AVIS N° 34 / 2000 du 22 novembre 2000

N. Réf. : 10 / A / 2000 / 035 / 002

OBJET : Avis d'initiative relatif à la protection de la vie privée dans le cadre du commerce électronique.

La Commission de la protection de la vie privée,

Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en particulier l'article 29;

Vu le rapport présenté par le Président;

Emet, d'initiative, le 22 novembre 2000, l'avis suivant :

I. INTRODUCTION

Le réseau Internet, à l'origine destiné à faciliter les échanges d'informations à l'échelle planétaire, représente également aujourd'hui un outil commercial de choix pour les entreprises.

Celles-ci bénéficient ainsi d'une plus grande visibilité, de coûts de gestion réduits et de contacts plus immédiats avec le consommateur. Les entreprises de taille réduite, en particulier, peuvent tirer avantage des possibilités illimitées de diffusion que permet le réseau.

Eu égard à son caractère complexe et tentaculaire, les entreprises sont néanmoins conduites, afin de se distinguer de leurs concurrentes et d'attirer l'attention du consommateur, à utiliser les moyens technologiques les plus perfectionnés en matière de publicité et de techniques de vente en ligne.

Ces techniques qui visent à mieux identifier le consommateur afin de maximiser les chances de vente en ligne génèrent la collecte et le traitement d'un nombre toujours croissant de données à caractère personnel. Des atteintes à la vie privée peuvent être identifiées en particulier au stade de la prospection commerciale, et au stade de la transaction proprement dite.

1. Prospection commerciale.

Afin de cibler au mieux leurs publicités, les entreprises mettent en œuvre différentes techniques permettant de dresser le profil des visiteurs de sites web.([1])

- Le consommateur communique dans certains cas les informations le concernant **sur une base volontaire** : lors de la participation à un jeu ou à un concours sur Internet par exemple, lorsque cette participation est conditionnée par la communication de données à caractère personnel. La fourniture de services tels que la souscription à un abonnement Internet gratuit est en général également sujette à la collecte de données à caractère personnel concernant le futur abonné.

- Des informations sont collectées **à l'insu du consommateur** par certains gestionnaires de sites et entreprises publicitaires. Cette collecte s'opère à l'aide de « cookies ([2]) », c'est à dire sur base d'informations stockées dans un fichier texte sur l'ordinateur du consommateur. Lors de la visite d'un site web, des informations relatives par exemple aux pages visitées, aux préférences en matière de langue, à la nature des recherches effectuées sur un moteur de recherche, vont être stockées sur le cookie et renvoyées au gestionnaire du site lors de chaque nouvelle visite du particulier. Les informations contenues dans le cookie vont ainsi peu à peu constituer un profil de plus en plus précis des habitudes et préférences de l'utilisateur, ce qui permettra de lui proposer des produits censés correspondre à ses goûts.

---

1 La description qui suit repose en grande partie sur un rapport du groupe de l'article 29 de la Directive européenne 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 (J.O., L281 du 23 novembre 1995), ci-après la directive 95/46/CE. Le rapport « Privacy and the Internet – An integrated EU approach to on-line data protection » est issu des travaux de la Task Force Internet du Groupe de l'article 29, auxquels la Commission belge de la protection de la vie privée a activement pris part.
Le groupe de l'article 29 (ci-après « groupe 29 ») rassemble les représentants des commissions nationales de protection des données de l'Union européenne.

2 Ne sont pas visés ici les cookies de « session », utilisés par certains sites web dans le but de s'assurer que certaines requêtes indissociables les unes des autres sont bien émises par la même personne (par exemple lors d'achats successifs lors d'une même visite). Ce type de cookie, comme son nom l'indique, disparaît lorsque l'utilisateur clôture sa visite du site, sans conservation d'informations sur son disque dur.

L'envoi de cookies lors de la visite d'un site web n'est pas seulement le fait de gestionnaires de sites mais également celui d'entreprises publicitaires, qui sont présentes sur de nombreux sites web par l'intermédiaire de leurs bannières publicitaires. Si l'ordinateur de l'utilisateur n'est pas configuré afin de lui permettre de refuser en bloc tous les cookies, ou de soumettre chaque envoi de cookie à son autorisation, cet ordinateur emmagasinera dans son disque dur des cookies de diverses origines de façon tout à fait invisible.

- Une entreprise qui utilise le **courrier électronique** pour diffuser sa publicité dispose de différents moyens de se constituer une liste ciblée d'adresses de particuliers : en récoltant directement ces informations sur une base volontaire auprès de ses clients ou des visiteurs de son site, en achetant ou en louant des listes fournies par des sociétés tierces ([3]) ou en récoltant elle-même ces informations dans des espaces publics tels que des annuaires e-mail publics ou des listes de publipostage électronique, des groupes de nouvelles ou des espaces de conversation.
  Les recherches d'adresses e-mail dans les espaces publics peuvent être effectuées de façon automatique à l'aide de logiciels utilisant par exemple des listes de mots clés liés à un domaine d'intérêt prédéfini (ex: sports, voyages), afin d'obtenir des listes d'adresses d'utilisateurs ciblées selon leurs goûts et correspondant au domaine de commercialisation de l'entreprise.
  Certains outils informatiques sont également spécialisés dans l'envoi de courriers électroniques en masse de façon automatique (envois communément désignés par le terme « spam »). Ces outils peuvent être configurés pour contourner les filtres anti-spam installés par des fournisseurs de services.

