# Le commerce électronique et la vie privée

Louveaux, Sophie

*Published in:*
Le commerce électronique. 10e journée du juriste d'entreprise, 22 octobre 1999 = De elektronische handel. 10de dag van de bedrijfsjurist, 22 october 1999

*Publication date:*
1999

*Document Version*
le PDF de l'éditeur

# LE COMMERCE ÉLECTRONIQUE ET LA VIE PRIVÉE

PAR

SOPHIE LOUVEAUX

CHERCHEUR AU CRID

## 1. – INTRODUCTION

Le commerce électronique crée de nombreux risques pour la vie privée. Ces risques ne sont pas uniquement liés au commerce électronique en lui-même, mais également à l'utilisation d'Internet.

La masse d'informations qui circulent sur l'Internet ne fait qu'augmenter : il suffit à cet égard de penser aux 150 millions de personnes qui ont accès à l'Internet à travers le monde et qui peuvent transmettre des données à caractère personnel simplement en cliquant sur le bouton «send» de leur e-mail. L'intrusion dans la vie privée ne fait que grandir quand on pense que cette transmission peut également se faire de manière passive et occulte, notamment par le biais de l'utilisation de «cookies» et d'hyperliens invisibles (1).

Or le succès du commerce électronique dépend en grande partie de la confiance qu'ont les consommateurs vis à vis de la protection accordée aux données à caractère personnel qu'ils transmettent.

La nouvelle loi belge du 11 décembre 1998 transposant la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation des données (2), entrera en vigueur en Belgique après l'adoption des arrêtés royaux d'exécu-

(1) A propos des hyphyperliens, voir J.-M. DINANT, «L'électronisation du commerce», *La Revue Générale de Droit*, mars 1999, p. 39.

(2) Adoptée le 24 octobre 1995 et complétant la loi du 8 décembre 1992, *M.B.*, 18.03.1993, p. 5801.

tion (3). Nous devons dès lors envisager ses différents articles afin d'analyser de quelle manière elle s'appliquera aux transactions de commerce électronique et dans quelle mesure la loi peut garantir un niveau de protection adéquat aux yeux des consommateurs désirant effectuer leurs achats sur Internet tout en se préservant contre les atteintes à leur vie privée (4).

### 2. – Les concepts clés

La loi belge s'applique à tout traitement de données à caractère personnel automatisé ou en tout ou en partie, ainsi qu'à tout traitement de données à caractère personnel contenues ou appelées à figurer dans un fichier (5). Puisque le commerce électronique contient des traitements automatisés, il convient de déterminer ce que la loi entend par une «donnée à caractère personnel» afin de déterminer l'applicabilité de la loi. D'autre part, puisque les principales obligations sont à charge du responsable du traitement, il important de déterminer qui peut être qualifié de la sorte.

#### 2.1. – *Donnée à caractère personnel*

Le concept de donnée à caractère personnel est défini comme étant : «toute information concernant une personne physique identifiée ou identifiable» (article 1§ 1 de la nouvelle loi). Il est à noter que les personnes morales sont donc exclues de la protection légale. D'autre part, selon ce même article «est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale».

(3) Pour une analyse approfondie de la loi belge voir TH. Leonard et Y. Poullet, «La protection des données à caractère personnel en pleine (r)évolution la loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995», *J.T.*, 1999, p. 377. F. De Brouwer et S. Louveaux, «Protection des données à caractère personnel : vers une nouvelle loi belge», *Revue Ubiquité*, 1998, p. 83.

(4) Nous n'examinerons pas 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, dans la mesure où il n'est pas encore déterminé si l'ensemble de cette directive peut s'appliquer à l'Internet.

(5) Article 3 de la loi.



Le considérant n° 26 de la directive prévoyait que pour déterminer si une personne était identifiable, il fallait considérer l'ensemble des moyens susceptibles d'être *raisonnablement* mis en œuvre soit par le responsable du traitement, soit par un tiers pour identifier la dite personne. Cela permettait d'admettre comme anonymes des données pour lesquelles le responsable du traitement ne disposait pas des moyens techniques suffisants pour effectuer l'identification (et offrait des garanties suffisantes quant à l'absence de recherche d'identification) même si la possibilité d'identification existait *in abstracto* soit dans son chef soit dans celui d'un tiers (6).

L'exposé des motifs de la loi belge (7) rejette cette interprétation : dès qu'il existe un moyen raisonnable d'identifier la personne concernée soit dans le chef du responsable du traitement, soit dans le chef d'un tiers, il s'agit d'une donnée à caractère personnel et cela même s'il n'y aucune volonté de recherche d'identification de la part du responsable du traitement. Examinons les implications en matière de commerce électronique.

Très souvent, lorsque la personne concernée désire effectuer une transaction électronique, elle livre elle-même ses données à caractère personnel afin de permettre la réalisation de la transaction (elle donnera son nom et son adresse, par exemple, afin de se faire livrer les biens commandés). Nous nous retrouvons de toute évidence en présence d'une personne identifiée. Mais cela n'est pas toujours le cas. Si la personne navigue sur le Web sans livrer elle-même ses données à caractère personnel, elle laissera néanmoins des traces.

En effet, lors de la simple connexion à un site, les données suivantes sont transmises au site par le programme de navigation (8) :

(6) Voir en ce sens M.-H. Boulanger, C. De Terwangne, TH. Leonard, S. Louveaux, D. Moreau, Y. Poullet, «La protection des données à caractère personnel en droit communautaire», *J.T.D.E.*, 1997, p. 125.

(7) Voir Exposé des motifs, *Doc. Parl.*, Ch. Repr., Sess. ord. 1997-1998, n° 1586/1, (ci-après exposé des motifs), p. 12.

(8) Voir J.-M. Dinant, «User Identification and Privacy Protection, Applications in Public Administration and Electronic Commerce», *Proceedings of the joint IFIP WG 8.5 and WG 9.6 Working Conference*, 14-15 June 1999, Kista, Sweden.

- adresse TCP/IP (9),
- marque et version du programme de navigation,
- marque et version du système d'exploitation,
- langue parlée par l'internaute,
- page référante,
- cookies éventuels déjà envoyés par le site.

S'agit-il de données à caractère personnel au sens de la loi ?

