'hui également la possibilité, sans remettre en cause les fonctions et les possibilités des systèmes d'information, de préserver l'identité des personnes et leur sphère privée.

La première possibilité, qui n'évite pas le problème de l'identité, et qui dépend de la manière dont les mesures techniques et organisationnelles sont respectées, consiste à protéger les données contre des accès non autorisés par des mesures de sécurité. Dans ce cas, les données personnelles sont déjà enregistrées.

La seconde approche consiste à utiliser une technologie garante de la protection des données (Privacy enhancing technology, PET: système de mesures techniques permettant de protéger la sphère privée de l'utilisateur; recours à un protecteur d'identité). Cette technologie permet d'éviter que des données personnelles soient collectées et traitées, ou du moins limite au minimum l'utilisation et l'enregistrement des données d'identification.

Les systèmes d'information sont nécessaires pour la réalisation d'activités déterminées. Certains de ces systèmes d'information ne nécessitent pas la connaissance de l'identité de la personne, sauf en cas d'activités pénalement répréhensibles. L'identité doit certes être connue au moment de l'octroi d'un accès (par exemple, lors de l'ouverture d'un compte bancaire) ou pour certaines autorisations (en amont du système d'information). Par contre pour les procédures d'identification, d'authentification, de contrôle d'accès et d'examen qui se déroulent à l'intérieur du système d'information, la connaissance de l'identité n'est pas nécessaire. Le recours à un pseudonyme ou protecteur d'identité suffit.

Le protecteur d'identité est un élément du système qui gère l'échange d'identité entre les autres éléments du système interactif. Il protège l'utilisateur et assure le contrôle lors de la diffusion de son identité qui ne figure plus dans le système. Il peut ainsi transformer l'identité réelle de l'utilisateur en un ou plusieurs pseudonymes que celui-ci utilisera pour accéder aux systèmes d'informations: le protecteur d'identité peut être délivré par une fonction spécifique du système d'information, par un système d'information particulier sous le contrôle de l'utilisateur (carte à puce, par exemple) ou par un système d'information sous contrôle d'un tiers

32 Voir à ce sujet, Registratiekamer et Information Privacy Commissioner/Ontario, Privacy-Enhancing Technologies, 1995; Borking J., Der Identity-Protector, dans Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern (Hrsg.) Technik und Datenschutz, 1997, p. 144ss.

ayant la confiance du fournisseur de service et de l'utilisateur (Trusted Third Party, TTP), ou encore sous le contrôle d'un notaire numérique.

Avec le protecteur d'identité, le système d'information est divisé en deux domaines: l'un où l'identité est connue, l'autre où seul le pseudonyme apparait. Il peut être installé partout où un système d'information permet l'échange de données personnelles. Il permet de protéger la sphère privée de l'utilisateur lors de l'accès à un service, non seulement à l'égard du service, mais également vis-à-vis des autres utilisateurs. Par exemple, un utilisateur d'internet n'a pas toujours un accès direct au réseau. Il doit passer par un intermédiaire qui lui procure l'accès. Le système d'information lui procure le pseudonyme qui lui permet ainsi de bénéficier des prestations du service offert, par exemple la tv-payante ou l'achat de biens sur internet.

Le système doit être conçu de manière à ce que les abus ou les actes pénalement répréhensibles soient empêchés. Ceci peut se faire par des mesures de prévention, de détection ou de répression. Par le biais de données biométriques chiffrées ou d'une signature numérique, ou d'une combinaison des deux, on peut concevoir le protecteur d'identité de manière à ce que l'utilisateur ne puisse pas abuser de son identité.

Le protecteur d'identité permet donc l'annonce et le contrôle de l'identité, l'octroi d'un pseudonyme, la transformation du pseudonyme en identité (et vice-versa), la transformation du pseudonyme en d'autres pseudonymes, ainsi que la lutte contre les abus. ■

L'AUTRE REGARD
DIE ANDERE SICHT