2. Transactions en ligne.

Parmi les types de transactions qui se sont développées sur Internet, on distingue la fourniture de biens et services intangibles par des sociétés de logiciels et de communication (logiciels, jeux, musique, journaux) qui sont vendus et distribués en temps réel par le biais du réseau, et la fourniture de biens tangibles qui recouvre aujourd'hui des secteurs d'activité très variés, tels que la vente de vêtements, de livres, etc. Contrairement aux premiers, ceux-ci nécessitent une structure de livraison au particulier.

Ces sociétés peuvent avoir leur site propre, ou être intégrées à des centres commerciaux ou des portails, qui permettent à différents vendeurs, répertoriés selon le type de produits proposés, de bénéficier de la structure d'hébergement du site et parfois d'une infrastructure de paiement.

Dans le cadre d'une transaction en ligne, différents détails personnels sont habituellement communiqués au vendeur, en ce compris les noms et prénom de l'intéressé, son numéro de carte de crédit, son adresse, et ce, aux fins de garantir l'authentification de l'acheteur, le paiement, et la livraison des biens ou services commandés.

Outre les questions liées à la sécurité et à la confidentialité des informations transmises, les données collectées à l'occasion de la transaction risquent de faire l'objet d'utilisations secondaires, telles que constitution d'un profil du client à des fins ultérieures de marketing, ou telles que la combinaison de ces données de transaction avec des informations collectées de façon invisible à l'occasion des différentes visites du consommateur sur le site web du vendeur.

Les perspectives en matière de développement du commerce électronique passent en outre par l'utilisation de nouveaux moyens de profilage du consommateur. Ainsi, la naissance du commerce électronique mobile se base sur la nouvelle génération de téléphones mobiles qui permet d'accéder, via un nouveau protocole de transfert de données, au réseau Internet et à l'utilisation du courrier électronique. Les données de localisation de l'utilisateur du téléphone constituent autant d'indications sur les déplacements de celui-ci, ses habitudes de voyage, et permettent d'adapter des

[3] Ces listes peuvent également contenir des adresses e-mail récoltées sur des espaces publics Internet.

publicités envoyées directement sur le téléphone en tenant compte de l'endroit où se situe son utilisateur. Cette nouvelle perspective de commerce électronique est déjà mise en œuvre aujourd'hui par certains fournisseurs de services Internet, notamment aux Etats-Unis.

L'incertitude des utilisateurs quant à la façon dont sont traitées leurs données à caractère personnel lors de la visite d'un site Internet, les questions de sécurité relatives à la communication d'informations, en particulier dans le cadre de paiements en ligne, représentent à l'heure actuelle des freins majeurs au développement du commerce électronique.
Il importe dans ce contexte de rappeler le contenu des dispositions juridiques existantes qui visent à encadrer le traitement de données à caractère personnel sur Internet et à renforcer la transparence et la fiabilité de tels traitements. L'objectif du présent avis est d'expliciter l'application de ces principes en matière de protection de la vie privée.

II. PRINCIPES JURIDIQUES APPLICABLES.

Outre la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ([4]) qui s'applique de façon générale à tout traitement de données à caractère personnel sur Internet, certaines disposition spécifiques à la réglementation des courriers électroniques non sollicités doivent également être prises en compte : on se réfèrera en particulier à la loi du 14 juillet 1991 relative aux pratiques du commerce et à l'information et la protection du consommateur ([5]) , ainsi qu'à l'adoption récente de la directive 2000/31/CE relative au commerce électronique ([6]) et à l'initiative de révision de la directive 97/66/CE relative à la protection de la vie privée dans le secteur des télécommunications, qui vise à renforcer la protection du consommateur dans ce dernier domaine.

1. Champ d'application de la loi relative à la protection de la vie privée.

La loi s'applique à tout traitement de données à caractère personnel, une donnée à caractère personnel consistant en toute information concernant une personne physique identifiée ou identifiable.([7])
La question se pose de savoir à partir de quand une personne peut être considérée comme identifiable sur Internet. La réponse que fournit la loi à cette question est particulièrement large : une personne est identifiable « dès qu'elle 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 ».

Tant la directive européenne 95/46/CE ([8]) que l'exposé des motifs de la loi du 8 décembre 1992 ([9]) précisent que la personne concernée ne doit pas nécessairement être identifiée / identifiable par le responsable du traitement, mais par n'importe quelle personne, « par quelque moyen qui puisse raisonnablement être mis en œuvre par cette personne ».

---

4 Telle que modifiée par la loi du 11 décembre 1998, M.B., 3 février 1999, ci-après « la loi ». La Commission préconise d'ores et déjà la prise en considération des modifications apportées par la loi du 11 décembre 1998 qui entreront en vigueur dans les prochains mois, et qui auraient déjà dû être transposées en vertu de la directive européenne 95/46/CE depuis le 24 octobre 1998. Ces dispositions s'appliquent déjà à certains responsables de traitements en vertu des principes de l'effet direct et de l'interprétation conforme des textes de droit communautaire.

5 Telle que modifiée par la loi du 25 mai 1999, M. B., 23 juin 1999.

6 Directive 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, J.O. L178 du 17 juillet 2000.

7 Articles 1 et 3.

8 Considérant 26 de la directive.

9 Chambre des représentants de Belgique, exposé des motifs du projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 20 mai 1998, Doc. Parl. 1566/1 – 97-98, p. 12.