Internet permet d'acheminer tout type de données numériques entre deux machines respectivement identifiées par une adresse TCP/IP, c'est à dire l'identité du micro-ordinateur sur le réseau. Il s'agit d'un numéro unique. En pratique, un ordinateur connecté en permanence au réseau aura une adresse TCP/IP fixe, assignée par le gestionnaire de réseau. Un utilisateur occasionnel se connectant par modem recevra, pour la durée de sa connexion, une adresse TCP/IP dynamique, c'est à dire différente d'une connexion à l'autre. L'adresse TCP/IP révèle dès lors l'identité de l'ordinateur sur le réseau, mais elle ne révèle pas en elle-même l'identité de l'utilisateur de l'ordinateur. Dès lors, à moins que l'utilisateur n'ait révélé son identité au site Web, seul le fournisseur d'accès peut faire le lien entre l'adresse TCP/IP dynamique et l'utilisateur, et seul le gestionnaire de réseau peut faire ce même lien entre l'adresse TCP/IP fixe et l'utilisateur (10).

Si on prend cependant l'interprétation de la notion de donnée à caractère personnel telle que développée par l'exposé des motifs de la loi belge, il est clair que dès que le fournisseur d'accès (ou le gestionnaire du réseau) peut identifier la personne (11), il s'agit d'une donnée à caractère personnel, et ce même aux yeux du site Web qui ne connaît pas forcément l'identité de la personne. Le champ d'application de la loi est alors très large.

A cet égard, nous pouvons nous interroger sur le projet d'arrêté royal portant application de l'article 109*ter* E, § 2 de la loi du 21 mars 1991 portant réforme de certaines entreprises

(9) «Transmission control protocol/Internet protocol».

(10) Ou en tout cas l'ordinateur possédant le numéro en question (au sein d'une compagnie, par exemple, le fournisseur ne connaît pas précisément l'identité de l'utilisateur de l'ordinateur).

(11) Pour autant que la personne ne soit pas passée par un «proxy» qui masquerait son adresse TCP/IP au site visité.



publiques économiques (12) en ce qui concerne l'obligation pour les opérateurs de télécommunication et les fournisseurs de services de télécommunication de prêter leur concours (sic). En effet, le caractère particulièrement large du champ d'application de l'arrêté royal permet d'inclure tout fournisseur d'accès, ou fournisseur de service dans le secteur des télécommunications. Cela inclurait donc les fournisseurs d'accès à Internet et peut-être même les opérateurs de sites eux-mêmes. Or ce projet d'arrêté royal, dans le cadre des demandes et réquisitions judiciaires résultant des articles 46*bis*, 88*bis*, 90*ter* et suivants du Code d'instruction criminelle, oblige chaque opérateur de réseaux de télécommunication et, le cas échéant, chaque fournisseur de services de télécommunication d'être en mesure techniquement de repérer, de localiser, d'écouter, de prendre connaissance et d'enregistrer des télécommunications privées. Ils doivent en outre être en mesure non seulement de transmettre la communication en temps réel, mais également de transmettre des données concernant les données d'appel du service de télécommunication surveillé ainsi que le contenu de la communication, de façon à pouvoir les mettre en corrélation de manière précise (13).

D'autre part, les articles 3 et 4 du projet d'arrêté royal envisagent la mise en place, via un protocole conclu entre le Ministre de la justice et les opérateurs et fournisseurs de services, d'un accès direct et automatisé des autorités judiciaires aux banques de données de ces opérateurs et fournisseurs de services. Il nous semble dès lors que dès l'adoption de cet arrêté royal, il n'y aura plus aucun doute de la possibilité d'identification de la personne concernée via son numéro de TCP/IP, dans la mesure où le fournisseur d'accès aura l'obligation légale de pouvoir identifier la personne et de garder une trace des communications qui sont passées par son réseau. En d'autres termes, le numéro de TCP/IP sera, s'il ne l'est déjà, une donnée à caractère personnel.

Le système de cookies, quant à lui, permet à un site visité (ou invisiblement hyperlié : une société de «cybermarketing» infiltrant une bannière publicitaire, par exemple) d'inscrire sur

(12) Comme modifiée par la loi du 10 juin 1998.

(13) Voir article 6 du projet d'arrêté royal.

le disque dur de l'utilisateur des informations sur les sites visités et de marquer ces visiteurs en question, et ce généralement à leur insu. Les cookies permettent donc de s'affranchir du caractère variant de l'adresse TCP/IP dynamique : si celle-ci change, le cookie reste identique de connexion en connexion. A cette marque particulière peut alors être reliée toute une série d'informations sur le parcours de l'utilisateur sur l'Internet. Ces informations permettront notamment aux «cybermarketers» de cibler les consommateurs en fonction des sites visités. Ne s'agit-il pas alors d'une donnée de la personne par référence à un ou plusieurs éléments propres à son «identité économique, culturelle ou sociale»?

*Traitement*

La notion de traitement vise «toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel» (14). Au vu de cette définition élargie, il est difficile d'imaginer une opération sur des données à caractère personnel qui ne constituerait pas un traitement au sens de la loi.

*Responsable du traitement*

Le responsable du traitement est défini comme étant «la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement» (15).

Le commerce électronique est caractérisé par la multitude d'intervenants (fournisseurs d'accès, sociétés de télécommunications offrant le réseau de communication des données, sites

(14) Article 1er, § 2 de la loi.
(15) Article 1er, § 4 de la loi.



offrant leurs biens et services, ...). Il importe de déterminer qui peut être qualifié comme responsable du traitement, car c'est à lui qu'incombe principalement le respect des principes de protection des données que nous allons examiner ci-dessous.

La question qui se pose dès lors est de savoir si oui ou non la personne responsable du traitement détermine la ou les finalités du traitement et les moyens permettant de traiter les données. Un responsable de site effectuant des opérations de commerce électronique détermine les finalités pour lesquelles il traite les données à caractère personnel de ses clients (afin de conclure la transaction et de livrer les biens au client, par exemple) et les moyens du traitement (à savoir dans ce cas l'utilisation du réseau Internet).

La prise de décision quant aux finalités et aux moyens peut également être conjointe, ce qui impliquera alors l'identification de plusieurs responsables à l'égard d'un même traitement. Il se peut aussi que plusieurs entités différentes soient responsables de différentes parties de la transaction. A titre d'exemple, les considérants de la directive 95/46/CE avaient indiqué que «lorsqu'un message contenant des données à caractère personnel est transmis *via* un service de télécommunications ou de courrier électronique dont le seul objet est de transmettre des messages de ce type, c'est la personne dont émane le message, et non celle qui offre le service de transmission, qui sera normalement considérée comme responsable du traitement de données à caractère personnel contenues dans le message; que, toutefois, les personnes qui offrent ces services seront normalement considérés comme responsables du traitement des données supplémentaires nécessaires au fonctionnement du service» (16). Bien que l'exposé des motifs de la loi belge reste muet à ce propos, un raisonnement similaire peut être retenu en droit belge, dans la mesure où la loi a adopté textuellement la définition du «responsable du traitement» de la directive européenne. Ainsi, en matière de commerce électronique, le fournisseur d'accès au réseau n'est peut être pas le responsable du traitement des données émises pour la transaction commerciale qui s'effectue par le biais de son réseau,

(16) Voir le considérant 26 de la directive.

mais il pourra être qualifié de la sorte en ce qui concerne les données personnelles nécessaires à la facturation du service qu'il offre (nom et adresse de l'abonné, jour, heure et durée de la transmission).

