L'ASBL

http://www.droit-technologie.org

présente :

E-MARKETING ET PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Thierry LEONARD
Avocat au Barreau de Bruxelles
Assistant à la Faculté de Droit de Namur
Thierry.LEONARD@Stibbe.be

23/05/2000

QUELQUES CONSIDÉRATIONS SUR LA LICÉITÉ DES PRATIQUES NOUVELLES DE MARKETING SUR INTERNET[1]

§ 1. - Introduction

1. E-commerce et Marketing : une union "sacrée" - Quel directeur du marketing aurait pu imaginer, il y a dix ans à peine, pouvoir disposer pour chacun de ses clients actuels, voire potentiels, d'un profil de consommation généré non seulement par les informations issues de des contacts antérieurs avec son entreprise mais par l'enregistrement d'informations provenant des relations commerciales ou sociales tissées par chacun de ses (futurs) clients avec autrui ? Savoir ce qu'il mange, ce qu'il boit, les quantités consommées, ses marques préférées, la date, l'heure et le lieu de ses achats, les magasins dans lesquels il entre -ceux qu'il aime et qu'il déteste-, la durée de ses visites, le temps qu'il consacre à chaque type d'achats, ses lectures préférées, ses goûts musicaux, où et quant il voyage, sa profession, la structure de son ménage, le montant de ses revenus, ses moyens de paiement préférés, ses hobbies, ses coûts de gueule etc. Bref, savoir qui est exactement son client et ce qu'il attend de son partenaire commercial. Aucun, sans doute.

Avec internet et l'e-commerce, ce "rêve" devient "réalité". Sur internet, tout acte posé par l'internaute, et donc par le client potentiel, laisse une trace qu'il est loisible de récolter. Envoyer un e-mail, faire une recherche sur un moteur particulier, être présent et s'exprimer sur un forum de discussion, accéder à un site quelconque, enregistrer telle ou telle information, réagir ou non à un stimuli informationnel, bref tout mouvement, tout acte de navigation sur le net génère une information correspondante dans la mémoire électronique de l'un ou l'autre des acteurs présents sur la toile, que ces derniers soit directement ou non en contact avec l'internaute. Reste seulement à récupérer ces informations, à les rapprocher afin de les analyser pour les utiliser au mieux, voire pour les vendre au plus offrant.

L'e-commerce lui-même offre également une nouvelle occasion de collecter des données à caractère personnel auprès du client-Internaute. La collecte de données on-line peut s'introduire harmonieusement dans la procédure d'achat des biens et services. Sous le couvert de l'identification nécessaire à la mise à disposition du bien ou service proposé, il est aisé de collecter, au même moment, toutes sortes d'informations qui permettront de servir de base à l'élaboration du profil de consommation du client. Ces informations seront ensuite couplées à celles relatives aux achats eux-mêmes et aux traces laissées par l'internaute lors de ses visites. Ce profil pourra du reste encore être étoffé par l'achat de données auprès de sources externes.

[1] Tous les remerciements de l'auteur vont à Jean-Marc Dinant -informaticien et chercheur au C.R.I.D.- pour sa relecture et ses précieux conseils.

2. Plan de l'exposé - Tant le présent texte que l'exposé qu'il sous-tend sont fortement limités pour des raisons bien légitimes tenant à l'organisation du présent colloque. Les réflexions qui suivent ne tendent pas à l'exhaustivité. Les remous suscités par les nouvelles techniques de marketing sur internet et la compatibilité de ces dernières aux législations protectrices des données justifieraient à eux seuls l'organisation d'un colloque.

On se contentera de donner ici un aperçu du nouveau contexte des traitements de données en vue de la réalisation de finalités de cyber-marketing (2). On se limitera ensuite à confronter celles-ci au principe de légitimité des finalités et de licéité des traitements tels que prévus par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnels (3)[2] [3].

§ 2. - Le nouveau contexte DES TRAITEMENTS DE CYBER-MARKETING sur Internet

3. Les nouvelles techniques de collecte de données à caractère personnel sur l'internet - Les traces nécessairement laissées par l'internaute sur internet et la volonté des acteurs de récupérer celles-ci ont donné lieu au développement de collectes nouvelles sans équivalent dans le monde réelle. On ne retiendra ici que les techniques les plus courantes sans avoir la prétention de l'exhaustivité[4].

Les données issues de l'utilisation des protocoles de communication : La communication entre ordinateurs sur internet n'est possible que grâce à

[2] Nombreuses sont donc les questions qui ne seront pas abordées ici : les difficultés liées tant au champ d'application matériel -quand les informations récoltées sur internet doivent-elles être considérées comme des données à caractère personnel- que territorial, le principe de conformité des finalités -peut-on "récupérer" des données collectée initialement pour une finalité excluant le marketing ? , le principe de conformité des données -toutes les données peuvent-elles être traitées en vue d'une finalité de marketing ?-, etc. Voy. notamment sur certains de ces points, M.-H. BOULANGER, C. DE TERWANGNE, "Internet et le respect de la vie privée", in *Internet face au droit*, Cahier du C.R.I.D. n°12, Namur, C.R.I.D.-Story scientia, 1997, p. 189 à 213; J. -M. DINANT, "Law and Technology Convergence in the Data Protection Field ? Electronic threats on personal data and electronic data protection on the Internet", disponible à l'adresse http://www.droit.fundp.ac.be/Textes/privacy_law_tech_convergence.rtf; Y. POULLET, C. DE TERWANGNE, P. TURNER (eds), *Vie privée : nouveaux risques et enjeux*, Cahier du C.R.I.D. n°13, Namur, C.R.I.D.-Story scientia, 1997.

[3] La loi du 8 décembre 1992 a été modifiée par la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995. Ce dernier texte n'est cependant pas encore entré en vigueur à défaut d'arrêté royal d'exécution. Ci-après, on tentera de tenir compte des nouvelles dispositions. Toute référence à la loi du 8 décembre 1992 telle qu'en vigueur actuellement se fera par la mention "la Loi actuelle". Toute référence au nouveau texte se fera par la mention "la nouvelle Loi".

[4] Pour des explications plus précises, voy. notamment : .C.N.I.L., *17ème rapport d'activité 1996*, Paris, La Documentation française, 1997, p. 61 et s.; CONSEIL d'ETAT (fr), *Internet et les réseaux numériques - Etude adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998*, Documentation française, Paris, 1998,
p. 32 et s.; J. M. DINANT, *Les traitements invisibles sur l'Internet*, http://www.droit.fundp.ac.be/crid/eclip/luxembourg.html; "Law and Technology Convergence in the Data Protection Field ? Electronic threats on personal data and electronic data protection on the Internet", *op. cit.*

l'utilisation de protocoles standardisés. Le protocole TCP/IP permettra le transport des paquets d'informations sur le web et leur unification chez le destinataire en identifiant -par l'adresse IP[5] chacune des machines intervenantes. Les informations stockées sur les pages web sont codées grâce au langage HTML[6] et transmises à l'aide du protocole HTTP[7]. L'utilisation de ces protocoles implique la transmission de diverses informations, dont certaines sont nécessaires à la navigation et d'autres non, lors de tout mouvement sur le net : adresse IP, marque du navigateur en ce compris la version du logiciel utilisé et la langue utilisée par le programme, type d'utilisation (accès au web, messagerie etc.), date et heure de la connexion, la requête éventuelle (page que l'utilisateur va visiter), page sur laquelle est mise en oeuvre un hyperlien invisible etc. Ces informations sont susceptibles d'être enregistrées en tout ou partie par les fournisseurs d'accès, par le programme de navigation et par les serveurs auxquels l'internaute se connecte.

Les cookies : Les cookies fascinent et ont déjà fait couler beaucoup d'encre. Ils ont déjà une légende[8]. Le cookie est un paquet de données transmis par le serveur visité au logiciel de navigation qui le fixe sur le disque dur de l'ordinateur de l'internaute. Identifié par le nom de domaine auquel appartient l'ordinateur envoyant le cookie, il sera dorénavant uniquement accessible par le serveur qui en est à la source. Codé, il est inintelligible pour l'internaute. Sa durée de vie est variable selon la volonté du serveur source : quelques minutes (le temps d'une connexion) ou plusieurs années. Le serveur qui en est à la source peut le charger d'informations, le modifier, changer sa date d'expiration ou renvoyer des cookies supplémentaires (les logiciels de navigation peuvent en contenir plusieurs centaines!). Il peut également le supprimer. On l'aura compris, cette technique n'a été rendue possible que par la collaboration des producteurs de logiciels de navigation

[5] L'adresse IP est l'adresse de la machine d'un utilisateur connecté à l'internet. Elle peut être dynamique ou statique.

[6] Le HTML est le langage de codage d'un document hypertexte sur Internet.

[7] Le HTTP permet la transmission des documents décrits en HTML.

[8] L'explication qui suit provient d'un extrait traduit de C. BAYERS, "The promise of one-to-one, a love story", *Wired*, May 1998 in *Commerce Electronique, Marketing et Libertés*, Cahier Laser n°2, Paris, Ed. 00h00, 2000, p. 62 et s. disponible en ligne et gratuitement sur le site http://www.00h00.com. Les techniciens du web auraient été confrontés à une difficulté en travaillant sur une application d'achat en ligne. Le serveur auquel se connecte un internaute ne pouvait pas identifier l'auteur des diverses requêtes qui lui étaient transmises lors d'une visite par un internaute. En effet, l'adresse IP étant très souvent dynamique, le serveur ne pouvait pas unifier entre elles les très nombreuses requêtes reçues . Demander aux internautes de s'identifier à chaque connexion était une solution impraticable (oubli des mots de passe, demandes d'identification répétées constamment etc.). Dans ces circonstances, créer un panier à provision qui resterait lié au navigateur d'un utilisateur particulier afin de lui permettre de le remplir au fur et à mesure de sa visite pour ensuite effectuer un paiement unique pour tous ses achats paraissait impossible en l'absence d'identifiant unique. Le cookie fut alors créé comme identifiant unique de l'internaute.

qui ont programmé ces derniers afin de recevoir et de gérer la technique du cookie[9].

Autour de cette réalité technologique se sont greffés de multiples outils permettant de traiter l'information récoltée et rendue identifiable. Un profilage extrêmement fin devient possible par le rassemblement des multiples informations laissées par l'internaute sur sa route[10]. C'est un peu comme s'il se promenait avec, constamment, une caméra dirigée sur lui et un micro permettant de le rendre transparent pour l'observateur. On en arrive dès lors à pouvoir transmettre des informations différenciées à chaque internaute demandant une connexion à un serveur : les pages web deviennent personnalisées en fonction des informations déjà connues sur l'internaute qui demande la connexion. En outre, les publicités apparentes sur les "banners" vont différer selon le profil de consommation de chacun.

4. L'émergence de nouveaux acteurs dans le marché des données à caractère personnel - Dans le monde réel, le prestataire commercial utilise principalement les informations sur sa clientèle afin de conclure et d'exécuter les contrats qui le lient à elle. Il traite également ces données afin d'offrir à cette dernière d'autres produits ou services qui émanent tant de lui que d'entreprises liées. Le prestataire e-commerce, quant à lui, sera de plus en plus enclin à effectuer un pas supplémentaire en devenant un fournisseur de données à caractère personnel dans un marché de plus en plus juteux.