Outre les informations communiquées volontairement par l'utilisateur dans le cadre de réponses à un formulaire, des informations transmises de façon invisible par l'utilisateur (informations relatives aux pages visitées, préférences en matière de langue, adresse e-mail, etc.) peuvent être collectées via un identifiant tel que le cookie ou l'adresse IP (lorsque celle-ci est permanente ([10])) de l'utilisateur. La loi s'applique au profil de l'utilisateur ainsi constitué, sans qu'il soit nécessaire, aux termes de la loi, que le responsable du traitement dispose du nom ou de l'adresse de l'utilisateur.
Il est en tout état de cause possible, par l'intermédiaire du fournisseur d'accès Internet, d'obtenir des informations complémentaires relatives à l'utilisateur (et de retrouver par exemple son numéro de téléphone, son nom ou son adresse).

On se trouve donc dans de telles circonstances en présence de données à caractère personnel qui bénéficient de la protection prévue par la loi.

Toute personne qui détermine les finalités (par exemple collecte des données à des fins de constitution de profils marketing) et les moyens du traitement de telles données (formulaires en ligne, cookies, etc.) est considérée comme responsable du traitement aux termes de la loi, et devra prendre en considération les principes développés ci-après dans le cadre de ce traitement.

2. Finalité poursuivie par le responsable du traitement.

a. La détermination de la finalité du traitement est un élément essentiel de la protection des personnes. Elle aura des conséquences directes sur les modalités d'application de la loi, et devra de ce fait être établie de façon suffisamment précise. On souligne que cette disposition a pour conséquence d'interdire la collecte de données (par exemple les adresses des sites Internet visités par un utilisateur) simplement parce que ces informations « pourraient servir ultérieurement » à des fins non encore déterminées.

b. Le responsable du traitement devra s'assurer du **caractère légitime** de la finalité poursuivie, visé à l'article 4 de la loi.
La Commission rappelle que la légitimité des traitements doit être jugée en application du *principe de proportionnalité* : l'intérêt général ou les intérêts légitimes du responsable du traitement doivent être mis en balance avec le droit à la protection de la vie privée de la personne enregistrée.
Ce principe est repris à l'article 5f de la loi.([11]) Dans certaines circonstances, et notamment lorsque des données sont collectées et utilisées à des fins de marketing ciblé (marketing « one to one »), il ne paraît pas qu'un équilibre entre les droits et intérêts des parties en présence soit atteint. Il faudra dans de cas obtenir le consentement de la personne concernée, tel que le prévoit l'article 5a.([12])

---

[10] Une adresse IP permanente reste identique à chaque nouvelle session de l'utilisateur, contrairement à une adresse dynamique : le particulier qui dispose d'une adresse dynamique se voit attribuer à chaque nouvelle connexion une nouvelle adresse par son fournisseur d'accès. Jusqu'à présent les entreprises utilisaient majoritairement des connexions permanentes, alors que les particuliers se connectaient via des adresses dynamiques. Le développement de nouvelles techniques de connexion, en particulier par le câble et l'ADSL, va néanmoins contribuer à la généralisation de l'utilisation d'adresses IP permanentes.

[11] Ce caractère légitime peut découler de différentes hypothèses mentionnées à l'article 5 de la loi :
- lorsque la personne concernée a indubitablement donné son consentement (article 5, a.);
- lorsque le traitement est nécessaire à l'exécution d'un contrat (article 5, b.);
- lorsqu'il est nécessaire à l'exécution d'une loi, d'un décret ou d'une ordonnance (article 5, c.);
- lorsqu'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée (article 5, d.);
- lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique (article 5, e);
- et dans le respect de la balance des intérêts du responsable du traitement et de la personne dont les données sont collectées (article 5, f.).

[12] Un exemple de circonstances dans lesquelles l'équilibre entre les droits et intérêts des parties n'est pas atteint est développé au point 4 : il s'agit du commerce électronique non sollicité.

Le traitement de données doit en outre être un *moyen adéquat et nécessaire* à la réalisation de l'objectif poursuivi.

Ainsi, si le but d'une collecte d'informations sur les visiteurs d'un site Internet est d'effectuer des analyses statistiques sur la fréquentation du site, il n'est pas nécessaire de collecter des données qui permettent l'identification des visiteurs : des informations anonymes suffisent.

De même, l'utilisation de cookies, de plus en plus répandue car elle permet au responsable d'un site de mieux cibler le comportement d'un visiteur, est souvent présentée comme un moyen « indispensable » au bon déroulement de la visite du site. Or, si certains cookies peuvent faciliter la visite d'un site (par exemple lorsqu'ils évitent au particulier de préciser à chacun de ses passages la langue dans laquelle il souhaite voir les informations s'afficher), ils sont rarement nécessaires. Seuls les cookies de session, qui permettent d'établir un lien entre des requêtes indissociables les unes des autres ([13]) peuvent s'avérer nécessaires dans certaines circonstances (lors d'achats dans un supermarché en ligne, par exemple).

La Commission insiste sur le fait qu'il est contraire au principe de légitimité de subordonner l'accès à un site Internet à l'acceptation de cookies, sauf si ces cookies sont des cookies de session absolument nécessaires pour répondre à la requête de l'utilisateur.