*Sous-traitant*

Celui qui traite les données pour le compte du responsable du traitement est qualifié de «sous-traitant» (17). Celui-ci est à distinguer de celui qui traite les données sous l'autorité directe du responsable du traitement (préposé ou fonctionnaire agissant dans le cadre de ses fonctions).

L'Internet est caractérisé par de nombreux contrats de sous-traitance. De nombreux responsables de traitement font héberger leurs sites par d'autres sous-traitants, par exemple. Il s'agit toutefois d'être prudent dans cette qualification de sous-traitant : dans certains cas, l'hébergement d'un site Web peut donner un certain pouvoir à l'hébergeur qui permettrait de le qualifier de responsable, ou du moins de responsable conjoint. En effet, l'hébergeur peut non seulement héberger le site, mais il peut également fournir des services supplémentaires tels que l'analyse des fréquentations du site ou des moyens de paiement pour les transactions qui s'y effectuent.

### 3. – Champ d'application territorial de la loi belge (18)

La loi belge décrit deux facteurs qui déterminent le champ d'application territorial. Selon le premier facteur, la loi est applicable dès que le traitement «est effectué dans le cadre d'activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge ou en un lieu où la loi belge s'applique en vertu du droit international public» (19). Cette disposition suppose deux conditions : il faut d'abord que le traitement soit effectué dans le cadre des activités «réelles et effectives» d'un établissement fixe du responsable du traitement; et que l'établissement du responsable du traitement pour lequel le traitement est effectué soit sur le territoire belge.

(17) Article 1er, § 5 de la loi.

(18) Voir également C. De Terwangne et S. Louveaux, «Data protection and online networks», *The Computer Law and Security Report*, July-August 1997, Vol. 13, Issue 4, p. 237.

(19) Article 3*bis*, 1° de la nouvelle loi.



La première condition implique que c'est la loi du territoire sur lequel se situe l'établissement pour le compte duquel le traitement est effectué qui s'applique. Imaginons, par exemple, une société dont la maison mère est en Angleterre, disposant d'une filiale en Belgique, et qui vend des chaussures en Belgique via son site Web mais sans passer par sa filiale belge (le traitement se fait donc en Angleterre), la loi belge ne s'appliquera pas. Le traitement doit se faire dans «le cadre d'activités réelles et effectives» d'un établissement fixe du responsable.

La deuxième condition implique que l'établissement du responsable du traitement pour lequel le traitement est effectué soit en Belgique. A ce propos l'exposé des motifs de la loi reprend le considérant 19 de la directive selon lequel «l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable» et «la forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard».

Le deuxième facteur qui détermine si la loi belge est applicable, concerne les cas où le responsable du traitement n'est pas établi sur le territoire de la Communauté européenne et «recourt à des fins de traitement des données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire belge, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge» (20).

Une première interprétation de cette disposition consiste à appliquer le texte de l'article à la lettre. Dans le contexte de l'Internet, une telle solution mène alors à l'extension de l'ap-

(20) Article 3*bis*, 2° de la nouvelle loi. D'après l'exposé des motifs, le terme «moyens recouvre tout équipement possible, tels que les ordinateurs, les appareils de télécommunication, les unités d'impression, etc., à l'exclusion, formulée explicitement, des moyens qui sont uniquement utilisés pour le transit des données à caractère personnel par le territoire, tels que les câbles, les routers, etc.» (*Exposé des motifs*, p. 27).

plication de la loi belge dès qu'un utilisateur collecte des données à caractère personnel à partir d'une base de données ou d'un site Web situé sur le territoire belge. Cela impliquerait que cette personne soit qualifiée de responsable du traitement et doive nommer un représentant établi sur le territoire belge afin de respecter l'ensemble des principes de la loi, ce qui semble excessif. D'autre part, il reste le problème de la localisation de la base de données ou du site Web, dans la mesure où une adresse de site ne correspond pas nécessairement à la localisation géographique du site : http://www.telepathic.com ne nous dit pas où ce site se trouve, ni si en consultant les données à caractère personnel qu'il détient nous devons respecter la loi belge.

Une deuxième interprétation, pour laquelle j'opterai, consiste à rechercher la *ratio legis* de l'article 3*bis*. Celle-ci consiste à éviter que le responsable du traitement cherche délibérément à contourner les lois nationales prises en vertu de la directive en délocalisant son établissement dans un pays tiers, tout en utilisant des moyens situés sur le territoire européen, et ce sans tomber sous le coup de l'application des articles sur les flux de données vers les pays tiers. Deux types de catégories de traitement tombent alors dans le champ d'application de l'article 3*bis*, 2° de la loi : le premier vise les traitements portant sur des données à caractère personnel de personnes situées en Belgique effectués par une personne qui a délibérément cherché à contourner la loi en délocalisant son établissement dans un pays tiers, tout en utilisant des moyens situés sur le territoire belge; Le deuxième type vise le cas où le responsable du traitement réalise, par des moyens propres situés sur le territoire belge un flux de données vers un pays tiers où il traite les données (21) (on pense aux cas des cookies placées sur le disque dur d'un belge lors de la consultation d'un site Web). Le critère principal qui détermine l'application de la loi à des responsables situés en dehors du territoire de la Belgique n'est donc pas uniquement limité au recours à des moyens situés sur le territoire de la Belgique. Une analyse plus fouillée

(21) Les articles de la nouvelle loi belge relatifs aux transferts de données à caractère personnel vers des pays tiers non-membre de la communauté européenne ne s'appliqueraient pas dans ce cas, étant donné qu'ils ne s'appliquent que lorsque le responsable du traitement qui effectue le transfert est localisé en Belgique.



doit être effectuée afin de déterminer si le responsable du traitement s'est délocalisé de manière à éviter l'application de la loi belge.

### 4. – Principes de protection des données

#### *Le principe de finalité*

##### *La légitimité de la finalité*

Selon l'article 4, § 1er, 1° de la loi belge, les données à caractère personnel «doivent être traitées loyalement et licitement». Un traitement loyal semble impliquer un maximum de transparence : les données ne peuvent être traitées pour des finalités cachées ou peu claires (22). Dans le contexte d'Internet, l'utilisation de cookies se fait généralement à l'insu de la personne concernée, ce qui ne correspond nullement à un traitement loyal au sens de la loi.