Rentabiliser la masse d'informations collectées sur internet en la commercialisant à des tiers peut s'avérer extrêmement tentant. C'est d'autant plus vrai que l'outil utilisé permet à la société d'e-commerce de récolter à frais réduits[11] des données sans grand rapport avec ses propres produits et

[9] C'est pourquoi le groupe 29 a adressé, par la voie d'une recommandation, une mise en garde aux producteurs de logiciels de navigation et de hardware : Recommendation 1/99 on invisible and automatic processing of personal data ont the internet performed by software and hardware (WP17), disponible à l'adresse http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs. Le groupe 29 a été institué par l'article 29 de la directive 95/46/CE 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 des données. Même s'il est dénué de pouvoir décisionnel, les effets de ses avis et recommandations prendront une importance croissante. Composé de membres des Commissions nationales de protection des données, mais aussi de représentants de la Commission européenne et de ses organes de contrôle, il exprime l'opinion communément partagée par les Commissions de protection des données en Europe. Ces dernières y trouveront une source officielle pouvant permettre de justifier et fonder leurs décisions quant aux problèmes préalablement analysés au sein du groupe 29.

[10] Rares sont les sociétés qui admettent officiellement l'unification des données récoltées tant par formulaire que par des moyens techniques comme les cookies. Dans une récente étude commandée par l'OCDE, sur une cinquantaine de sociétés, seules trois d'entre elles reconnaissaient coupler les données récoltées directement auprès de l'internaute avec ses données de navigation. Plus de trente d'entre elles utilisaient cependant des cookies. (*Pratiques relatives à la mise en oeuvre sur les réseaux mondiaux des lignes directrices de l'O.C.D.E. sur la vie privée*, document DSTI/ICCP/REG(98)6/FINAL disponible à l'adresse http://www.ocde.org/dsti/sti/it/secur/act/privnote.htm).

[11] Les données sont en effet saisies par l'internaute lui-même en version numérique. On "gagne" la fastidieuse étape de saisie des informations sur supports papiers vers un support numérique.

services. La tentation est d'autant plus forte que l'on se situe encore en la matière dans une étape de recherche de rentabilité et de prises d'occupation du marché, sans possibilité réelle de retirer rapidement de substantiels bénéfices. La vente de données à caractère personnel apparaît dès lors comme une source de financement propre inespérée. Tout fournisseur de services ou produits sur le web est donc potentiellement un revendeur de données à caractère personnel.

D'autres acteurs importants du web sont susceptibles de devenir -ou sont déjà - de grands collecteurs, voire des fournisseurs de données à caractère personnel. On pense principalement aux fournisseurs d'accès et aux moteurs de recherche[12]. Les premiers, en tant qu'intermédiaires obligés entre l'internaute et les fournisseurs de contenu présents sur internet, occupent une place privilégiée dans la connaissance des abonnés et de leur comportement sur le réseau. Les seconds drainent un très important trafic -l'étendue et la complexité de l'internet attire irrésistiblement les surfeurs vers ces acteurs- et sont théoriquement capables, par une analyse des requêtes formulées par les internautes et des contenus des sites répertoriés dans leurs index, d'en dresser des profils d'une richesse et d'un raffinement sans précédent. Un simple exemple laisse rêveur. Certains moteurs de recherches permettent des requêtes sur la base du nom patronymique : tous les sites où la personne est mentionnée s'affichent en un simple click[13]. En outre, par le biais d'offres de services connexes, comme les espaces de discussion et autres "chats", jeux, tests, sondages etc., ces deux acteurs peuvent enrichir d'autant leurs banques de données comportementales. Autant d'acteurs dont les pratiques réelles en matière d'utilisation des données à caractère personnel apparaissent comme ambiguës, voire tout simplement inconnues parce que, très souvent, non transparentes.

La même évolution pourrait apparaître par la mise en oeuvre des grands sites "*portails*" et autres "*vortails*". Accès uniques à de multitudes de services et de contacts avec des prestataires de services tiers, ils sont appelés, par la place centrale qu'ils occupent dans l'accès de l'internaute vers les informations ou les prestataires recherchées, à devenir de grands récolteurs -et donc vendeurs- de données. D'autres acteurs, tels que les

---

[12] Voy. sur ce point l'intéressante étude ARETE effectuée pour la Commission Européenne : S. GAUTHRONET, F. NATHAN, *Les services en ligne et la protection des données et de la vie privée*, décembre 1998, disponible à l'adresse http://europa.eu.int/comm/dg15/en/media/dataprot/studies/servint.htm spéc. p. 42 et suivantes où les auteurs passent en revue les contrats de quatre grands fournisseurs d'accès (Compuserve, AOL, Microsoft et Prodigy); aussi p. 33 et s. concernant les moteurs de recherche.

[13] *Idem*, p. 71 : les auteurs donnent l'exemple de cet américain pris comme cobaye dans une campagne destinée à dénoncer l'illusion de l'anonymat sur internet. Après avoir exploité, par le biais de moteurs de recherche, le contenu de tous les groupes de discussion auquel cette personne avait pris part, le Minneapolis Star Tribune pouvait ainsi avancer le profil suivant : lieu de naissance, université fréquentée, anciens et actuel employeurs, pratique du théâtre dans telle ville, marque de sa bière préférée, aimant la bonne chère et le Mac Intosh etc. Quelque temps après la publication de l'article, la personne déménageait : sa nouvelle adresse s'est retrouvée en moins de quinze jours dans un annuaire électronique.

agents intelligents, les fournisseurs de webcasting ou les fournisseurs d'annuaires, sont susceptibles de devenir de plus en plus actifs sur le marché des données à caractère personnel[14].

Une autre évolution se marque de plus en plus depuis un an. La collecte des données se transforme en une condition d'accès au service, voire au site connecté. Elle représente la contrepartie même de la gratuité de cet accès ou de l'offre d'informations. Certains y voient le signe avant coureur d'une modification de la nature même des services offerts par les fournisseurs d'accès : de transporteur à exploitant de données à caractère personnel[15].

5. Du marketing de masse au marketing "one-to-one" - Cette évolution technologique trouve son pendant dans les nouvelles théories du Cyber-marketing, dont la plus connue est le "marketing one-to-one"[16]. Réaction contre le phénomène de consommation de masse de ces cinquante dernières années -tout produit est une marchandise substituable, tout client est substituable- , le marketing "one-to-one" prône la débanalisation de l'échange commercial et la restauration de la spontanéité des échanges entre le vendeur et son client. Comment ? En s'appuyant "*sur la panoplie complète des avancées des technologies de l'information et de la communication et sur l'interactivité qu'elles autorisent*"[17].

M. Barchechath énonce les trois concepts-clé de cette théorie :

"*-La différenciation un par un des clients, sur la base de leurs besoins différents, permet de construire une offre sur l'équation personnelle du client, dans son rapport aux produits et aux services, et de mettre à sa disposition des produits et des services ajustés à ses attentes.*

-La création de barrière à l'entrée permet de s'abriter des concurrences trop vives et par là même de lutter efficacement contre la désertion des clients. Faire investir le client dans l'entreprise en temps et en effort pour spécifier ses besoins, c'est l'attacher à l'entreprise.

[14] *Idem*, p. 35 et s.

[15] E. BARCHECHATH, "Protection des données personnelles et respect de la vie privée à l'heure d'Internet et du commerce électronique - Un entretien avec Serge Gauthronet" in *Commerce Electronique, Marketing et Libertés, op. cit.*, p. 51.

[16] La présente explication est reprise principalement de l'exposé de E. BARCHECHATH, "Une lecture critique du One-to-One", in *Commerce Electronique, Marketing et Libertés, op. cit.*, p. 89 à 104; pour plus d'informations sur cette théorie, consultez les sites web qui lui sont consacrés, notamment le site de leurs "gourous", Don Peppers et M. Rogers : http://www.1to1.com.

[17] *Idem*, p. 92.

-La différenciation des clients sur la base de leur valeur pour l'entreprise permet de structurer son portefeuille client sur le critère de la rentabilité de chaque client."[18]**.**

Plus qu'en terme d'"*augmentation des parts du marché*", c'est en terme de "*part du client*" qu'il convient de penser. Il faut tenter de découvrir la valeur réelle de chacun de ses clients et de l'optimaliser au mieux dans la construction d'une relation durable. Bien évidemment, dans cette optique, le "one-to-one" ne vise qu'à garder les clients les plus profitables. Le succès ne dépendra pas tellement du produit ou du service qui est a priori offert : c'est l'information que l'on détient sur le client qui constitue la clé de la réussite. C'est elle et elle seule qui permettra tant d'en jauger la valeur que d'ajuster toujours mieux le produit ou le service à sa demande[19].

De ce point de vue, les bases de données qui permettent d'enregistrer et de conserver la totalité des informations concernant un client constituent l'outil essentiel pour aller vers "*le sur mesure de masse, à la fois premier pas, passage obligé et part intégrante du One-to-One*"[20]**.**

Malheureusement, en pratique : "*capture des informations, traitement et exploitation conduisent à la création d'un profil de l'utilisateur, le plus souvent à son insu, en dehors de lui, sans que jamais sa participation intentionnelle ou son accord ne soient requis. On veut ainsi le bonheur du client malgré lui*"[21]**.** Les tenants de cette théorie sont cependant conscients des problèmes liés à la confidentialité des données. C'est pourquoi ils prônent de plus en plus une transparence dans le traitement des données à caractère personnel[22]. Cependant, cette transparence n'implique pas une remise en cause de la légitimité même des techniques de collecte et de traitement des données. En effet, pour eux, le "one-to-one" est par principe respectueux du client puisque son but est de se mettre à son service.

6. L'amorce d'une prise de conscience quant aux risques générés par une recherche effrénée de l'identification : le cas de Doubleclick - Ces derniers mois diverses "affaires" ont défrayé la chronique outre-Atlantique provoquant une crainte bien légitime chez les défenseurs des libertés individuelles. Elles révèlent toutes des risques de dérapage issus de la mise

[18] *Idem*, p. 93.

[19] *Idem*, p. 94.

[20] *Idem*, p. 98.

[21] *Idem*, p. 99.

[22] *Idem*, p. 101 et s. ; voy. également, D. PEPPERS, "Respecting the value of privacy", article disponible à l'adresse http://www.1to1.com/articles/il-020499/index.html; M. ROGERS, "Wanted : privacy officers", article disponible à l'adresse http://www.1to1.com/articles/il-120999/index.html.

en place de procédés permettant le "traçage" des internautes[23]. Elles mettent toutes en cause certains logiciels utilisés par les internautes.