En principe, l'utilisateur devra donc toujours être mis en mesure de refuser les cookies que le responsable du site lui envoie, et être à même néanmoins d'accéder aux différentes pages du site concerné.

c. Le principe de finalité implique également que les données traitées **ne peuvent être utilisées d'une manière incompatible** avec le but clairement défini et légitime. En d'autres termes, les données doivent être utilisées dans le cadre de la finalité déclarée et ne peuvent donner lieu à d'autres utilisations, telles que celles qui suivent :

Les données communiquées par un acheteur, par exemple dans le cadre d'une transaction (nom, adresse, centres d'intérêts déduits de la nature des achats), ne peuvent ainsi être réutilisées et transmises par le vendeur à un tiers (une société de crédit, une compagnie d'assurances, etc.) qui serait intéressé par le profil des clients.

En ce qui concerne la collecte d'adresses de courrier électronique sur des sites publics tels que des forums, groupes de discussion (généralement désignés par le terme « chat »), annuaires ou listes de diffusion, le principe de compatibilité a pour conséquence que ces adresses, qui sont diffusées dans un contexte bien spécifique, ne peuvent pas être collectées et réutilisées à des fins de prospection commerciale.

d. Ce principe stipule encore que les données traitées par rapport aux finalités clairement définies et légitimes, doivent être **adéquates, pertinentes et non excessives.**

Un particulier désirant par exemple s'abonner à une revue gratuite d'information en ligne devra nécessairement communiquer son adresse e-mail. Par contre, il ne devrait pas voir sa demande conditionnée par le renvoi d'un formulaire par lequel on lui demanderait son nom, son numéro de téléphone, son adresse, ses centres d'intérêts, etc. Si un tel traitement devait être envisagé par le responsable du site, à des fins de profilage des abonnés par exemple, il s'agirait d'une finalité distincte, devant être clairement identifiée comme telle et donnant lieu à une collecte facultative, et séparée de celle nécessaire à la procédure d'abonnement.

[13] Voyez supra, note 2.

3. Droit d'opposition et conditions de traitement des données.

La loi prévoit en son article 12 le droit pour toute personne de s'opposer, pour des raisons sérieuses et légitimes tenant à une situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf lorsque celui-ci est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie, ou lorsque le responsable du traitement doit effectuer ce traitement en vertu d'une obligation légale.

Ce droit d'opposition peut en revanche être exercé sans aucune justification lorsque les données sont collectées à des fins de marketing direct. Les modalités d'exercice de ce droit sont développées ci-après (point 4).

La Commission rappelle par ailleurs qu'en vertu de l'article 12bis de la loi, un traitement de données automatisé, destiné à évaluer certains aspects de la personnalité d'un particulier, ne peut constituer le seul fondement d'une décision produisant des effets juridiques à l'égard de ce particulier.

Ce traitement pourra néanmoins être utilisé si la décision est prise dans le cadre d'un contrat (article 12 bis, § 2), à condition que des mesures soient prises afin de sauvegarder les intérêts légitimes de l'intéressé. Celui-ci devra au moins être à même de faire valoir utilement son point de vue.

Si par exemple une entreprise de crédit effectue une évaluation de solvabilité en se basant sur des données à caractère personnel collectées sur le réseau, l'intéressé aura le droit de faire valoir son point de vue avant qu'une décision ne soit prise à son égard en matière d'octroi d'un crédit.

4 Transparence du traitement.

La loi prévoit en son article 9 les informations qui doivent être communiquées à la personne dont les données sont collectées :

a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant;
b) les finalités du traitement;
c) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de direct marketing;
d) d'autres informations supplémentaires, notamment :
- *les destinataires ou les catégories de destinataires des données,*
- *le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse,*
- *l'existence d'un droit d'accès et de rectification des données la concernant;*
  sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont obtenues, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

La collecte des données à caractère personnel peut être effectuée de façon visible ou invisible.

- Lorsqu'elle est visible, et qu'elle a lieu par exemple de façon volontaire par le biais d'un formulaire en ligne, le particulier devra recevoir les informations mentionnées supra au moment de la collecte, c'est-à-dire par un encart bien en évidence sur la page où figure le formulaire de collecte des données.
  L'information relative au caractère obligatoire ou non des informations à communiquer par le particulier peut être indiquée par exemple à l'aide d'un astérisque.
  Le droit de s'opposer au traitement des données à des fins de marketing direct ainsi qu'à la transmission des données à des tiers peut être effectué via deux cases distinctes à cocher selon que le particulier s'oppose ou non à de tels traitements.

Il ne devra être effectué aucune discrimination dans le cadre de la fourniture du service ou du produit demandé vis-à-vis de ceux qui auront refusé de répondre aux questions facultatives, ou qui auraient utilisé la faculté ou le droit de s'opposer au traitement de leurs données à des fins de marketing.

- Lorsque la collecte est invisible, ce qui est le cas des collectes d'informations à l'aide de cookies, une information générale devra être fournie à l'utilisateur sur la nature et la fonction précise de chaque cookie utilisé par le responsable du traitement. Il devra également être indiqué à l'utilisateur de quelle façon celui-ci a la possibilité de refuser ces cookies.
  On souligne que si des cookies sont envoyés au particulier non seulement par le site sur lequel il se trouve mais également par une société présente sur le site par l'intermédiaire d'une bannière publicitaire, l'information fournie au particulier devra également faire état de l'existence et de la finalité de ces cookies, et des garanties prises par le responsable du site avec la société de publicité afin d'assurer la protection de la vie privée des visiteurs du site.

Cette information sur les cookies, de même que la politique générale du responsable du site en matière de vie privée (en ce compris les conditions d'exercice du droit d'accès et de rectification des données), devrait être rendue accessible, par le biais d'un hyperlien,([14]) depuis la page d'accueil ainsi qu'à partir de toutes les pages du site où une collecte de données à caractère personnel est effectuée.