L'article 4 de la loi belge indique également que les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. La finalité déterminée et explicite renvoie de nouveau à l'idée de transparence telle qu'elle se manifeste dans l'obligation d'information de la personne concernée. Quant à la notion de légitimité, déjà présente dans la loi précédente, elle a fait l'objet de nombreux commentaires auxquels nous renvoyons (23).

En ce qui concerne l'obligation de ne pas traiter les données ultérieurement de manière incompatible avec les finalités pour lesquelles les données ont été collectées, la loi précise que la compatibilité doit tenir compte de tous les facteurs pertinents, notamment «des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables». Le recours aux attentes de l'intéressé se comprend de nouveau dans cette

(22) Ce principe est sous-jacent au devoir d'information tel que nous le verrons *infra*.

(23) Voir principalement : Th. Leonard, Y. Poullet, «Les libertés comme fondement de la protection des données nominatives», in F. Rigaux, *La vie privée une liberté parmi les autres?*, Travaux de la faculté de droit de Namur n° 17. Bruxelles, Larcier, 1992, pp. 231 et suiv.; M.-H. Boulanger, C. De Terwangne, Th. Leonard, S. Louveaux, D. Moreau, Y. Poullet, *op. cit.*, p. 145-146.

idée de transparence, afin d'éviter que la personne méconnaisse une utilisation ultérieure des données la concernant. En matière de commerce électronique, par exemple, en ce qui concerne la vente de produits via Internet, les consommateurs qui transmettent leurs données à des fins d'achats sur le site considèrent que les données ainsi transmises ne seront traitées qu'à des fins en lien direct avec le service offert (envoi de la marchandise, facturation du service, ...). Toute autre finalité qui n'entre pas dans le champ de l'attente raisonnable de l'intéressé devra lui être signalée et sera considérée comme une nouvelle finalité à part entière.

*Fondement du traitement*

L'article 5 de la loi prévoit que les traitements ne peuvent être poursuivis que dans l'un des cas visés par cette disposition. Nous allons donc parcourir cet article afin de retenir quelles hypothèses pourraient servir de base à une transaction électronique comportant des données à caractère personnel «non-sensibles» (24). Il convient cependant de signaler que le fait de remplir l'une des conditions de l'article 5 n'implique pas que l'exigence de légitimité de l'article 4, 2° soit d'office rencontrée (25). Les différentes dispositions s'appliquent en effet de manière cumulative : le consentement de la personne concernée, par exemple, ne suffit pas pour légitimer le traitement.

*Le consentement de la personne concernée*

Le traitement peut d'abord avoir lieu «si la personne concernée a indubitablement donné son consentement» : un consommateur qui introduit ses propres données afin d'effectuer un achat sur Internet sera considéré comme ayant donné son consentement au traitement de ses données. Le consentement écrit n'est pas requis.

(24) Par données «sensibles» nous entendons les données qui «révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi (que) les données relatives à la vie sexuelle» et les données médicales et les données judiciaires. Pour une analyse du régime gouvernant ces données voir TH. LEONARD et Y. POULLET, *op. cit.*, p. 386.

(25) Voir «A Business Guide to Changes in European Data Protection Legislation», *Crid-Cullen International*, Kluwer Law International, 1999, p. 46.



Le consentement doit en tout cas être «une manifestation de volonté, libre, spécifique, et informée» (26). Une manifestation de volonté *libre* implique qu'il ne devrait y avoir aucune pression sur l'individu afin d'obtenir son consentement. Le refus d'acceptation du consommateur lors de la demande de données à caractère personnel par un site ne devrait pas être retenu contre lui. Cela est également vrai pour l'utilisation de cookies : le refus d'un cookie ne devrait pas porter préjudice à l'accès au site par le consommateur ni le service fourni par ce site.

Le consentement doit être spécifique : il doit porter sur des traitements précisément définis et non sur des objets généraux. Toute modification de la finalité qui n'est pas considérée comme compatible avec la finalité déclarée requiert donc un nouveau consentement.

Enfin, le consentement doit être *informé* : cela suggère que les vendeurs sur Internet informent les utilisateurs des risques potentiels de l'Internet vis à vis de la protection de leurs données à caractère personnel. Cela permet au consommateur de mettre en balance ces risques avec les bénéfices attendus.

L'interactivité qui caractérise les réseaux tels qu'Internet offre certaines facilités en ce qui concerne le consentement de la personne concernée. Plutôt qu'un consentement donné une fois pour toutes au début d'une série d'opérations, l'interactivité permet de moduler le consentement. Un message peut apparaître sur l'écran annonçant que si le consommateur veut poursuivre la transaction, il doit consentir à livrer telle ou telle information. Il peut accepter une partie de l'opération mais refuser de donner davantage de données à caractère personnel pour une autre partie de la transaction. De plus les mécanismes de «opt-in» ou d"opt-out» prennent une dimension immédiate et effective à travers l'interactivité : le consommateur peut cocher les cases correspondant à des utilisations secondaires de ses données.

(26) Voir la définition donnée à l'article 1er, § 8 de la loi.

*Le contrat*

Le traitement se justifie également si «il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci». Des données à caractère personnel peuvent être requises afin de livrer un bien ou de fournir un service à un consommateur. Cette disposition sert également de base au traitement des données pour l'exécution de mesures précontractuelles mais celles-ci doivent être prises à la demande de la personne concernée. Cette disposition ne peut donc servir de base à l'envoi de mails publicitaires.

*L'intérêt légitime*

Le traitement peut également avoir lieu 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» (27). Cette disposition rappelle de manière explicite le principe de proportionnalité présent dans le principe de légitimité. Se baser sur ce fondement afin de traiter des données à caractère personnel dans le cadre d'une transaction électronique présente cependant un risque dans la mesure où si la balance des intérêts penche plutôt en faveur de la personne concernée, il peut être difficile pour le responsable de trouver une autre base de justification au traitement dans l'article 5.