L'affaire DoubleClick retient particulièrement l'attention. DoubleClick est une des plus grosses agences de commercialisation d'espaces publicitaires (Rep-Agency) sur internet[24]. Sur ce média, la publicité prend le plus souvent la forme d'un "*banner*", annonce d'un format standard qui s'affiche sur l'écran de l'internaute en même temps que le contenu provenant de la requête effectuée par son navigateur. Ces "*banners*" contiennent un hyperlien permettant à l'utilisateur qui clique sur ce dernier d'accéder directement au site web de l'annonceur ("click-through"). Le procédé présente une opportunité inégalée de développer des relations de marketing "one-to-one".

Les sites supports sur lesquels apparaissent les "banners" passent de plus en plus d'accords avec des sociétés du type de DoubleClick. Ces dernières offrent aux annonceurs une prestation intégrée en matière de campagne publicitaire : media planning, ciblage "one-to-one", contrôle, impact et reporting client[25]. La particularité du service provient du fait que le contenu des "banners" qui apparaissent sur le réseau de sites-supports liés à l'agence[26] est ciblé en fonction du profil individuel du visiteur du site[27]. Pour offrir ces services, DoubleClick utilise notamment les techniques des

[23] D'abord, la révélation de l'existence du Processor Serial Number (PSN) de chez Intel, ensuite, le numéro d'identification unique du Windows 1998 (Global Unique Identifier) et enfin le mouchard électronique implanté dans le lecteur audio RealjukeBox de la Société RealNetworks. Pour un résumé de ces trois affaires, voy. *Expertises*, Janvier 2000, p. 406. Pour une explication plus technique des deux premières affaires, J. -M. DINANT, "Law and Technology Convergence in the Data Protection Field ? Electronic threats on personal data and electronic data protection on the Internet", *op. cit.*, p. 2 et 3.

[24] Le marché mondial de la publicité sur Internet poursuit une croissance exponentielle. D'après les estimations on passerait d'un investissement global de 175 millions $US en 1996 à 8 milliards $ en 2002. En 1999, c'est près de 2,2 milliards $US qui auraient été dépensés en publicité sur le net. Il faut rappeler également que tant la taille de l'internet que le nombre d'internautes double tous les 6 mois depuis 1995 (102 à 153 millions d'utilisateurs au début 1999). (source: *Inside Internet*, Novembre 1999, p. 34).

[25] Doubleclick est capable de fournir à ses clients une analyse du comportement de l'utilisateur qui a effectué un click-through : à quelle cible il appartient, quelles sont les pages de l'annonceur qui paraissent les plus motivantes pour l'internaute, si les utilisateurs achètent suite au click-through, quelle est leur navigation sur le site et à quel endroit ils abandonnent la visite du site etc. (S. GAUTHRONET, F. NATHAN, *Les services en ligne et la protection des données et de la vie privée*, *op. cit.*, p. 90).

[26] Actuellement, près de 11. 500 sites seraient liés à Double-click (source : J. BERST, "Why We're losing the privacy war", 31 janvier 2000 article disponible à l'adresse http://www.zdnet.com/anchordesk/story/story_4400.html). On peut donc imaginer que plusieurs millions d'européens visitant ces sites sont déjà ciblés dans ses banques de données.

[27] 100 millions d'internautes seraient actuellement enregistrés et profilés (source : plainte de l'EPIC contre DoubleClick devant le FTC; disponible à l'adresse http://epic.org/privacy/internet/ftc/DCLK_complaint : pdf).

cookies et des hyperliens invisibles[28]. Durant plusieurs années, DoubleClick annonçait ne pas individualiser les internautes autrement que par un identifiant unique[29] : les informations collectées restaient donc, selon elle, "*anonymes*" puisqu'elle affirmait ne pas connaître le nom, l'adresse e-mail, le numéro de téléphone et l'adresse postale des internautes. Elle déclarait donc ne pas céder de listes nominatives de prospects à des tiers[30]**.** Durant le second semestre 1999, DoubleClick acquérait l'Abacus Direct Corp., société américaine de marketing direct spécialisée dans le profilage et l'analyse des informations sur les consommateurs américains. Le 31 décembre 1998, Abacus était en possession d'un banque de données comportementales portant sur 88 millions de personnes liées à de l'information sur 2 milliards d'achats... Ces personnes sont identifiées par leurs noms et adresses. DoubleClick modifiait alors le "Privacy Policy" accessible sur son site. Elle y annonçait que sa propre banque de données était unifiée à celle d'Abacus[31].

Diverses plaintes ont ou vont être déposées contre DoubleClick devant le Federal Trade of Commerce et devant la justice américaine[32]. Il est notamment reproché à DoubleClick d'avoir commis des pratiques déloyales en ayant annoncé que les informations qu'elle collectait étaient et resteraient toujours anonymes (Deceptive Trade Pratice), en ayant omis d'informer les

[28] Grâce à un hyperlien invisible vers son site, DoubleClick est prévenue de la requête d'un internaute identifié par un cookie. Elle transmet alors un "banner" ciblé. Pour une description exacte de la technique utilisée par DoubleClick, voy. J.- M. DINANT, *Les traitements invisibles sur l'Internet*, *op. cit.*, n°5.

[29] A cet identifiant étaient liés l'adresse IP, le Domaine, le pays, l'Etat, le code postal, le titre et la fonction dans l'entreprise, la taille et le chiffre d'affaire, le type de browser utilisé, le système d'exploitation, le numéro de version, le fournisseur de service, et le référencement de la navigation du surfeur (collecte et analyse des sites visités, détermination des mots-clés contenus dans les pages affichées, heure des sessions et jour de la semaine où elles se déroulent) ((S. GAUTHRONET, F. NATHAN, *Les services en ligne et la protection des données et de la vie privée*, *op. cit.*, p. 92).

[30] *Idem*, p. 93; aussi la plainte d'EPIC, *op. cit.*

[31] On peut lire dans le Privacy Policy actuel (4 février 2000) : "*Name and adress information volunteered by a user on an Abacus Alliance Web site is associated by Abacus through the use of a match code and the DoubleClick cookie with other information about that individual. Information in the Abacus Online database includes he userrs name, address, retail, catalog and online purchase history, and demographic data. The database also includes the users non-personally-identifiable information collected by Web sites and other businesses with which DoubleClick does business. Unless specifically disclosed to the contrary in a Web site's privacy policy, most non-personally-identifiable information collected by DoubleClick from Web sites on the DoubleClick Network is included in the Abacus Online Database(...)*". Cette "Privacy Policy" est disponible à l'adresse suivante : http://www.doubleclick.com/privacy_policy.

[32] Voy. la plainte déposée par EPIC (*op. cit.*); aussi, divers articles parus dans la presse électronique, notamment F. LATRIVE, "Quand internet vous colle au clic. La régie publicitaire DoubleClick accusée de violer la vie privée", 16 février 2000, disponible à l'adresse http://www.liberation.com/multi/actu/20000214/20000216.html; K. MAGILL, "Update : CDT Blasts DoubleClick's profiling effort", 4 février 2000, disponible à l'adresse http://www.dmnews.com/articles/2000-01-31/6275.html; W. RODGER, "Activists charge DoubleClick double cross", 31 janvier 2000, disponible à l'adresse http://www.usatoday.com/life/cyber/tech/cth.htm; W. L. WATTS, "FTC probing Doubleclick data collection", 16 février 2000, disponible à l'adresse http://cbs..marketwatch.com/news/current/dclk.htx?source=htx/http2_mw.

internautes du placement des cookies et en n'ayant pas obtenu leur consentement pour ce faire (Unfair Trade Practice) et en violant la vie privée des consommateurs (Consumer Injury)[33].

§ 3. - le principe de LEGITIMITE en question : application auX finalites de marketing one-to-one

7. Les principes de légitimité et de licéité : rappel théorique - Toute finalité poursuivie par un traitement de données à caractère personnel doit être *légitime*. Tel est le principe qui résulte tant de l'article 5 de la Loi actuelle que des nouveaux articles 4 et 5.

La Loi actuelle ne donne pas de définition du caractère légitime d'une finalité. On s'accorde pour dire que la finalité du traitement et sa mise en œuvre doivent concilier les droits et libertés de la personne concernée par les données et l'intérêt général ou l'intérêt particulier poursuivi par le responsable du traitement[34]. L'analyse se fera alors en fonction des circonstances objectives de l'espèce.

Une précision supplémentaire est apportée par l'article 5 de la nouvelle Loi. Le traitement déterminé doit, pour être admis, se fonder nécessairement sur une des hypothèses visées par cette disposition[35] :

- la personne concernée a donné son consentement indubitable (art. 5 a);

- le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par responsable du traitement ou par les tiers à qui sont communiquées les données, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée (article 5 f).

Ces situations ne permettent cependant que de présumer l'équilibre des intérêts en présence, sous réserve d'un contrôle ultérieur fondé sur le respect du principe de légitimité présent à l'article 4 §1er, 2° de la nouvelle loi[36].

[33] Plainte d'EPIC, *op. cit.*

[34] Voy. notamment, S. GUTWIRTH, "De toepassing van het finaliteitbeginsel van de privacywet van 8 december 1992 tot de bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens", *T.P.R.*, 1993, pp. 1409 et s.; TH. LÉONARD, 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, p. 250 et s.; A. PIPERS, P. DE HERT, *Handboek Privacy - Persoonsgegevens in Belgie*, Brussel, Politeia, sept. 1999, p. 56 et s.

[35] On ne retient ici que les hypothèses potentiellement applicables aux finalités de marketing direct.

[36] Cette disposition énonce notamment de façon générale que les données à caractère personnel doivent être collectées pour des finalités légitimes; dans le même sens, R. FELTKAMP, M. FLAMÉE, "Telecommunicatie, privacy en bescherming van persoonsgegevens - Deel II. Bescherming van persoonlijke levensfeer t.o.v. de verwerking van persoonsgegevens bij de telecommunicatie", *A. & M.*, 1999, p. 325, spéc. note 72; Th. LEONARD, Y. POULLET, "La protection des données à caractère personnel

La licéité renvoie au respect de toute autre législation susceptible de s'appliquer au prestataire de service à l'occasion des traitements effectués dans le cadre d'internet. Il serait vain de passer en revue les multiples textes qui ont vocation à s'imposer aux prestataires de services sur internet qui font du e-commerce. On pense ainsi, par exemple, à certaines obligation de discrétion ou de confidentialité (secret professionnel, secret bancaire etc.), à la réglementation sur les pratiques du commerce, à certaines obligations qui seront prévues dans les lois particulières sur la preuve etc.

Vu les contraintes inhérentes à l'exposé que soutient le présent texte, seule certaines dispositions de la législation spécifique au secteur des télécommunications retiendra ici l'attention.

I. - La légitimité des finalités de marketing one-to-one sur internet

A. - Les conditions de la légitimité des finalités de marketing "one-to-one"

8. La légitimité de la finalité de marketing direct dans le monde réel - Bien avant le marketing one-to-one et son application sur internet, les pratiques de marketing direct ont été confrontées au principe de la légitimité des finalités. On peut définir le marketing direct comme "*l'ensemble des activités ainsi que tout service auxiliaire à celles-ci permettant d'offrir des produits et des services ou de transmettre tous autres messages publicitaires à des segments de population par le moyen du courrier, du téléphone ou d'autres moyens directs dans le but d'information ou afin de solliciter une réaction de la part de la personne concernée*"[37].