Un moyen simple de contacter le responsable du traitement (afin notamment d'exercer le droit d'accès) devra être prévu et indiqué dans cette même rubrique. Outre l'adresse physique et le nom de la personne à contacter, une adresse e-mail pourra également être indiquée.

Ces principes sont d'application lorsque les données sont collectées directement auprès de la personne concernée. Lorsque ce n'est pas le cas, la loi prévoit que l'information devra être communiquée au particulier dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données.

En pratique, le particulier sera le plus souvent informé de l'existence d'un traitement concernant ses données à caractère personnel lors de la réception d'un courrier électronique publicitaire non sollicité. C'est à l'occasion de cet envoi que sont en général communiquées les informations concernant le traitement de données.

5. Réglementation de l'envoi de courriers électroniques non sollicités (« spam »).

Ainsi qu'il l'a été mentionné supra, la collecte d'adresses e-mail à des fins de marketing peut avoir différentes origines. La Commission rappelle qu'elle considère contraire au respect du principe de finalité la collecte effectuée à des fins de marketing sur des sites de discussion ou autres espaces publics dont le but est par exemple l'échange de vues sur des sujets déterminés.

Les adresses sont parfois acquises par d'autres moyens, tels que la communication par un proche du particulier. Un certain nombre de sites proposent ainsi aujourd'hui à leurs visiteurs de fournir des informations les concernant, mais concernant également leurs proches ou amis.

Ces informations concernant des tiers vont être utilisées par l'entreprise, le plus souvent à des fins de marketing direct par le biais du courrier électronique (c'est-à-dire de « spam »). Ce type de pratique doit selon la Commission être soumis à des conditions strictes en matière de protection de la vie privée.

[14] Il s'agit d'un lien pré-défini, qui se présente, sur une page web, sous la forme d'un texte (habituellement en bleu, souligné) ou d'une petite image. Lorsque l'utilisateur clique sur ce lien, la page ou l'objet auxquels le lien renvoie s'affiche directement sur l'écran de l'utilisateur.

La Commission rappelle qu'en vertu de l'article 5f de la loi, le traitement des données peut être effectué *« lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui peut prétendre à une protection au titre de la présente loi.»*

La Commission est d'avis que la collecte d'adresses électroniques et leur utilisation à des fins de marketing à l'insu de l'individu est un exemple d'utilisation de données à caractère personnel à des fins de marketing « one to one » contraire aux intérêts et aux droits et libertés fondamentaux de l'individu. La collecte ne devrait pouvoir être effectuée que si l'individu a donné son consentement préalable (opt in) au traitement de ses données à caractère personnel.

La faculté qui serait laissée au particulier de s'opposer a posteriori (opt out) à ce traitement est insuffisante.

Cette position prend en considération le fait que, lors de la réception d'un courrier électronique non sollicité, c'est le particulier qui subit les contraintes financières et les contraintes de temps liées au téléchargement des messages non sollicités. Elle observe en outre que l'utilisation de systèmes automatiques d'envoi de courriers électroniques en masse accroît les risques d'une utilisation non contrôlée et systématique des adresses de particuliers, sans véritable possibilité de réaction de ces derniers. Elle insiste, dès lors, pour que ce type de courrier se voie appliquer le régime dont bénéficie aujourd'hui la publicité par fax et par automate d'appel, tel que visé par l'article 82 de la loi du 14 juillet 1991.

L'adoption d'un tel régime est rendue possible par les directives européennes 97/66 relative à la protection de la vie privée dans le secteur des télécommunications,([15]) et 97/7 relative aux ventes à distance.([16]) Le régime de l' « opt in » a déjà été mis en application dans cinq pays de l'Union européenne ([17]) et pourrait se voir généralisé dans un avenir proche à l'ensemble des Etats de l'Union européenne. Le principe du consentement préalable en matière de courrier électronique non sollicité à des fins de marketing est en effet rendu obligatoire par la Commission européenne dans son projet de modification de la directive 97/66/CE relative à la protection de la vie privée dans le secteur des télécommunications.

En attendant que le régime de l' « opt in » soit rendu obligatoire de façon explicite en droit belge, des moyens complémentaires de protéger le particulier doivent être adoptés. Ainsi, les communications commerciales devront pouvoir être identifiées de manière « claire et non équivoque dès leur réception par le destinataire.»([18])
Cette information devrait consister en l'insertion dans l'en-tête du message du signe « Pub » ou « Ad », qui permettrait aux fournisseurs d'accès Internet et aux particuliers de filtrer les messages qui leur sont destinés et le cas échéant de refuser directement et automatiquement les messages à caractère commercial.

Le corps du message devra également contenir des informations complètes et précises relatives à l'identité du responsable du traitement, son adresse, la finalité du traitement, et indiquer une façon simple et directe au particulier de demander la suppression de ses données, par exemple en cliquant sur un hyperlien figurant dans le message ou en renvoyant une réponse directement à l'adresse électronique mentionnée dans le message.

---

15 Article 12 al. 2
16 Articles 10 et 14.
17 L'Allemagne, l'Autriche, l'Italie, la Finlande et le Danemark.
18 Ces principes sont prévus par la directive sur le commerce électronique, pour les pays qui à l'heure actuelle se contentent d'un droit d'opposition du particulier (article 7) : 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 («directive sur le commerce électronique») Journal officiel n° L 178 du 17/07/2000. Cette directive devra être transposée en droit interne avant le 17 janvier 2002.