### *Les principes de conformité et de qualité des données*

Selon l'article 4 § 1er, 3° de la loi, les données à caractère personnel doivent être «adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement». Cette exigence assure qu'il existe un lien suffisant entre les données et

(27) La loi stipule que le Roi peut, par arrêté délibéré en Conseil des ministres et après avis de la Commission de la vie privée, préciser les cas où cette dernière situation est considérée comme n'étant pas remplie.



la finalité poursuivie. De nombreux sites demandent aux visiteurs réguliers, et parfois même également aux surfeurs occasionnels, de remplir un formulaire d'inscription avant de pouvoir accéder au site. Il est essentiel que les données à caractère personnel qui sont demandées soient pertinentes. L'adresse e-mail de l'utilisateur peut être nécessaire afin de fournir le service, alors que des informations sur l'âge de la personne, son statut civil ou ses revenus peuvent être considérées comme des données excessives ou non pertinentes. Ce type de données peut aider l'opérateur du site à constituer des profils de visiteurs soit pour des fins propres, soit pour le compte d'un tiers, mais si ces profils ne cadrent pas dans les finalités déclarées, un tel traitement des données serait incompatible avec les finalités déclarées.

Les données doivent également être «exactes et si nécessaires mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées» (28). Il s'agit donc d'une obligation de diligence du responsable du traitement qui doit tout faire pour que les données soient exactes. La configuration d'Internet ne facilite pas le respect de cette obligation. Il s'agit d'un réseau de données variables en qualité et en exactitude.

La participation de la personne concernée à la collecte des données et la possibilité effective d'un droit de rectification (29) sont des mesures qui peuvent contribuer à la qualité des données.

Les données doivent être «conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement» (30). Ainsi des données collectées auprès d'un client afin de fournir des biens et services, ne devraient pas être gardées au-delà de la période nécessaire pour cette finalité, sauf consentement exprès de la personne concernée.

(28) Article 4, § 1er, 4° de la loi.
(29) Voir *infra*.
(30) Article 4, § 1er, 5° de la loi.

*Le principe de sécurité des données*

L'article 16 de l'ancienne loi belge (31) prévoyait une obligation pour le responsable du traitement de prendre certaines mesures de sécurité. Cette obligation a été maintenue à charge du responsable; mais est maintenant également à charge du sous-traitant. La loi ne prescrit pas de mesures particulières : elles peuvent être de nature organisationnelle ou technique. Le choix des mesures est donc laissé au responsable du traitement qui doit trouver un niveau de protection adéquat compte tenu non seulement de la nature des données à protéger et des risques potentiels, mais également de l'état de la technique, et des frais qu'entraîne l'application de ces mesures. Il est clair à cet égard que l'introduction d'un réseau à échelle mondiale augmente considérablement les risques d'accès par des personnes non autorisées. D'autre part, la publication sur un site d'information qui est déjà dans le domaine public nécessitera moins de précautions que la collecte par e-mail de données médicales, par exemple.

La nouvelle loi définit dans l'article 16 les conditions dans lesquelles les traitements peuvent être confiés à des sous-traitants. Ces derniers doivent apporter des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements, le responsable du traitement devant veiller au respect de ces mesures. Un contrat doit fixer la responsabilité du sous-traitant à l'égard du responsable et prévoir que le sous-traitant ne peut agir que sur l'instruction du responsable.

*Les transferts de données vers des pays tiers*

Le commerce électronique peut et va certainement générer des transferts de données vers des pays tiers. Quels sont les principes et exceptions établis par la loi belge à cet égard ?

(31) Loi du 8.12.92, *M.B.*, 18.03.1993, p. 5801.



*Le principe*

En principe, selon l'article 21 de la loi, «le transfert de données à caractère personnel faisant l'objet d'un traitement après leur transfert vers un pays non-membre de la Communauté européenne, ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions de la présente loi et de ses arrêtés d'exécution». Il semblerait que l'appréciation du caractère adéquat revient au responsable de traitement; toutefois, il est loisible pour le Roi, «après avis de la Commission de protection de la vie privée», de déterminer «pour quelles catégories de traitements et dans quelles circonstances la transmission n'est pas autorisée» (32).

L'évaluation du caractère adéquat de la protection doit se faire avant la transmission des données. Cela ne va pas sans poser certains problèmes dans le contexte du commerce électronique. A cet égard, nous devons distinguer deux types de transferts : les transferts actifs de données, qui sont des transferts initiés par la personne concernée, ou en tout cas avec son accord; et les transferts passifs, qui eux se font à l'insu de la personne concernée.

En ce qui concerne les transferts actifs, en principe la personne concernée consent, au moins implicitement, au transfert de ses données vers un pays tiers (33). Cependant il convient de faire remarquer que les règles émises dans la directive sont basées sur une présomption que les transferts de données suivent toujours un itinéraire précis et direct, ce qui n'est pas le cas des flux sur l'Internet. En effet les messages, ou l'ensemble des données transférées, sont envoyés via le routing le plus rapide au moment de la transmission. Tout obstacle technique lors de la communication engendre un éclatement du message en «paquets» qui suivront un itinéraire différent à travers le

(32) Il est intéressant à cet égard de constater que le Groupe dit de l'article 29 de la Directive a adopté un document de travail intitulé «Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données», qui énonce une méthodologie d'évaluation du niveau adéquat du régime existant dans les pays tiers (*http://europa.eu.int/comm/dg* 15/fr/media/dataprot/wpdocs/index.htm).

(33) Nous tombons alors dans une des exceptions visées à l'article 26 de la directive (cfr. *infra*).

réseau pour arriver en entier chez le destinataire. Les pays destinataires dans le cadre du transfert des données sont donc imprévisibles, et une évaluation à priori de la protection offerte semble donc difficilement praticable. D'autre part, puisqu'il est possible d'accéder à un site Internet de partout à travers le monde, il semble difficile pour le responsable du site en question de limiter l'accès seulement aux pays offrant une protection adéquate. Quand bien même cela serait le cas, comment le responsable du site pourrait-il être sûr de la localisation physique certaine de la personne accédant au site ?

Quant aux flux passifs, à savoir les flux de données à caractère personnel qui sont effectués à l'insu de la personne concernée, nous distinguons l'hypothèse des cookies des autres traces électroniques laissées lors de la visite d'un site (34). A propos des cookies, puisqu'ils permettent une collection discrète de données à l'insu de la personne concernée, il nous semble difficile de qualifier la personne en question d'expéditeur des données ni même de parler d'un transfert de données. Il s'agit plutôt en effet d'une collecte de données, et puisque la personne responsable de la collecte est située en dehors de la Communauté européenne mais recourt à des moyens situés sur le territoire d'un Etat membre, c'est l'article 3*bis* plutôt que les articles 21 et 22 de la loi qui devrait s'appliquer (35).