La légitimité de la finalité de promotion et de prospection commerciale a été affirmée par la jurisprudence. Il s'agissait d'affaires concernant le secteur bancaire[38] . De même, le Conseil de l'Europe a affirmé le principe d'admissibilité des finalités de marketing direct dès lors que le droit d'opposition était reconnu à la personne concernée[39].

---

en pleine (r)évolution", *J.T.*, 1999, p. 384 et 385, n° 27; A. PIPERS, P. DE HERT, *Handboek Privacy - Persoonsgegevens in Belgie*, Brussel, Politeia, sept. 1999, p. 65.

[37] Article 1.2. de la Recommandation n° R (85) 20 adoptée par le Comité des ministres du Conseil de l'Europe le 25 octobre 1985 et relative à la protection des données à caractère personnel utilisées à des fins de marketing direct (document disponible à l'adresse http://www.coe.fr/dataprotection/rec).

[38] Comm. Bruxelles (prés.), 15 sept. 1994 et Comm. Anvers, 7 juill. 1994, *Computerr.*, 1994, p. 244, note J. DUMORTIER ET F. ROBBEN, p. 247 à 250; *D.C.C.R.*, 1994, p. 77 et s. et note TH. LÉONARD; *D.I.T.*, 1994, p. 55 et note O. LESUISSE; *R.D.C.*, 1995, p. 297 et s. et note M. DASSESSE; *Jaarboek Handelspraktijk - 1994*, Diegem, Kluwer-Rechtswetenschappen, 1995, p.361 à 391 et note S. GUTWIRTH.

[39] Cfr art. 2 et 4 de la Recommandation n°R (85) 20 du 25 octobre 1985, *op. cit.*

La nouvelle Loi prévoit en son article 12 la reconnaissance d'un droit d'opposition en faveur de la personne concernée. Ce droit d'opposition a pour conséquence la disparition des personnes qui en font la demande des fichiers utilisés à des fins de marketing direct. L'exercice de ce droit est gratuit et n'implique aucune justification dans le chef de la personne concernée.

En général, l'intérêt commercial d'une entreprise est suffisant pour légitimer la collecte et le traitement de données non sensibles relatives à ses clients actuels ou potentiels en vu d'une finalité de marketing dès lors qu'un droit d'opposition est reconnu à la personne concernée. On peut assurément pour ce faire se fonder sur l'article 5, f précité de la nouvelle Loi.

9. Les traitements à finalité de marketing one-to-one : éléments de déséquilibre - Les traitements opérés sur internet, en vue de la réalisation de finalités de marketing, révèlent des circonstances objectives qui, à notre avis, sont susceptibles de rompre l'équilibre entre l'intérêt des responsables de traitement et ceux des internautes.

On peut tenter de systématiser ces éléments de déséquilibre comme suit :

1°. *La collecte est effectuée sur internet*.. Les possibilités nouvelles de collecte et de traitement issues de la technique de l'internet impliquent des risques accrus pour les droits et libertés. Les données qui seront potentiellement traitées visent souvent à tracer l'internaute dans ses moindres déplacements sur les sites visités. Ces techniques permettent d'être utilisées sans que l'internaute ait la possibilité de les identifier ou de les contrôler. La technique numérique permet de traiter ces informations pour soi ou pour des tiers dans une proportion jamais égalée auparavant. Les possibilités de communication des données entre acteurs du réseau sont fortement facilitées. Souvent, les transferts de données à caractère personnel sur l'internet ne sont pas sécurisés.

2°. *La multiplication des rôles remplis par un seul et même prestataire de service sur internet.* La recherche de synergies, tant économiques que techniques, expliquent que certains acteurs ont tendance à multiplier le type de services offerts. Le cas des moteurs de recherches transformés en "portails" est très significatif à cet égard (ex.: Yahoo, Infoseek, Altavista etc.)[40]. On peut penser également à la multiplication des services offerts par des fournisseurs d'accès qui s'allient avec des prestataires de services. La synergie attendue entre l'internet et les technologies sans fils, telle le WAP[41], en offre un autre exemple[42]. Ces synergies et la multiplication des

[40] Voy. par exemple, S. SALVAGGIO, M. BAUWENS, "Les portails européens en sursis ?", *Inside Internet*, Novembre 1999, p. 66; M. HÉDO, "Portails, qui va gagner ?", *Inside Internet*, Décembre 1999, p. 28.

[41] Le "*Wirless Application Protocol*" est un nouveau standard pour la fourniture d'informations et de services aux téléphones mobiles numériques. Cfr sur cette évolution "Le GSM et la communication de

services offerts permettent à ces sociétés d'augmenter leurs moyens de collecte d'informations à l'égard du même internaute. Le matching des différentes bases de données liées à chacun des services s'impose d'autant plus que le but avéré est souvent celui de fidéliser la clientèle au site, et donc de la profiler a priori au maximum.

3°. *Une centralisation d'informations collectées pour des finalités initialement différentes*. Un risque supplémentaire, lié au précédent, apparaît également de façon claire. Les réutilisations de données se multipliant, elles s'éloignent souvent du but initial justifiant directement la collecte. Les collectes d'adresses e-mail, de contenu des chats, de contenu des requêtes, de données de trafic etc. sont a priori effectuées pour des buts très éloignés du marketing one-to-one.

4°. La *communication de ces données à des tiers ou le traitement de celles-ci au profit de tiers* intervient comme quatrième source de déséquilibre. Toute communication de données à des tiers représente une source de perte potentielle de contrôle de la personne sur les données la concernant. Elle ne sait pas nécessairement -même dans le cadre de l'application de la loi- à qui ces données vont être communiquées et à quelles finalités elles vont servir. Le risque existe toujours que ce tiers ne respecte pas lui-même une législation sur la protection des données.

5°. *Les conditions de la collecte des données*. Si l'internaute refuse que ses données soient collectées, le prestataire de service peut lui interdire l'accès à son site. Une pression peut donc être opérée sur la personne afin d'obtenir les données. Le refus d'accès libre aux prestataires présents sur le web, fondé entièrement sur un refus de transmission de données, à l'exception de tout autre fondement objectif, peut également énerver la liberté d'anonymat sur internet, de plus en plus affirmée tant au niveau international que national[43].

10. Le consentement indubitable comme source principale de légitimité du marketing "one-to-one" - Au vu des éléments de déséquilibre identifiés ci-avant, le consentement de l'internaute paraît, a priori et in abstracto, la voie principale de légitimation des traitements à finalité de marketing sur internet. Le surcroît de risques pour les droits et libertés individuelles paraît qualitativement plus important que l'intérêt purement commercial poursuivi par les différents responsables de traitement intervenants dans les processus de profilage.

---

données", *Mobile Word*, décembre 1999, p. 10 et s.; L. GILLES, "Le Wap remporte tous les suffrages", *Inside Internet*, Décembre 1999, p. 78 et s.

[42] On imagine sans difficulté les applications de profilage qui pourraient résulter du rapprochement des données collectées par un opérateur de téléphonie mobile et d'une agence de cyber-marketing comme DubbleClick.

[43] Cfr *infra*, n°17.

Bien entendu, une pondération plus fine pourrait être effectuée au cas par cas et permettre, éventuellement, l'admission du traitement sur la base de l'article 5, f précité de la nouvelle Loi. Ainsi par exemple, lorsque le traitement est opéré sur la seule base d'une collecte via un formulaire à remplir par l'internaute[44].

L'obligation de passer par le consentement de la personne concernée en vue de la poursuite de finalités commerciales ou de marketing est confirmée par différents textes internationaux émanant de sources diverses, à tout le moins en ce qui concerne les données de trafic et les données sensibles.

Ainsi, la recommandation n° R(99)5 du Conseil de l'Europe[45] sur la protection de la vie privée sur internet prévoit à destination des fournisseurs de services internet énonce le principe suivant: "*N'utilisez des données aux fins de promouvoir ou de commercialiser vos propres services que si la personne, après avoir été informée, n'y a pas mis objection ou si, en cas de traitement de données de trafic ou de données sensibles, elle y a consenti explicitement*"[46].

Le consentement est également prôné, pour le traitement des données de trafic, par le groupe européen de protection des données - dit groupe 29- dans sa recommandation 3/97concernant l'anonymat sur internet : "*A moins que l'utilisateur ne veuille que cela soit possible, l'identification des traces n'est justifiée ni par l'ordre public, ni par l'intérêt général. La collecte des noms et adresses électroniques des visiteurs d'un site à vocation commerciale sera naturellement souvent précieuse pour son propriétaire qui utilisera ces données à des fins de marketing. Toute collecte des données sur des personnes navigant sur la Toile doit cependant se faire dans la transparence avec le consentement éclairé de l'internaute concerné. Les personnes souhaitant de manière anonyme naviguer sur le réseau des réseaux doivent être entièrement libres de pouvoir le faire*"[47]

B. - Les conditions du consentement comme source de la légitimité des finalités de marketing "one-to-one"

[44] Voy. par exemple, M. GEORGES ("Relevons les défis de la protection des données personnelles : l'Internet et la CNIL", in *Commerce Electronique, Marketing et Libertés, op. cit.*, p. 73) pour qui la légitimité de ces collectes en vue de finalité de marketing one-to-one"*ne fait pas de doute*". Nous pensons cependant qu'une analyse concrète de l'application du principe de légitimité est nécessaire dans chaque cas afin de déterminer si aucun élément de déséquilibre n'implique une légitimation plus forte que la simple application d'une pondération en faveur du prestataire de services.

[45] Celle-ci n'est pas une norme juridique obligatoire. Elle invite cependant les États Membres du Conseil de l'Europe, dont la Belgique, à diffuser largement les principes directeurs prônés concernant la conduite loyale à observer par les fournisseurs de services internet.

[46] Point III, 10, document disponible à l'adresse http://www.coe.fr/dataprotection/flignes.htm.

[47] P. 9; document disponible à l'adresse http://europa.eu.int/comm/dg15/fr/media/dataprot/wpdocs/index.htm.

11. Le consentement au sens de la Loi - La loi définit ce qu'il faut entendre par "*le consentement de la personne concernée*"[48]. Elle vise "*toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement."*

Toute manifestation de volonté peut constituer un consentement. Il ne doit donc pas être nécessairement donné par écrit pour être valable. Ce consentement peut être implicite, sauf exception prévue par la loi[49].

Qu'est ce qu'un consentement *libre, spécifique* et *informé*?

12. Le consentement doit être libre - Le consentement doit être donné en dehors de toute pression contraignant l'internaute à accepter le traitement. Le refus du traitement par l'internaute ne peut impliquer pour lui un risque de discrimination[50].

13. Le consentement doit être spécifique - Le consentement ne peut pas avoir un objet général mais doit porter sur des traitements précisément définis poursuivis par des responsables déterminés.

Afin d'assurer l'effectivité de cette condition sur l'internet, il est également nécessaire de distinguer les diverses finalités concernant les types de collecte qui seront effectuées. Si le prestataire offre par exemple un service de moteur de recherche, un service de e-mail et la possibilité d'effectuer des achats en lignes, l'internaute devra savoir, pour chaque type de collecte, les finalités d'utilisation auxquelles elles participent.