Le particulier devra être informé de ce qu'il peut exercer ce droit de refus à tout moment ultérieurement.

La Commission recommande en outre que les prestataires qui envoient de tels messages respectent les registres "opt-out" existant en Belgique, dans lesquels les personnes physiques qui ne souhaitent pas recevoir de communications commerciales peuvent s'inscrire.

6. Sécurité et confidentialité.

L'article 16 de la loi dispose que :

> *§ 3. Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance.]*
>
> *§ [4]. Afin de garantir la sécurité des données à caractère personnel, le [responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel] contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.*
>
> *Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels. »*

Les articles 314 bis du Code pénal et 109 ter D de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques posent également le principe de la confidentialité des communications et télécommunications.

En vertu de l'article 314 bis, il est interdit de prendre connaissance, faire prendre connaissance, enregistrer ou faire enregistrer, pendant leur transmission, des communications ou télécommunications privées auquel on ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications.

L'article 109 ter D prévoit qu'il est interdit, « *sous réserve de l'autorisation de toutes les autres personnes directement ou indirectement concernées par l'information (…) de prendre frauduleusement connaissance de l'existence de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature transmis par voie de télécommunication (…) [et] de prendre connaissance intentionnellement de données en matière de télécommunications, relatives à une autre personne*. »

En pratique, les responsables de données doivent prendre des mesures appropriées pour protéger les informations fournies par leurs clients contre tout accès ou divulgation non autorisés, et en particulier lorsque le processus implique la transmission de données sur un réseau, ce qui est le cas notamment des transactions électroniques sur Internet.

Selon les risques identifiés d'atteinte à la protection des données, des mesures organisationnelles et techniques devront être adoptées afin de sécuriser les traitements de données. Parmi les mesures techniques appropriées, la technologie du cryptage devrait être employée pour protéger la confidentialité de certains messages, et leur intégrité devrait être garantie par le biais de la signature électronique.

Pour sécuriser les transactions, différentes méthodes sont actuellement développées, qui se basent sur la technologie du cryptage et des certificats électroniques (ces derniers permettent notamment de vérifier l'identité du serveur). Le système SSL (Secure socket layer) par exemple, utilisé par les navigateurs les plus courants, permet d'ouvrir un canal sécurisé entre les ordinateurs du consommateur et du vendeur. Certains protocoles plus récents visent à garantir la confidentialité des communications (par cryptage), l'authentification des parties - titulaire de la carte de crédit, émetteur de la carte, vendeur, acheteur, et plate-forme de paiement (grâce aux certificats électroniques), et l'intégrité et l'irrévocabilité des instructions de paiement pour les biens et services (grâce aux signatures électroniques).

La Commission considère qu'une distinction doit être faite entre les certificats qui concernent *l'identité* de l'utilisateur, et ceux qui concernent les *attributs, ou certaines qualités* de cet utilisateur. Parmi les différents attributs que peuvent comporter les certificats, l'utilisateur auquel se rapportent ces informations devrait techniquement être mis en mesure de sélectionner ceux des attributs qu'il désire faire parvenir à son interlocuteur dans le cadre d'une communication déterminée. Un certificat pourrait ainsi être utilisé de façon à communiquer au correspondant une certaine qualité de l'utilisateur – comme sa fonction professionnelle, si cela s'avère nécessaire dans le cadre de cette communication, sans que d'autres attributs non nécessaires, par exemple sa qualité de membre d'une association, ne soient transmis. Il importe également que l'utilisateur puisse utiliser et envoyer un certificat concernant son identité sans que ne soient joints des certificats concernant ses différents attributs.

La Commission souligne en outre que dans certaines circonstances, la transmission d'informations contenues dans le certificat relatives à *l'identité* de l'utilisateur ne doit pas être requise : ainsi, une transaction qui dans la vie « réelle », peut être effectuée sans communication d'identité, doit pouvoir l'être de la même façon sur Internet, à partir du moment où le vendeur a obtenu des garanties suffisantes quant à la fiabilité (en particulier la solvabilité) de son interlocuteur.([19])

Les mesures adoptées en matière de sécurité des données de transaction ne doivent pas se limiter à la protection des *échanges* de données lors de transactions, mais assurer également la sécurité des données *stockées* par le responsable du traitement. L'accès à ces données doit être restreint, de façon électronique par le biais de logiciels filtrant l'accès aux données, et de façon physique, en limitant la qualité et le nombre des personnes habilitées à accéder et à consulter les données.

7. Conservation des données à caractère personnel.

L'article 4, 5° de la loi dispose que les données à caractère personnel ne peuvent être conservées plus longtemps que nécessaire à la réalisation des finalités pour lesquelles elles ont été obtenues.

Les numéros de cartes de crédit utilisés pour une transaction spécifique ne peuvent par exemple être gardés en mémoire dans un fichier du vendeur une fois que le paiement a été effectué.

[19] Voyez à cet égard les dispositions relatives à l'utilisation de pseudonymes, telles que prévues à l'article 8 de la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, J.O., L13/12 du 19 janvier 2000.