Quant à la deuxième hypothèse des traces laissées lors de la visite d'un site à l'insu de la personne concernée, il ne peut s'agir d'un transfert de données à caractère personnel puisque la personne concernée n'effectue pas un flux conscient de données. L'article 3*bis* ne s'appliquera pas non plus étant donné que le responsable peut prétendre ne pas collecter les données en ayant recours à des moyens situés sur le territoire d'un Etat membre : il ne fait que collecter les données lors de la visite de la personne sur son propre site. La loi laisse donc la personne concernée sans protection quant aux traces qu'elle peut laisser. Elle doit être informée de ce danger.

(34) Voir *supra* : identification des données laissées lors de la visite d'un site.
(35) Voir *supra* : Champ d'application territoriale.



*Les exceptions*

L'article 22 de la loi prévoit des exceptions à la restriction des transferts de données vers des pays tiers n'offrant pas un niveau de protection adéquat. Les flux de données actifs au cours d'une transaction de commerce électronique tomberaient vraisemblablement dans le cadre des exceptions prévues.

En effet, le transfert peut avoir lieu si la personne concernée a indubitablement donné son consentement au transfert envisagé (36). Ce consentement doit être, rappelons-le, libre, spécifique et informé (37). Dans le contexte d'un transfert de données vers un pays tiers n'offrant pas un niveau de protection jugé adéquat, un consentement éclairé implique que la personne soit pleinement informée des risques que ce transfert présente en termes d'atteintes à sa vie privée. La nécessité d'un consentement spécifique dans le cadre d'une transaction électronique entraînant des flux de données, suppose non pas l'accord de la personne concernée à ce que les données soient traitées pour la transaction électronique mais un consentement spécifique au transfert en lui-même.

Le transfert peut également avoir lieu lorsqu'il est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou s'il est nécessaire aux mesures préalables à la conclusion de ce contrat prises à la demande de la personne concernée (38). Nous songeons, par exemple, à la commande de biens ou de services dans un pays tiers impliquant l'envoi de données nécessaires pour finaliser la commande : nom, adresse, numéro de carte de crédit ... Seules les données nécessaires à la transaction peuvent être transférées (voir principe de conformité *supra*). Une bonne information de la personne concernée (voir *infra*) implique qu'elle soit avertie qu'une fois que les données nécessaires au contrat sont envoyées vers le pays tiers, la personne concernée ne dispose plus de moyens pour en limiter l'usage pour d'autres finalités sans rapport aucun avec la finalité du transfert. Les données peuvent ainsi être revendues à des sociétés

(36) Article 22, § 1er, 1° de la loi.
(37) Voir *supra* : la définition du consentement.
(38) Article 22, § 1er, 2° de la loi.

de marketing, par exemple, afin d'élaborer des profils de consommation en fonction du type de biens commandés.

Enfin, les données peuvent être transférées vers des pays tiers lorsque le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers (39). Nous songeons, par exemple, à une réservation d'hôtel dans un pays tiers effectuée par une agence de voyage pour le compte d'un de ses clients.

Le deuxième paragraphe de l'article 22 de la loi prévoit également que le Roi peut, après avis de la Commission de la protection de la vie privée, autoriser un transfert ou un ensemble de transferts vers des pays n'offrant pas un niveau de protection adéquat, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée, notamment par le biais de garanties contractuelles.

### 5. – Droits de la personne concernée

#### *Le droit à l'information*

L'article 9 de la loi prévoit le devoir d'information de la personne concernée à charge du responsable du traitement. La loi prévoit deux instants d'information de la personne selon que les données ont été directement obtenues auprès de la personne concernée ou lorsque l'information est obtenue auprès d'un tiers.

Dans les deux cas, la personne doit être informée du nom et de l'adresse du responsable du traitement (ou de son représentant), des finalités du traitement et de la possibilité pour la personne concernée de s'opposer sur demande et gratuitement au traitement des données lorsque le traitement est envisagé à des fins de «direct marketing».

D'autres informations devront être données, sauf si ces informations supplémentaires ne sont pas nécessaires pour assurer un traitement loyal des données à l'égard de la personne concernée (40). Ces informations supplémentaires couvrent notamment les catégories de données concernées (lorsque les données n'ont pas été obtenues auprès de la personne concernée), les destinataires ou catégories de destinataires des données, l'existence d'un droit d'accès et de rectification des données concernant la personne et le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse (lorsque les données ont été obtenues auprès de la personne concernée).

(39) Article 22, § 1er, 3° de la loi



Ces informations supplémentaires suscitent certaines interrogations. En effet nous pouvons d'abord nous poser la question des circonstances dans lesquelles ces données doivent être fournies. Si nous reprenons les termes de la loi, elles ne doivent pas être fournies «sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données ont été obtenues, ces informations ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données» (41). A ce propos il nous semble que le terme de traitement loyal fait appel aux termes de l'article 4, § 1er, 1° de la loi et l'exigence de transparence du traitement à l'égard de la personne concernée. Si on replace cette exigence dans le contexte des transactions électroniques («compte tenu des circonstances particulières dans lesquelles les données ont été obtenues»); il nous semble qu'un maximum de transparence et donc d'informations devraient être données à la personne concernée.

Cela est d'autant plus vrai lorsqu'un transfert vers des pays tiers n'offrant pas un niveau de protection adéquat est envisagé. L'hypothèse spécifique d'envoyer des données à caractère personnel en dehors de la zone protégée par les lois nationales transposant la directive européenne 95/46/CE, requiert alors une bonne information du sujet des risques que cela implique. Le problème dans le contexte de réseau ouverts comme l'Internet est qu'il n'est pas toujours aisé de déterminer à l'avance si les données sortiront de la Communauté euro-

(40) Article 9, § 1er, d) et § 2, d) de la loi.

(41) Il est à noter que la directive utilisait une formulation inverse : les informations n'étant dues que dans la mesure où elle permet d'assurer un traitement loyal des données.

péenne ou pas (42). Dans un souci de transparence il serait peut-être préférable d'avertir la personne concernée de l'éventualité d'un transfert de ses données vers des pays tiers.

Un réseau tel qu'Internet se caractérise par les multiples acteurs qui interviennent dans la transmission d'une communication (fournisseurs d'accès, opérateurs de télécommunications, responsables de sites, ...). La question qui se pose dès lors est de savoir s'il faut les considérer comme des «destinataires» au sens de l'article 1er, § 7 de la loi et informer la personne concernée de leur identité ? En effet, la loi définit le destinataire comme étant « la personne physique, la personne morale, l'association de fait ou l'administration publique qui reçoit communication des données, qu'il s'agisse ou non d'un tiers». Puisqu'une simple réception de la communication et non une connaissance des données est requise par la loi, il nous semble qu'afin d'assurer un traitement loyal, la personne concernée devrait être informée de ces intervenants.