Ainsi par exemple, une information spécifique quant aux finalités d'utilisation de chaque cookie transmis devrait être transmise.

On retrouve l'élément de spécificité du consentement en matière de droit fondamental. Pas question d'admettre un blanc seing tant pour une utilisation en interne des données que pour la communication de données à des tiers sous le couvert d'une finalité générique de marketing "one-to-one". En outre, si ces données sont transmises à des tiers, il faut également distinguer pour quelles finalités les informations seront transmises.

[48] Article 1er §8 de la nouvelle loi.

[49] Th. LÉONARD ET Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution", *op. cit.*, p.379.

[50] *Idem*, p. 380, n°7.

14. Le consentement doit être informé - La personne concernée doit être informée avant qu'elle ne donne son consentement. L'information doit lui permettre d'analyser le risque de chacune des finalités de traitement envisagées. On renvoie ici aux obligations d'informations prévues par la Loi.

Dès lors que la collecte et les traitements ultérieurs s'effectuent dans le cadre de l'internet et que le consentement est requis pour légitimer les finalités, l'information à transmettre aux internautes doit s'appréhender de la manière la plus large qui soit. Elle comprend non seulement les éléments d'informations qui doivent nécessairement être transmis lors de toute collecte ou traitement de données transmises par des tiers[51] mais également toute information nécessaire pour assurer à l'égard de la personne concernée un traitement loyal des données au vu des techniques de traitement utilisées.

Ainsi, il dès lors nécessaire d'informer l'internaute sur les techniques de pistage utilisés (cookies, java script etc.), sur les matching qui seront opérés grâce à des données transmises par des tiers, sur l'identification automatique du visiteur en cas de transmission d'un e-mail, sur les possibilités d'opt-out qui existent sur le site ou chez le destinataire des données etc.

Le Conseil de l'Europe va encore plus loin et prévoit dans sa recommandation n° R(99)5 précitée que le fournisseur de service informe l'utilisateur de tous les risques liés à l'utilisation de l'internet : risques concernant l'intégrité des données, leur confidentialité, la sécurité du réseau, les collectes invisibles etc.

Il va de soi que cette extension de l'obligation d'information loyale sur internet impose l'utilisation d'un support spécifique qui s'éloigne très fort de la simple clause "vie privée" insérée sur les formulaires de collecte dans le monde réel. La technique de la "Privacy Policy", apparue depuis longtemps sur internet, répond adéquatement à cette réalité pour autant qu'elle soit suffisamment accessible à l'internaute. Si le consentement informé est requis, cette "Privacy Policy" devrait apparaître à l'écran de l'internaute avant l'obtention de son consentement.

C. - Application : la transmission de données à caractère personnel comme condition d'accès à un service sur internet

15. Problématique - Les pratiques contractuelles conditionnant l'accès gratuit à l'internet, à certains sites ou à certains services par la transmission de données à caractère personnel de l'internaute sont-elles licites au regard des principes développés ci-avant? La réponse à cette question n'est pas évidente. Elle implique, à tout le moins, une importante réticence[52].

[51] Cfr article 9§1er et 9 §2 de la nouvelle Loi.
[52] CONSEIL d'ETAT (fr), *Internet et les réseaux numériques - Etude adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998, op. cit.*, p. 34 et 35.

Elle se trouve au centre d'une problématique où s'opposent différentes libertés ou intérêts contradictoires : la liberté de la personne concernée qui implique une possibilité d'accepter un traitement considéré comme attentatoire à ses droits et libertés individuelles et donc de renoncer partiellement à ceux-ci, la liberté d'accéder anonymement aux informations présentes sur l'internet et la liberté contractuelle des parties -internautes et fournisseurs de services- qui impliquent le libre choix des conditions de toute transaction.

16. La licéité de la contractualisation de l'exploitation des données à caractère personnel - Le titulaire d'une liberté -fut-elle considérée comme fondamentale[53]- peut généralement renoncer à l'exercer en certaines circonstances. La question demeure cependant discutée concernant les droits fondamentaux protégés par la Convention européenne des droits de l'homme[54]. Il semble cependant indiscutable que la Loi elle-même, est venue couvrir les renonciations relatives à la protection des données à caractère personnel aux conditions qu'elle détermine. Si non, comment comprendre l'admission même du consentement comme source de légitimation de tout traitement ou des traitements portant sur les données sensibles ? Les conditions du consentement telles que exigées par la Loi sont du reste analogues à celles qui sont généralement admises aux renonciations aux libertés fondamentales[55].

On ne peut nier également que nos sociétés reconnaissent la validité de l'exploitation des biens de la personnalité : "*Dans une société qui forme un marché d'échanges généralisés il n'est guère de bien de la personnalité qui ne puisse, avec le consentement du sujet, se transformer en valeur patrimoniale. L'image, les souvenirs personnels, y compris les faits de la vie affective ou sexuelle, la pudeur, jusqu'à la qualité de victime d'un crime, d'un accident ou d'un cataclysme naturel, mais aussi la renommée que s'acquiert un criminel par ses forfaits, plus aucun bien n'est soustrait à une exploitation patrimoniale. (…) La conclusion d'un contrat ayant pour objet un bien de la personnalité a pour effet de conférer à chacune des deux parties le droit de créance afférent à la prestation de l'autre*"[56]. La condition

[53] Voy. par exemple, concernant la liberté de la vie privée, F. RIGAUX, *La protection de la vie privée et les autres biens de la personnalité*, Bruylant-L.G.D.J., Bxl-Paris, 1990, p.761., n°685.

[54] Pour un résumé clair et actualisé du débat, voy. S. VAN DROOGHENBROECK, obs. sous Cass. (1ère ch.), 14 mars 1991, in O. DESCHUTTER, S. VAN DROOGHENBROECK, *Droit international des droits de l'homme devant le juge national*, Bruxelles, Larcier, 1999, p. 130 et s. selon lesquelles on chercherait en vain actuellement une position claire issue de la jurisprudence de la Cour européenne des droits de l'homme.

[55] *Idem*, p. 136 et 137 : "*Pour se voir accorder quelque effet, cette renonciation doit être libre, éclairée et non équivoque. Enfin se dégageant implicitemnt, tant de la jurisprudence strasbourgeoise, que, semble-t-il, de la jurisprudence interne, l'exigence d'une certaine spécialité, ponctualité du consentement (...)*".

[56] F. RIGAUX, *La protection de la vie privée et les autres biens de la personnalité, op. cit.*, p. 763; aussi, notamment, dans le sens de la patrimonalisation du droit à la vie privée, la validité des contrats portant sur celle-ci ou l'admission de l'atteinte en cas de consentement : B. BEIGNIER, "La protection de la vie privée", *in Droits et libertés fondamentaux*, 4ème éd., Paris, Dalloz, 1997, p. 138, n°189; C. BIGOT,

du consentement implique normalement la naissance d'un contrat : "*Il [ndlr : le contrat] consiste en effet dans l'acceptation, par une personne, de la proposition d'une autre de s'immiscer dans sa vie privée ou de la divulguer, de réaliser ou de publier son image*"[57].

La liberté contractuelle implique que les parties fixent les conditions de leurs accord de volonté. La condition du consentement imposée par la Loi ne peut empêcher a priori la soumission de l'accès à l'internet, à un site ou à une information présente sur le web à certaines conditions contractuellement prévues entre parties. Les informations personnelles sont depuis longtemps un objet d'échange. Cet échange est permis -voire organisé- par la nouvelle Loi qui fait du consentement une condition de la légitimité du traitement. Rien n'interdit donc a priori d'intégrer le consentement visé par les lois sur la protection des données au processus d'échange de volontés qui fonde toute relation contractuelle dès lors que l'intégralité des autres dispositions de la Loi sont respectées.

17. Les limites à la validité des conventions portant sur l'exploitation des données à caractère personnel en vue de finalités de marketing "one-to-one" - De même que les contrats portant sur l'exploitation de la vie privée sont soumis à des limitations issues du caractère d'ordre public de la protection accordée à cette liberté[58], les contrats portant sur l'exploitation des données à caractère personnel n'ouvrent pas un champ illimité permettant de réduire à néant la protection légale qui leur est accordée.

Si la Loi actuelle permet qu'un traitement soit effectué moyennant le consentement de la personne concernée par les données, le responsable du traitement reste néanmoins soumis au respect de l'intégralité des dispositions légales. Outre que le consentement doit être libre, spécifique et informé, le respect de la loi implique qu'un équilibre subsiste entre les parties contractantes. Cet équilibre est plus spécifiquement assuré par le respect de la reconnaissance d'un droit d'opposition à la personne concernée et par le

"Protection des droits de la personnalité et liberté de l'information", *D.*, Chr., 1998, 235 et s., spéc. n°4; G. GOUBEAUX, *Traité de droit civil-Les personnes*, Paris, L.G.D.J., 1989, p.256, n°285; E. GULDIX, "De rechtsbescherming van de persoonlijke levensfeer door perssoonlijkheidsrechten", *Vl. T. Gez.*, 1986-1987, p.215, n°33; P. HUMBLET, "Het (Grond)recht op privacy : een blinde vlek in het arbeidsrecht", *Mensenrecht tussen retoriek en realiteit*, Gent, Mys & Breesch, S. Parmentier ed., Tegenspraak-cahier n°14, 1994, p. 210 et 211; B. OVERSTEYNS, "Het recht op eerbieding van het privé-leven", *R.W.*, 1988-1989, I, p. 496, n°25.

[57] P. KEYSER, *La protection de la vie privée par le droit - Protection du secret de la vie privée*, 3ème éd., Paris, Economica-Presses Universitaires d'Aix-Marseille, 1995, p. 236, n°136.

[58] Cfr *supra* note 54; *adde* P. KEYSER, *La protection de la vie privée par le droit - Protection du secret de la vie privée, op. cit.*, p. 238 et s., n°137. L'auteur indique notamment : "*Une personne ne peut consentir à la divulgation de sa vie privée que pour des événements déjà accomplis ou sur le point de s'accomplir. Elle ne peut l'autoriser pour des événements futurs et indéterminés, car elle renoncerait ainsi au droit au respect de sa vie privée, qui, étant un droit de la personnalité, n'est pas susceptible de renonciation. Elle ne peut de même consentir qu'une investigation déterminée dans sa vie privée*".

respect du principe de proportionnalité, au fondement de l'exigence de légitimité de la finalité. Le droit commun des contrats offre en outre des moyens de défense contre les abus du prestataire de service.

Comme on l'a vu précédemment, la Loi nouvelle reconnaît un droit d'opposition à la personne concernée en matière de marketing. Il implique la possibilité laissé à l'internaute de refuser pour l'avenir de voir ses données traitées pour une finalité de marketing "one-to-one". L'exercice de ce droit est gratuit et n'implique pas une motivation particulière. C'est, pour la finalité de marketing direct, la manière dont le législateur vient en aide au plus faible. Cette disposition, d'ordre public, ne souffre pas d'exception. Le contrat conclu entre l'internaute et le prestataire de service devra donc en tenir compte. La reconnaissance du droit d'opposition pourrait, le cas échéant, impliquer pour l'internaute la possibilité de résilier le contrat qui contiendrait une clause d'exploitation des données à caractère personnel en vue d'une finalité de marketing.