En ce qui concerne les données de trafic, la Commission a considéré, dans son avis 33/99 rendu dans le cadre de l'examen de projets de lois relatifs à la criminalité informatique, qu'un fournisseur d'accès Internet ne devait pouvoir être contraint à enregistrer et conserver des données de télécommunication concernant ses clients que lorsqu'une instruction est ordonnée vis-à-vis d'une personne en particulier.»([20])

Cette position a été affirmée également à plusieurs reprises par le groupe 29, notamment dans ses recommandations 2/99 et 3/99 concernant respectivement le respect de la vie privée dans le contexte de l'interception des télécommunications et la préservation des données de trafic par les fournisseurs de services Internet.([21])

8. Transmission vers des pays tiers ou collecte à partir de ces pays.

Le caractère international du commerce électronique, directement lié aux possibilités de diffusion offertes par Internet, a pour conséquence une circulation fréquente de données à caractère personnel des particuliers entre différents pays, parfois sans que la destination des données soit même identifiée par le consommateur. La Commission est saisie d'un nombre croissant de demandes d'entreprises visant à s'informer des dispositions juridiques à respecter lors de la collecte et du traitement de données à caractère personnel sur une échelle internationale.

Outre une obligation d'information préalable du particulier (et selon le cas l'obtention de son consentement), le responsable du traitement qui envisage de **transmettre des données à caractère personnel vers l'étranger** devra se conformer à différentes obligations, selon le pays vers lequel il entend transférer les données à caractère personnel.([22])

- S'il s'agit d'un pays membre de l'Union européenne, l'harmonisation mise en œuvre en vertu de la Directive 95/46 a pour effet de faciliter la circulation des données à caractère personnel au sein de l'Union européenne. Le responsable du traitement devra en application de ce principe respecter la loi du pays dans lequel il a établi son activité, et sous réserve du respect des dispositions de cette loi (examen de la finalité du traitement, information des personnes concernées, etc.), pourra transférer les données vers un autre pays de l'Union européenne.
- S'il s'agit d'un pays non membre de l'Union européenne, le transfert ne pourra être effectué que si le pays concerné offre un niveau de protection adéquat.([23]) Dans le cas contraire, le transfert ne pourra être effectué qu'en application d'une des conditions de l'article 22 de la loi, et notamment le consentement indubitable au transfert donné par la personne concernée ou des garanties offertes par l'adoption de clauses contractuelles appropriées par l'exportateur et l'importateur des données.([24])

---

20 Avis n° 33/99 du 13 décembre 1999 concernant des projets de loi relatifs à la criminalité informatique. A l'heure où le présent avis est adopté, les projets de loi en question ne sont pas encore définitifs.

21 Recommandation 3/99 relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit, 7 septembre 1999, WP 25 ; Recommandation 2/99 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications, 3 mai 1999, WP 18.
http://europa.eu.int/comm/internal_market/fr/media/dataprot/wpdocs/wpdocs_99.htm

22 Articles 21 et 22 de la loi.

23 Le caractère adéquat du niveau de protection de plusieurs pays a déjà fait l'objet d'une évaluation par le groupe de l'article 29 et le comité de l'article 31 de la directive 95/46/CE (alors que le groupe de l'article 29 rassemble les représentants des commissions nationales de protection des données, le comité de l'article 31 rassemble les représentants des gouvernements des pays membres de l'Union européenne), et d'une décision finale de la Commission européenne en juillet 2000. Il s'agit de la Suisse, de la Hongrie, et des Etats-Unis en ce qui concerne les entreprises qui auront adhéré aux principes dits des « Safe harbors ». Pour plus d'informations à ce sujet, voy. le site de la Commission européenne, Direction générale Marché Intérieur :
http://europa.eu.int/comm/internal_market/fr/media/dataprot/news/index.htm

24 La Commission européenne travaille actuellement à l'élaboration d'un avant-projet de décision, en vertu de l'article 26(4) de la directive 95/46/CE, relative aux clauses types pour le transfert des données à caractère personnel vers des pays tiers qui ne prévoient pas un niveau adéquat de protection pour le traitement de données à caractère personnel (29 Septembre 2000) : http://europa.eu.int/comm/internal_market/fr/media/dataprot/news/index.htm

Lorsque des données sont collectées en Belgique (ou dans tout autre pays de l'Union européenne) **à partir d'un pays tiers**, les dispositions de la loi belge (ou de cet autre pays de l'Union européenne) trouvent à s'appliquer dans des circonstances précises. Ce sera le cas lorsque le responsable du traitement recourt, à des fins de traitement des données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire belge.

Si la notion de moyen n'a pas encore à l'heure actuelle donné lieu à une interprétation définitive, la doctrine s'accorde en général pour considérer que l'utilisation de cookies, qui sont placés sur le disque dur du particulier en Belgique et qui stockent les informations avant de les renvoyer au responsable du traitement à l'étranger, sont bien des moyens de traitement au sens de la loi.

Le particulier résidant en Belgique doit donc dans une telle hypothèse bénéficier de la protection offerte par la loi belge vis-à-vis du responsable du traitement.

9. Mise en œuvre effective des principes de la loi.

1. Codes de conduite

Que ce soit au niveau national ou international, l'élaboration de codes de conduite sur la question du commerce électronique est en pleine croissance. Ces codes abordent en général la question de la protection des données à caractère personnel parmi d'autres aspects tels que la propriété intellectuelle, la sécurité et la confidentialité des réseaux, le respect d'une certaine éthique quant au contenu, ou les questions de responsabilité.