Quant à l'utilisation de cookies, il est recommandé d'en informer les internautes dans la mesure où il y a un manque de transparence non seulement quant à l'existence du cookies en lui-même mais également de l'exploitation des données collectées à partir des cookies.

L'interactivité du réseau facilite l'information de la personne concernée. En effet, dans le cas où les données à caractère personnel seraient directement obtenues auprès de la personne concernée, un message peut apparaître sur son écran au début des opérations, afin de fournir les informations essentielles. Quand les données ne sont pas obtenues directement auprès de la personne (lorsque, par exemple, les données sont collectées par une société de marketing afin d'établir des profils de consommation) la possibilité de les avertir électriquement est nettement moins coûteuse que par les voies traditionnelles.

La loi prévoit une exception à l'obligation d'information, lorsque, en particulier pour un traitement aux fins de statistiques ou de recherche historique ou scientifique (43) l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés. Nous pouvons imaginer ce cas lorsque les données sont collectées par le responsable du traitement à partir de bases de données sur le réseau et qu'il est impossible de retrouver la trace de la personne concernée elle-même afin de l'informer. Cela ne dispense toutefois pas le responsable du respect des autres dispositions de la loi.

(42) Voir *supra*, les transferts vers pays tiers.

(43) «Ou pour le dépistage motivé par la protection et la promotion de la santé». Voir article 9, § 2, alinéa 2 de la loi.



*Les droits d'accès* (44) et de rectification

Le droit d'accès est le droit pour la personne concernée d'obtenir du responsable du traitement (45), la confirmation de l'existence du traitement portant sur des données la concernant, ainsi que des informations sur les finalités du traitement, les catégories de données traitées et les destinataires, la communication des données traitées et la connaissance de la logique suivie lors d'un traitement automatisé de données. La personne concernée peut également être avertie des différentes possibilités ouvertes à elle pour donner suite à cet accès (demande de rectification, consultation du registre public, ...) et être informée de toute information «disponible» sur l'origine des données. A ce propos, dans le contexte de la communication de données par le réseau, l'information sur l'origine des données n'est justement pas toujours disponible.

Le droit de rectifier des données incomplètes, incorrectes ou non pertinentes est accordé à la personne concernée. Le responsable du traitement doit communiquer cette rectification dans le mois qui suit la demande tant à la personne concernée qu'aux tiers auxquels les données ont été communiquées. Toutefois les tiers ne reçoivent cette communication que pour autant que le responsable «ait encore connaissance des destinataires de la communication et que la notification à ces destinataires ne paraisse pas impossible ou n'implique pas des efforts disproportionnés» (46). Dans le contexte de transactions électroniques il est évident que la connaissance des destinataires de la communication est plus difficile que dans l'hy-

(44) Nous n'envisagerons pas le régime spécifique des données à caractère personnel relatives à la santé.

(45) Ou de toute autre personne désignée par le Roi (article 10, § 1er, al. 2 de la loi).

(46) Article 12, 4° de la loi.

pothèse d'une transaction classique où le responsable du traitement a en principe lui-même consciemment communiqué les données. En effet, le captage des données sur le réseau par des tiers peut se faire à l'insu du responsable du traitement. Toutefois, dans l'hypothèse où le responsable connaît l'identité des destinataires, les caractéristiques mêmes du réseau facilitent la notification des rectifications.

### *Le droit d'opposition*

La personne concernée a le droit de s'opposer pour des raisons légitimes et tenant à sa situation particulière à ce que des données la concernant fassent l'objet d'un traitement sauf lorsque le traitement est nécessaire à la conclusion ou à l'exécution d'un contrat ainsi qu'au respect d'une disposition légale (47).

Le droit d'opposition est accordé gratuitement et sans justification lorsque les données sont destinées à un traitement pour des finalités de «direct marketing» (48). Un droit d'opposition ne peut toutefois être effectif que si la personne concernée en est dûment informée et si elle dispose d'un moyen efficace de marquer son opposition. A cet égard, il faut rappeler l'obligation du responsable du traitement d'informer la personne concernée de son droit d'opposition soit lorsque les données sont collectées, soit avant que les données ne soient communiquées pour la première fois à des tiers pour des fins de direct marketing ou utilisées par un tiers à ces mêmes fins. Ainsi le droit d'opposition peut soit s'effectuer directement lorsque les données sont collectées à des fins de marketing, soit avant la communication ou la première utilisation à ces mêmes fins.

Quant à l'établissement d'un mécanisme d'opposition il est préférable que celui-ci soit centralisé et permet aux fournisseurs, avant même d'envoyer un message d'accéder aux listes reprenant les personnes qui ont marqué leur opposition à la réception de messages non sollicités. A cet égard, les entreprises belges de marketing direct on déjà créé une liste Robinson reprenant l'identité des personnes s'opposant à la réception d'offres individualisées (49). Toutefois ce mécanisme semble inadapté dans le contexte global d'Internet. L'idée anglaise de créer au sein même de l'adresse e-mail une indication du refus de recevoir des envois non sollicités est peut être à retenir, même si elle ne permet pas de moduler le refus en fonction de l'étendue de l'opposition : refus à toute communication commerciale, refus de communications en provenance de tel ou tel pays, ...

(47) Article 12, § 1er de la loi.

(48) Il est regrettable que la loi n'ait pas défini ce qu'elle entendait par «direct marketing». A ce propos le Registrar britannique a interprété les termes de «direct marketing» dans la législation transposant les directives 95/46/CE et 97/66/CE (The telecommunications (Data Protection and Privacy)(Direct Marketing) Regulations 1998) comme couvrant aussi bien les offres de biens et services mais également les promotions de partis politiques ou d'organisations de bienfaisance. Voir *http://www.open.gov.uk/dpr/telecom* 1.htm.



### *La non-soumission à des décisions individuelles automatisées*

L'article 12*bis* de la nouvelle loi interdit qu'une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative soit prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité. Selon l'exposé des motifs, cette disposition vise « des systèmes de décisions automatisées générant des scores et/ou autres résultats qui ont un impact direct sur la personne concernée, par exemple, pour ce qui concerne l'octroi ou non d'un crédit» (50). Elle vise à éviter que des décisions soient prises directement sur la base du résultat d'un traitement automatisé sans aucune intervention humaine. Dès lors, on ne tombe pas sous le coup de cette disposition lorsqu'il y a une intervention humaine minimale.