La Loi nouvelle dispose certes que le consentement suffit pour légitimer un traitement, fut-il de marketing one-to-one. Cette possibilité de légitimation n'est cependant pas absolue. Le jeu des articles 4 et 5 de la loi impose, selon nous[59], de considérer que la condition de légitimité, présente à l'article 4, l'emporte sur les conditions de légitimité posés a priori par l'article 5 de la même loi. L'article 4 joue comme un garde fou qui peut trouver à s'appliquer dans la problématique à analyser. Le consentement donné dans le cadre de l'application de la loi implique une condition particulière : l'atteinte librement consentie ne peut-être manifestement disproportionnée.

Le droit commun implique -outre un objet licite[60]- que le consentement doit être exempt de vices. Ce faisant il offre des moyens de défense à l'internaute. On peut penser particulièrement au dol ou à la lésion qualifiée[61]. Ces deux conditions supposent cependant que les pratiques en cause aient eu un effet déterminant sur le consentement de la partie qui s'en prévaut. Le dol pourrait par exemple être retenu si la personne concernée n'est pas suffisamment ou incorrectement informée des buts d'utilisation et des modalités des traitements des données exigées par le contrat. La lésion qualifiée pourrait être constituée d'un déséquilibre manifeste entre les prestations réciproques -transmission des données v. accès au site ou à l'information- issu de l'abus du prestataire de services des circonstances d'infériorité dans lesquelles se retrouveraient les internautes -en cas d'absence de transmission des données, ces derniers ne pourraient plus accéder au net, au site ou à l'information en cause-. On peut également

[59] Voy. également dans le même sens, les auteurs cités supra, note 36.

[60] On retourne alors à la case départ. L'objet du contrat ne peut être contraire à l'ordre public et aux bonnes moeurs. L'ordre public renvoie in casu notamment au respect de la Loi.

[61] Voy. par exemple, S. STIJNS, D. VAN GERVEN, P. WERY, "Chronique de jurisprudence - Les obligations : les sources (1985-1995)", *J.T.*, 1996, p. 709 et s.

penser à l'interdiction des clauses abusives présente à l'article 31 de la loi sur les pratiques du commerce. Dans certaines circonstances, le droit commun pourrait donc voir dans les stipulations contractuelles soumettant l'accès à l'internet, à un site ou à certains services, à une transmission de données à caractère personnel comme constitutives d'un vice de consentement ou d'une clause abusive.

En cas de déséquilibre manifeste entre les prestations des parties, l'accès gratuit soumis à la condition d'un transfert de données à caractère personnel en vue de la réalisation de finalités de marketing direct serait illicite. Commence alors la recherche de l'équilibre, forcément mouvant en raison des circonstances de l'échange de consentement. Ainsi, il faudra tenir compte de la prestation promise -accès à l'internet lui-même ou à un site spécifique-, à la nature des données transmises -données sensibles, données de trafic etc.-, à la portée du consentement en terme de finalités -possibilité de transmission d'autres produits ou services, commercialisation de profils etc.-, aux effets réels du refus d'accès -accès possible moyennant paiement, le prestataire est en situation de monopole et refuse tout accès, le service peut être considéré comme essentiel etc.- etc. Il reviendra aux organes de contrôle, à la jurisprudence et à la doctrine d'étudier plus finement cette recherche d'équilibre.

18. Anonymat sur internet : l'émergence d'une nouvelle facette de la liberté ? - En réaction contre les risques d'abus constitués par les nouvelles techniques de collecte et de traitements de données à caractère personnel sur internet, il est de plus en plus affirmé que l'internaute devait se voir reconnaître l'anonymat sur l'internet[62].

Le raisonnement se fait généralement par une analogie à la situation effective dans le monde réel: "*il faudrait retenir comme principe que l'utilisateur doit pouvoir choisir de rester anonyme en ligne lorsqu'il a le même choix hors ligne*"[63].

Ce principe porte en lui-même ses limites. Comme l'indique le Conseil d'Etat français, "*L'anonymat est une question complexe, au carrefour*

[62] Voy. par exemple la recommandation 3/97 du groupe 29 "L'anonymat sur Internet" disponible à l'adresse http://europa.eu.int/comm/dg15/fr/media/dataprot/wpdocs/index.htm; J. KUOPUS, "Direct marketing and privacy : new perspectives", in *Privacy : new risks and opportunities*, Cahier du Crid n°13, Namur, 1997, p. 165 concernant certains développement en Allemagne; S. RODOTA, "Beyond the EU Directive : Directions for the future", in *Privacy : new risks and opportunities, op. cit.*, p. 209 et s.; aussi le considérant 16 de la Proposition modifiée de directive du 17 août 1999 du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur (Com (1999) 427 Final, document disponible à l'adresse http://europa.eu.int/comm/dg15/en/media/eleccomm/com427fr.pdf) qui énonce que ses dispositions ne peuvent empêcher "*l'utilisation anonyme des réseaux ouverts, tels que l'internet*".

[63] Recommandation 3/97 du groupe 29, "L'anonymat sur Internet", *op. cit.*, sous titre "Tirer les leçons du passé pour résoudre les problèmes du futur".

d'intérêts éthiques, économiques et politiques : l'individu veut se promener et agir librement comme dans sa vie quotidienne réelle, les entreprises veulent l'identifier pour mieux le servir, les autorités répressives ont besoin de retrouver les coupables d'infractions et donc les identifier"[64]. Un droit à l'anonymat sur l'internet paraît a priori une chimère. Comme dans la vie réelle, il faudra tenir compte d'une opposition d'intérêts et rechercher un équilibre acceptable.

Le principe, tel que invoqué actuellement, pose également des interrogations. Est-il réaliste de se baser sur une analogie avec le monde réel et, dans ce cas, à quoi comparer l'internet dans le monde réel ? Surfer revient-il nécessairement à consulter anonymement une bibliothèque ou à faire du "*lèche-vitrine*"[65] ? Dans le monde réel, n'est-ce pas déjà très souvent le commerçant qui décide de transmettre ou non de l'information à des clients potentiels après avoir effectué un ciblage (direct marketing) ? L'entrée dans une bibliothèque n'est-elle pas toujours soumise à une inscription et sinon, ne faut-il pas toujours s'identifier pour les besoins du prêt ? Un abonnement à un journal ou à la télévision par câble n'implique-t-il pas toujours l'identification de l'abonné ? etc. Ne vaudrait-il pas prendre acte des évolutions et des spécificités de l'internet où l'anonymat est a priori un leurre pour repenser la protection de façon générale "*en réfléchissant à la question des droits de la personne virtuelle, différents peut-être de ceux de la personne réelle ?*"[66].

Les pistes de réflexion sont multiples mais il y a urgence. La technique n'attend pas. Elle n'a que faire des hésitations éthiques et juridiques qui, en toute hypothèse, n'auront que des conséquences dans un avenir relativement éloignée.

II. - Le respect du secret des télécommunications comme condition de licéité des collectes et traitements de marketing "one-to-one"

19. L'existence de dispositions spécifiques à la protection des données dans le secteur des télécommunications - Il est permis de se demander comment la réglementation spécifique au secteur des télécommunication va

[64] CONSEIL d'ETAT (fr), *Internet et les réseaux numériques - Etude adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998, op. cit.*, p. 47.

[65] Récemment, un auteur indiquait sous un sous-titre optimiste ("L'accès libre aux sites marchands paraît acquis"): "*La crainte que se développe la pratique de certains sites marchands américains exigeant, notamment des enfants, la communication de données personnelles pour l'accès aux services qu'ils offraient gratuitement, a conduit la CNIL à recommander tout d'abord que tout accès à un site marchand soit libre. C'est-à-dire que ne doit pas être exigé de l'internaute qu'il s'identifie a priori. Une telle identification serait disproportionnée. Il doit être possible de "regarder", de faire du "lèche-vitrine" sans être identifié. L'intérêt du commerce a conduit de manière naturelle au respect de ces recommandations de sagesse.*" (M. GEORGES, "Relevons les défis de la protection des données personnelles : l'Internet et la CNIL", *op. cit.*, p. 71 et 72).

[66] CONSEIL d'ETAT (fr), *Internet et les réseaux numériques - Etude adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998, op. cit.*, p. 49.

s'appliquer aux différents prestataires de services sur internet et par là même, à certains acteurs au processus du marketing "one-to-one".

Trois textes particuliers d'origine distincte retiennent particulièrement l'attention : d'une part, l'article 314bis du Code pénal et l'article 109 ter d de la loi du 21 mars 1991 sur la réforme de certaines entreprises économiques; d'autre part certaines dispositions issues de la directive 97/66/CE du 15 décembre 1997 concernant les traitements de données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications[67].

Une étude systématique de ces dispositions dépasse de loin le cadre limité de la présente contribution. Il est néanmoins utile de montrer qu'elles recèlent de nombreuses limites d'utilisation des données relatives à l'internaute.

20. L'article 314 bis du Code pénal et l'enregistrement des données relatives aux internautes - L'article 314bis du Code pénal punit "*d'un emprisonnement de six mois à un an et d'une amende de deux cents francs à dix mille francs ou d'une de ces peines seulement, quiconque (…) intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications*".

Le champ d'application matériel de cette disposition s'est voulu extrêmement large. L'exposé des motifs[68], comme les commentateurs de cette loi, admettent que les communications ou télécommunications visent également "*la transmission électronique de données dans des ordinateurs ou des réseaux d'ordinateurs*"[69]. Il ne fait dès lors aucun doute que la transmission de données sur internet est visée par cette disposition[70].

D'après l'exposé des motifs de cette loi, "*Les communications ou télécommunications sont privées lorsqu'elles ne sont pas destinées à être*

[67] *J.O.C.E.*, L 24, 30 janvier 1998.

[68] *Doc. Parl.*, Sénat, sess. ord. 1992-1993, n°843-1, p. 7.

[69] Voy. par exemple, H.-D. BOSLY, D. VANDERMEERSCH, "La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées", *R.D.P.*, 1995, p. 304, note 11; T. HENRION, "Les écoutes téléphoniques", *J.T.*, 1995, p. 209, note 26 et 28.

[70] Voy. également dans ce sens R. FELTKAMP, M. FLAMÉE, "Telecommunicatie, privacy en bescherming van persoonsgegevens - Deel I. Bescherming van het communicatiegeheim", *A. & M.*, 1999, p. 173; P. LAMBERT, "Bescherming van prive-(tele)communicatie", in *Recente ontwikkelingen in informatica- en telecommunicatierecht*, Icri, Brugge, die Keure, 1999, p. 185 et 193.

entendues par tout un chacun"[71]. Peu importe dès lors également que le mode de transmission se fasse par un réseau de télécommunication privé ou public[72]. Les critères à prendre en considération sont le contexte et les intentions des parties[73].