La Commission tient à souligner que l'élaboration et l'utilisation de tels codes au sein de l'Union européenne, et plus particulièrement en Belgique, sont encadrées par les dispositions juridiques citées ci-dessus. La Commission encourage l'élaboration de ces codes dans la mesure où les principes qu'ils proposent présentent une qualité et une cohérence interne suffisantes, et apportent une valeur ajoutée par rapport à la législation applicable en matière de protection des données. Le code doit être suffisamment centré sur les questions et les problèmes spécifiques au secteur du commerce électronique,([25]) et comporter de véritables engagements des acteurs concernés face aux questions propres à ce secteur : par exemple un engagement, de la part des responsables de sites Internet, de ne pas collecter d'adresses e-mail sur les espaces publics à des fins de prospection, de ne pas envoyer de courriers électroniques non sollicités.

L'efficacité d'un tel code de conduite sera d'autant plus grande que celui-ci aura été élaboré en concertation avec les différents acteurs impliqués, et notamment, les entreprises commerciales, les organisations scientifiques impliquées dans le développement des technologies de l'information et de la communication, les instances gouvernementales et les organisations de consommateurs.

2. Normes techniques

Si chaque acteur concerné doit intégrer, au stade du traitement de données auquel il participe, les principes de protection des données à caractère personnel, la Commission constate que l'industrie du software, du hardware ainsi que les responsables de l'élaboration des protocoles et des standards techniques utilisés pour transmettre les informations en réseau ont un rôle primordial à jouer dans la configuration des produits et services mis sur le marché.

[25] Voyez notamment le document du groupe de l'article 29 du 10 septembre 1998 relatif aux « Travaux futurs sur les codes de conduite: Document de travail concernant la procédure d'examen des codes de conduite communautaires par le groupe de travail », WP13.

Eu égard aux possibilités qu'offrent les nouvelles technologies, celles-ci devraient non seulement permettre l'élaboration de produits :

- *conformes* au cadre légal (par exemple par la transmission par les navigateurs Internet du minimum d'informations nécessaires à une connexion, ou par l'adoption de mesures de sécurité adéquates), mais également

- qui *facilitent* l'application des principes (et permettent par exemple un accès direct en ligne par le particulier à ses données, ou un droit d'opposition automatique),

- et qui *améliorent* le niveau de protection des données à caractère personnel : de nouveaux outils, plus connus sous le terme de « privacy enhancing technologies », ont ainsi pour vocation de limiter ou d'empêcher la collecte de certaines données par des moyens techniques ; c'est en particulier la vocation des serveurs proxy, des logiciels de destruction des cookies ("cookie killers"), des logiciels permettant l'anonymat ou l'utilisation de pseudonymes en ligne, ou des filtres e-mail.

La Commission tient à rappeler que ce type de produit ne suffit pas en lui-même à assurer une protection satisfaisante sur le réseau. Il doit être utilisé dans le cadre plus large des règles obligatoires en matière de protection des données, faute de quoi le risque existe de faire reposer la responsabilité de sa propre protection essentiellement sur l'utilisateur, alors qu'en vertu des principes établis au niveau international ([26]) et national, c'est au "responsable du traitement qu'il incombe de respecter les principes prévalant en matière de protection des données".([27])

Compte tenu du degré de connaissance technique nécessaire pour configurer un navigateur Internet ou tout autre outil destiné à la gestion de données à caractère personnel en réseau (par exemple afin de refuser les cookies, de limiter les données qui seront transmises en ligne), il est ainsi primordial que la configuration *par défaut* des outils employés offre le niveau de protection des données à caractère personnel le plus élevé possible, et en tout état de cause un niveau de protection adéquat au regard du dispositif légal applicable. Dans cette optique, la Commission encourage les concepteurs de navigateurs Internet qui sont actuellement configurés pour accepter par défaut les cookies à configurer par défaut ces navigateurs *au moins* pour demander l'autorisation du particulier avant l'envoi de cookies, et à distinguer les conditions d'acceptations des cookies selon que ces derniers sont des cookies permanents ou de session. La Commission recommande en outre que soit simplifié l'accès à ces options de configuration des navigateurs.

III. CONCLUSION

La Commission encourage l'ensemble des acteurs impliqués dans le développement du commerce électronique à prendre en considération le présent avis. Elle souligne qu'une politique de commerce en ligne conforme aux principes légaux de protection des données à caractère personnel est dans l'intérêt du consommateur autant que dans celui de l'entreprise concernée et de son image auprès du public.

---

[26] Lignes directrices de l'OCDE de 1981, Convention 108 du Conseil de l'Europe de 1981, lignes directrices des Nations unies de 1990, directives européennes 95/46/CE et 97/66/CE

[27] Avis 1/98 du 16 juin 1998 relatif à la Plate-forme d'expression de choix en matière de respect de la vie privée (Platform for Privacy Preferences ou P3P) et standard d'établissement de profils ouvert (Open Profiling Standard ou OPS), WP11.

Afin d'augmenter la confiance du consommateur et de favoriser l'utilisation du commerce en ligne par ces derniers, elle émet par ailleurs le souhait de voir la politique suivie en la matière s'aligner sur les exigences de protection actuellement développées au niveau européen et déjà mises en œuvre dans certains pays de l'Union européenne. Une protection particulière du consommateur devrait notamment être imposée en matière de courriers électroniques non sollicités.

La Commission est disposée à cet égard à apporter son assistance à toute initiative législative ou réglementaire visant à promouvoir un cadre juridique certain au développement du commerce électronique.

Pour le secrétaire,
légitimement empêché :

Le président

(sé) G. POPLEU,
conseiller adjoint.

(sé) P. THOMAS.