La loi prévoit deux exceptions à cette interdiction. La première vise les décisions prises dans le cadre d'un contrat. La deuxième permet les décisions automatisées fondées sur une disposition prévue dans une loi, un décret ou une ordonnance. Dans les deux cas, le contrat ou la disposition doivent contenir des mesures appropriées garantissant la sauvegarde des inté-

(49) Voir à cet égard le code de déontologie de l'Association belge du Marketing Direct.

(50) *Exposé des motifs*, p. 52.

rêts légitimes de la personne concernée et doivent lui permettre au moins de faire valoir utilement son point de vue. On peut s'interroger sur la portée de cette exception dans le contexte des transactions électroniques. Permet-elle des décisions d'octroi de crédits basés sur la création de profils de consommation (type d'achats effectués, rapidité de paiement, zone géographique d'habitation ...) ? Si tel est le cas comment la personne concernée pourrait-elle faire valoir utilement son point de vue ?

## 6. Recommandations (51)

Outre les dispositions légales belges, nous trouvons dans les recommandations européennes ou les législations étrangères des dispositions qui pourraient contribuer à assurer la protection des données à caractère personnel par les fournisseurs de biens et services sur Internet. En guise de conclusion, nous proposons, dès lors, d'examiner certaines de ces recommandations qui à nos yeux contribueraient, aux côtés de la loi belge examinée ci-dessus, à garantir une protection adéquate des données à caractère personnel des utilisateurs d'Internet.

### *L'anonymat*

La recommandation d'offrir l'anonymat aux utilisateurs de l'Internet ne s'adresse pas aux fournisseurs d'accès à Internet qui devraient, si le projet d'arrêté royal examiné auparavant (52) entre en vigueur, au moins être susceptibles de pouvoir identifier les appelants. Par contre la recommandation 3/97 du groupe de protection des personnes à l'égard du traitement des données à caractère personnel (53), préconise la possibilité d'effectuer le paiement d'achats sur Internet de manière anonyme et ce dans les limites compatibles avec d'autres considérations d'intérêt général, la plus importante étant la lutte contre le blanchiment des capitaux. A ce propos il faut signaler la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment des capitaux (54), qui oblige les établissements de crédit et les institutions financières (55), à obtenir l'identité de leurs clients lorsqu'ils nouent des relations d'affaires avec eux ainsi que pour toute opération supérieure ou égale à 10.000 euros. Elle oblige également ces mêmes personnes à conserver les documents relatifs aux transactions pendant une période d'au moins cinq ans.

En soi, cette loi n'est toutefois pas incompatible avec l'anonymat des paiements sur Internet puisqu'elle porte principalement sur les transactions avec les banques et les autres établissements de crédit et institutions financières, alors que l'exigence d'anonymat existerait plutôt dans la relation entre particuliers et commerçants ne faisant pas partie du système financier. De plus, les transactions portant sur des petits montants ne devraient pas poser de problèmes à cet égard.

### *Minimalisation*

A défaut d'anonymat, il est recommandé qu'à chaque étape de l'opération de commerce électronique ne pourront, à défaut de consentement express de l'utilisateur, être collectées et traitées que les données nécessaires à la transaction. Il s'agit ici de l'application du principe de proportionnalité. Ainsi, les fournisseurs doivent configurer leurs systèmes ainsi que les programmes qu'ils livrent aux utilisateurs de manière à ce que la collecte des données soit limitée aux seules données nécessaires à l'utilisation du service (56).

(51) Ces recommandations sont le résultat du travail effectué par A. Salaun, Y. Poullet et S. Louveaux dans « Recommendations on user protection », dans le cadre d'Eclip (*Electronic Commerce Legal Issues Platform*) : *http://www.jura.uni-muenster.de/eclip*.

(52) Projet d'arrêté royal portant application de l'article 109*ter* E, § 2 de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, voir *supra*, section consacrée aux « données à caractère personnel ».

(53) Adoptée le 3 décembre 1997 et intitulé « L'anonymat sur Internet ». La loi allemande « Informations - und Kommunikationsdienste - Gesetz - IuKDG » du 1.08.1997 (publiée au Bundesgesetzblatt du 28 juillet 1997) préconise également l'utilisation ou le paiement anonyme sur Internet.

(54) *Moniteur belge*, 9 février 1993, pp. 205 à 253.

(55) Ainsi que les notaires, huissiers de justice, experts comptables, réviseurs d'entreprises et personnes exploitant un ou plusieurs jeux casinos.

(56) Il s'agit d'une recommandation du Groupe de protection des données Recommandation 1/99 adoptée le 23 février 1999.

*Réciprocité des Avantages*

Puisque le fournisseur se sert des avantages de l'Internet pour collecter plus facilement des données sur la personne concernée, le principe de la réciprocité des avantages implique que le fournisseur permette à la personne concernée de profiter également des avantages de ce médium. Cela implique non seulement que la personne concernée doit pouvoir exercer ses droits d'accès et de recours directement par le biais d'Internet, mais aussi qu'elle puisse accéder, par exemple, à l'information relative à la politique suivie par le responsable en matière de protection des données et ce de manière aisée. Ainsi, nous pouvons imaginer qu'en cliquant sur un sigle nous accédons directement à son «privacy statement» (57) ou aux F.A.Q.s correspondant à la question ou, dans le cas d'une labellisation du site, un hyperlien doit pouvoir être ouvert par l'internaute vers le site qui a procédé à l'audit.

*Déclaration de protection des données à caractère personnel (Privacy Statement)*

Même si la législation belge actuelle ne rend aucunement obligatoire cette déclaration, il est recommandé d'informer les visiteurs d'un site des pratiques du site en matière de protection des données. Cela permet de montrer que le responsable du site se préoccupe du respect des données à caractère personnel, élément non négligeable afin d'obtenir la confiance des utilisateurs. Ainsi sur la première page du site devrait figurer un sigle permettant d'accéder à la déclaration du site visité et toutes les pages qui collectent des données à caractère personnel devraient avoir un lien avec la dite déclaration (58).

Une telle déclaration devrait contenir au moins les informations suivantes :

- Qui collecte des données à caractère personnel;
- Quelles données sont collectées;
- Pour quelles finalités les données sont-elles collectées;
- Quels sont les droits de la personne concernée;

(57) Voir infra.

(58) Cette idée a notamment été émise dans l'avis de la Commission de Protection de la Vie Privée sur le projet d'arrêté royal n° 18 relatif à la déclaration.



- Pendant combien de temps les données vont-elles être conservées;
- A qui les données peuvent-elles être communiquées;
- Comment s'opposer à des publicités par e-mail;
- Quelles mesures de sécurité sont mises en place;
- Est-ce que l'on peut rester anonyme en visitant simplement le site;
- Quelle est la politique adoptée quant aux cookies.