Ne peut-on dès lors raisonnablement soutenir que la simple visite d'un site[74], et a fortiori toute expression d'une interactivité entre un site et un internaute -par exemple, lors de la rédaction d'un bon de commande d'un produit ou service par l'internaute et son renvoi vers le site ou lors de l'envoi des informations relatives à un paiement-, sont constitutives de communications et/ou de télécommunications privées entre le prestataire de service et l'internaute ?[75] Ne faut-il pas également qu'il en soit de même concernant les informations issues de l'utilisation des protocoles techniques utilisées et du bavardage des logiciels de navigation ? En effet, éléments indispensables de toute communication ou télécommunication sur internet, ces informations s'identifient ou constituent l'accessoire indispensable au contenu même des

[71] *Doc. Parl.*, Sénat, sess. ord. 1992-1993, n°843-1, p. 7.

[72] H.-D. BOSLY, D. VANDERMEERSCH, "La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées", *op. cit.*, p.305.

[73] P. DE HERT, "Schending van het (tele)communicatiegeheim in het beroepsleven", *R.D.S.*, 1995, p. 263, n°49; R. FELTKAMP, M. FLAMÉE, "Telecommunicatie, privacy en bescherming van persoonsgegevens - Deel I. Bescherming van het communicatiegeheim", *op. cit.*, p. 176.

[74] A notre sens, la réponse est généralement positive. Toute "visite" d'une page suppose une transmission de données de l'ordinateur de l'internaute vers celui du serveur du fournisseur d'informations et une réponse de ce dernier avec la transmission de nouvelles informations. Cette transmission est privée dès lors qu'il découle de l'intention des parties et du contexte que ces informations ne sont pas destinées à être captées par tout un chacun. C'est généralement le cas dès lors que si page web est offerte au public, sa lecture par une personne identifiée ou identifiable via un cookie n'en reste pas moins privée et confidentielle a priori. Il faut en outre tenir compte de la différence entre la captation des données de trafic et celle du résultat de la communication qui peut impliquer une publication ultérieure du message transmis. *contra* P. LAMBERT, "Bescherming van prive-(tele)communicatie", *op. cit.*, p. 201 : "*Het bezoeken van een vrije toegankelijke website op het Internet is evenmin privé-communicatie of -telecommunicatie, maar kan het wel worden als het gaat om een afgeschermde besloten website*".

[75] On en arrive à une telle conclusion lorsque l'on considère, comme le groupe 29, que la directive 97/66/CE du 15 décembre 1997 s'applique à l'internet. L'article 5 oblige en effet les Etats Membres à garantir la confidentialité des communications effectuées au moyen d'un réseau public de télécommunications ou de services de télécommunications accessible au public sans distinguer selon qu'il s'agit d'une communication privée ou non (sans distinguer non plus suivant que l'interception se fait durant la transmission ou non). Voy. aussi la Recommandation 2/99 du groupe 29 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications du 3 mai 1999 (disponible à l'adresse http://europa.eu.int/comm/dg15/fr/media/dataprot/wpdocs/index.htm) où, analysant la résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications (*J.O.*, C329 du 14 novembre 1996), il constate que les données visées par les interceptions concernent "*les appels téléphoniques mobiles ou non, les courriers électroniques, les télécopies et messages télex, les flux de données Internet, tant au niveau de la prise de connaissance du contenu des télécommunications que des données afférentes aux télécommunications (celles-ci se réfèrent notamment aux données de trafic, mais également à tout signal émis par la personne faisant l'objet de la surveillance -point 1.4.4. de la résolution)*".

requêtes ou des informations transmises[76]. Tout tiers qui intentionnellement viendrait enregistrer ces informations lors de leur transmission agirait donc en violation de l'article précité si il n'obtenait pas le consentement des parties.

Cependant la solution du consentement pourrait s'avérer illusoire. En effet, l'intention du législateur a bien été que le consentement soit spécifique : l'insertion d'un consentement général dans un contrat est a priori exclue[77]. On pourrait cependant considérer que l'obtention du consentement est valide dès lors qu'il serait obtenu par click-wrap avant chaque transmission d'information captées.

Un participant à la communication et/ou la télécommunication pourrait cependant enregistrer son contenu, même à l'insu des autres interlocuteurs[78]. Le serveur du prestataire de service pourrait donc éventuellement enregistrer le contenu des requêtes adressées par l'internaute, ses données de trafic etc. Pas une société tierce de marketing.

21. L'article 109ter D de la loi du 21 mars 1990 et l'enregistrement de certaines données relatives aux internautes - L'article 109ter D de la loi 21 mars 1990 sur la réforme de certaines entreprises économiques énonce que :"*Sous réserve de l'autorisation de toutes les autres personnes directement ou indirectement concernées par l'information, l'identification ou les données visées ci-après, il est interdit à quiconque, qu'il agisse personnellement ou par l'entremise d'un tiers : 1° 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 télécommunications, en provenance d'autres personnes et destinées à celles-ci; 2°. de transformer ou de supprimer frauduleusement par n'importe quel procédé technique l'information visée au 1° ou d'identifier les autres personnes; 3° de prendre connaissance intentionnellement de données en matière de télécommunications, relatives à une autre personne; 4° de*

[76] C'est particulièrement vrai lorsque le tiers -telle l'agence de publicité- obtient le contenu des requêtes effectuées par l'internaute (ex. : le mot introduit dans un moteur de recherche).

[77] Exposé des motifs, *op. cit.*, p. 6 et 7 où le législateur vise expressément l'emploi de clauses contractuelles dans un contrat de travail; voy. également en doctrine, **;** L. ARNOU, "Het respecteren van het telefoongeheim in België na de afluisterwet van 30 juni 1994", *Computerrecht*, 1995, p. 160, n°18; H.-D. BOSLY, D. VANDERMEERSCH, "La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées", *op. cit.*, p. 306; P. DE HERT, "Schending van het (tele)communicatiegeheim in het beroepsleven", *op. cit.*, p. 268, n°54.

[78] L. ARNOU, "Het respecteren van het telefoongeheim in België na de afluisterwet van 30 juni 1994", *Computerrecht*, 1995, p.159, n°14; H.-D. BOSLY, D. VANDERMEERSCH, "La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées", *op. cit.*, p. 305. Pour une opinion plus nuancée, voy. P. DE HERT, "Schending van het (tele)communicatiegeheim in het beroepsleven", *op. cit.*, p. 272 et s.

révéler ou de faire un usage quelconque de l'information, de l'identification et des données obtenues intentionnellement ou non et visées aux 1°, 2° et 3°, de les modifier ou de les annuler".

Le contenu des communications ne sont plus visés mais bien leur existence[79]. Appliqué à l'internet, il s'agirait, pour un tiers, de prendre connaissance du fait que Monsieur X a transmis (ou reçu) des données à (de) la société Y.

Les "*données en matière de télécommunication*" sont des données de trafic comme le lieu de la transmission, un numéro secret etc. à l'exclusion des données généralement connues comme le nom, l'adresse etc.[80]. Des données telles que le browser utilisé par l'internaute lors de la transmission, son numéro TCP/IP etc. paraissent donc bien tomber sous le champ d'application de cette disposition[81].

La technique du cookie elle-même pourrait également être visée. Le cookie, on l'a vu, permettra bien souvent d'identifier l'internaute. Cette identification est précisément interdite par le 2° de la disposition commentée.

Le consentement de l'internaute s'imposerait ici également comme une solution pour ne pas violer ladite disposition[82] [83].

22. La directive 97/66/CE du 15 décembre 1997 et l'enregistrement de certaines données relatives à l'internaute - Il faut également tenir compte des dispositions issues de la directive 97/66/CE du 15 décembre 1997 concernant les traitements de données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Une analyse complète des dispositions de cette directive est impensable dans le cadre de cette contribution.

On attire cependant particulièrement l'attention sur l'article 6 de la directive récemment introduit en droit belge par l'article 4 de l'arrêté royal du 21 décembre 1999 introduisant un nouvel article 105 nonies dans la loi du

[79] La prise de connaissance durant la transmission n'est pas une condition d'application de la disposition. Cette condition spécifique, retenue expressément par l'article 317 bis du Code pénal y est en effet absente.

[80] P. DE HERT, "Schending van het (tele)communicatiegeheim in het beroepsleven", *op. cit.*, p. 248, n°30.

[81] Cfr supra également la note 74.

[82] Il faut cependant apporter la preuve du caractère frauduleux de la prise de connaissance.

[83] L'article 109 ter E prévoit en outre que les actes visés tant à l'article 314 bis du Code pénal qu'à l'article 109 ter D de la loi du 21 mars 1991 ne sont pas punissables si la loi le permet ou lorsque les données sont utilisées pour contrôler le bon fonctionnement du réseau ou assurer la bonne exécution du service de télécommunication. Il est clair que le traitement poursuivi en vue de la constitution d'une banque de données de marketing n'a rien à voir avec un contrôle de bon fonctionnement ou la bonne exécution du service de télécommunication.

21mars 1991[84]. Cette nouvelle disposition de droit belge indique en son §1er que "*(...) les opérateurs d'un réseau public de télécommunications et/ou les fournisseurs d'un service de télécommunications accessible au public, effacent et rendent anonymes les données relatives au trafic*[85] *concernant les abonnés*[86] *et les utilisateurs et traitées en vue d'établir des communications. Ces opérations sont exécutées dès que la communication est terminée*". Le §2 précise néanmoins qu'en dérogation au §1er, les mêmes destinataires peuvent stocker et traiter certaines données énumérées limitativement[87] en vue d'établir les factures des abonnés ou les paiements d'interconnexion mais pour une durée limitée[88].

En son dernier alinéa, cette disposition ajoute que "*Le traitement de ces données ne peut avoir lieu qu'en vue de la vente des services. Le traitement ne peut avoir lieu que moyennant l'autorisation expresse de l'abonné*". Pour comprendre cette disposition, a priori sibylline, il convient de se référer à l'article 6.3. de la directive : on y vise clairement la finalité de marketing portant sur les propres services du prestataire d'un service de télécommunications accessibles au public[89].

Le prestataire de services de télécommunications accessible au public au sens de la loi du 21 mars 1991 ne peut donc ni traiter des données relatives à

[84] Arrêté royal du 21 décembre 1999 adaptant certaines dispositions de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques aux directives de l'Union européenne, *M.B.*, 9 février 2000, p. 3916 et s.

[85] Ni la loi, ni la directive 97/66 ne donnent une définition de la donnée de trafic. Le considérant 17 de la directive 97/66 indique qu'il s'agit des "*données relatives aux abonnés qui sont traitées pour établir des communications*". Il semble dès lors raisonnable de considérer qu'il s'agit non seulement de l'adresse TCP/IP de l'internaute mais également, de manière plus générale, de toutes les informations transmises par l'internaute ou son browser pour les besoins des connexions aux divers prestataires de services sur internet, dont l'accès provider ou le fournisseur de service au sens de la loi du 21 mars 1991 a ou peut avoir connaissance lors de l'exécution de leurs missions. Il s'agirait donc, mutatis mutandis, des données de télécommunication au sens de l'article 109 ter D de la même loi.

[86] Un nouvel article 68, 21°bis de la loi du 21 mars 1991 est inséré par l'article1er du même arrêté royal. Il définit l'abonné comme "toute personne qui a conclu un contrat avec le prestataire de services de télécommunications accessibles au public en vue de la fourniture de tels services". L'article 2, a de la directive 97/66 précise en outre qu'il s'agit tant d'une personne physique que d'une personne morale.

[87] Ces données sont très réduites : le numéro et le poste de l'abonné, l'adresse de l'abonné et le type de poste, le nombre total d'unités à facturer pour la période de facturation, le numéro de l'abonné appelé, le type d'appels, l'heure à laquelle l'appel a commencé et la durée des appels effectués et/ou la quantité de données transmises, la date de l'appel ou du service ainsi que d'autres informations relatives aux paiements, telles que celles qui concernent le paiement anticipé, le paiement échelonné, la déconnexion et les rappels.

[88] L'avant dernier alinéa précise qu'il s'agit de "*la fin de la période de contestation de la facture ou jusqu'à la fin de la période au cours de laquelle des poursuites peuvent être engagées pour en obtenir le paiement*".

[89] Article 6.3. de la directive 97/66/CE : "*Dans le but de commercialiser ses propres services de télécommunications, le prestataire d'un service de télécommunications accessible au public peut traiter les données visées au paragraphe 2, pour autant que l'abonné ait donné son consentement*".

ses abonnés pour le compte de tiers, ni les communiquer à des prestataires de services tiers, ni traiter d'autres informations que celles énumérés dans la loi en vue d'une finalité de marketing. Ce traitement est en outre conditionné à l'autorisation expresse de l'abonné. Quid en ce qui concerne l'application de cette disposition aux acteurs présents sur internet ?

Un doute important existait -et persiste- quant à l'applicabilité matérielle à l'internet et personnelle aux fournisseurs de services sur internet de la directive 97/66. Il existe une contradiction évidente entre les définitions présentes dans ce texte[90], qui permettent sans doute de comprendre dans leur champ les internet Access Provider, voire certains fournisseurs de services sur internet (comme les prestataires de services d'e-mail[91]) et son contenu même qui, explicitement, ne vise que la téléphonie fixe et mobile[92].[93]. De plus en plus, l'application de ce texte à l'internet est affirmée[94].

[90] Le service de télécommunications y est défini en son article 2 d) comme : "*les services qui consistent, en tout ou partie, en la transmission et l'acheminement de signaux sur des réseaux de télécommunications, à l'exception de la radiodiffusion et de la télévision*". Voy. l'article 68, 19° de la loi du 21 mars 1991 qui contient une disposition quasi-identique.

[91] Certains commentateurs vont plus loin et visent indistinctement les services de presse électronique ou l'e-commerce en général (Cullen International, *A business guide to changes in eurpean data protection legislation*, Kluwer Law International, 1999, p. 129).

[92] Le but de ce texte était au départ de réglementer les seuls réseaux RNIS et qu'elle fut ensuite étendue à la téléphonie vocale et mobile. Il n'a pas été rédigé en tenant compte du phénomène, naissant à l'époque, de l'Internet. Le considérant ne parle à aucun moment de l'Internet. Du reste, certaines des dispositions qui y sont contenues (par exemple l'article 12 concernant les appels non sollicités) paraissent, de par le vocabulaire employé, exclure toute application à l'Internet.

[93] En Grande-Bretagne, le "*Interim guidance*" annexée à certaines dispositions réglementaires implémentant certaines dispositions de la directive litigieuse -mais pas son article 6- indique que "*The Registrar's view is that the transmission of messages using the above media will be covered by the Directive unless specifically excluded (radio and television broadcasting). There is an argument, therefore, that e-mail may be covered. The DTI has taken the view that not all the provisions of the TDPD [ndlr : pour "Telecommunications Data Protection Directive". apply to email. This is based on the use of the word "call" in Article 10 and 12 of the Directive which they consider implies that those provisions only apply to conventional telephone calls. The Registrar recognises the basis of this approach but considers that the relevant definitions are those relating to public telecommunications network and telecommunications services and these cover email. Before coming to a formal view the Registrar will consider the matter further. The Registrar recognises that it may not, in practice, be easy to apply all the provisions of the TDPD, and of the Regulations giving effect to the Directive, to email services as they are currently organised (…)*". Document disponible à l'adresse : http;//www.open.gov.uk/dpr/telcom1.htm).

[94] Ainsi, le groupe 29 l'a affirmé à diverses reprises (cfr. par exemple Document de travail : Traitement des données à caractère personnel sur l'Internet (WP16), Recommandation 3/99 relative à la préservation des données de trafic par les fournisseurs de services internet pour le respect du droit (WP25), disponibles à l'adresse http://europa.eu.int/comm/dg15/en/media/dataprot/WPdocs/. On remarque également que la directive 97/66 est explicitement visée par les considérants 6bis, 11, 15, 16 précédant le projet de directive e-commerce. comme s'appliquant aux fournisseurs de services de la société de l'information. Dans l'esprit des rédacteurs, la directive 97/66 s'applique donc bien à internet. (Proposition modifiée de directive du 17 août 1999 du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur, Com (1999) 427 Final, document disponible à l'adresse http://europa.eu.int/comm/dg15/en/media/eleccomm/com427fr.pdf.

En droit belge, la situation paraît s'être éclaircie depuis l'adoption des mesures d'exécution de la loi du 21 mars 1991 concernant la soumission de certains services à des conditions d'exploitation et les commentaires qui en ont été donnés par l'IBPT. Les fournisseurs d'accès à l'internet sont explicitement visés comme étant un service de données compris dans la notion d'"*autres services de télécommunications*" au sens de l'article 90 de la loi. Or, ces autres services se comprennent par rapport à la définition générale du "*service de télécommunications*". L'accès à l'internet est donc bien un service de télécommunications au sens de cette définition[95]. L'IBPT vise également d'autres fournisseurs de services sur internet : "Voice over Internet", courrier électronique etc.

A tout le moins, on peut donc soutenir que le nouvel article 105 nonies de la loi du 21 mars 1991 pourrait restreindre fortement la possibilité, pour les fournisseurs d'accès et services de télécommunications[96] soumis à cette législation, de traiter des données de trafic relatives à leurs internautes-abonnés en vue de la poursuite d'une finalité de marketing direct.

§ 4. - conclusions

23. Conclusions - Tous les facteurs convergent vers l'existence d'une union providentielle entre l'e-commerce et les techniques les plus avancées de profilage des internautes. En matière d'internet, ce qui se fait actuellement aux Etats-Unis préconise souvent la situation future qui prévaudra dans le reste du monde. Du reste, l'internet est un réseau mondial : les internautes européens, en visitant les sites américains, sont soumis au même régime attentatoire que leurs homologues américains.

Les principes de légitimités et de licéité, proclamés par les lois protectrices des données à caractère personnels en Europe paraissent pouvoir fournir un rempart aux dérives rendues possibles par l'évolution incessante des technologies de l'information. On pourrait trouver, en outre, dans les

[95] Ce raisonnement se retrouve dans la Communication de l'IBPT concernant les conditions d'accès aux marchés belges des services des télécommunications visés aux articles 88 et 90 de la loi du 21 mars 1991, document disponible sur le site de l'IBPT (http://www.ibpt.be). Il découle du rapprochement des articles 68, 19° et 90 de la loi du 21 mars 1991, de l'arrêté royal du 20 avril 1999 concernant les catégories de services de télécommunication soumis à des conditions d'exploitation (*M.B.*, 21 juillet 1999) et de l'arrêté ministériel du 11 juin 1999 fixant les conditions d'exploitation imposées à certains services de télécommunications (*M.B.*, 21 juillet 1999, p; 27725 et s).

[96] Ce texte pourrait encore être interprété plus largement. L'article 1er de l'arrêté royal du 20 avril 1999 précité, définit le service de données -dont on a vu que l'accès à internet fait partie- comme le "*service consistant en la transmission, la commutation ou le traitement de données destinées à être envoyées via un réseau de télécommunications*". On peut dès lors se demander si tous les prestataires de services en ligne sur internet ne répondent pas très exactement à cette définition. En effet, mettre des pages web à disposition d'autrui ne revient-il pas toujours à fournir un service de traitement et de transmission de données destinées à être envoyées via un réseau de télécommunications aux internautes ? On admet cependant qu'une telle interprétation paraît fortement éloignée de la notion de "service de télécommunications" au sens de l'article 68, 19° précité.

législations spécifiques aux télécommunications des moyens supplémentaires pour renforcer la protection des données relatives aux internautes.

L'application de ces principes protecteurs -créés pour faire face à une réalité de traitement dépassée- amène paradoxalement avec elle de nouvelles difficultés et de nouveaux enjeux pour la protection elle-même. Le consentement de l'internaute engendre un risque de contractualisation généralisée de la protection des données sur internet et donc un risque de discrimination entre les internautes ayant transmis leurs données et les autres.

Si ces nouvelles paraissent alarmantes, tout n'est pas noire dans ce tableau. Les nouvelles techniques de marketing en appellent à une transparence des pratiques de collectes. Les internautes, qui constituent encore aujourd'hui une caste de gens aisés sensibles à la problématique des atteintes aux libertés individuelles, sont plus enclins à réagir que dans le monde réel. Les consommateurs américains n'ont peut-être pas de loi protectrice spécifique mais de très nombreuses associations de consommateurs très actives sur leur territoire. Bien implantées sur l'internet lui-même, connaissant parfaitement l'outil, elles sont bien décidées à combattre le rouleau compresseur de l'industrie e-commerce américaine. La technologie elle-même recèle également de nouveaux moyens permettant d'adapter les exigences de la protection au nouveau média (P3P, labellisation des sites etc.[97]). Enfin, l'Union Européenne brandit encore -mais pour combien de temps ?- la menace de l'interdiction des flux de données à caractère personnel vers les Etats-Unis en cas d'absence d'un système de protection efficace.

Ne nous voilons pas la face. Si les lois sur la protection des données restent peu et mal appliquées dans le monde réel, la situation est encore pire à l'heure actuelle sur internet (et notamment sur les sites e-commerce "belges"). Ces lois souffrent toujours de l'absence de contrôle réel et efficace de leur application, de leur méconnaissance généralisée tant par le public que par le monde judiciaire et de leur complexité qui décourage les meilleurs volontés. La majorité des Etats ne se sont toujours pas dotés de ce type de législation. Internet et l'e-commerce offrent peut-être la chance ultime de rattraper un train qui déjà s'éloigne dangereusement... Saurons-nous la saisir ?

Thierry Léonard
Avocat au Barreau de Bruxelles
Assistant à la Faculté de Droit de Namur (Centre de Recherche Informatique et Droit)
thierry.leonard@fundp.ac.be
Février 2000

[97] Pour une analyse critique de ces procédés techniques, J. -M. DINANT, "Law and Technology Convergence in the Data Protection Field ? Electronic threats on personal data and electronic data protection on the Internet", *op. cit.*