
Denise Lebeau-Marianna
Avocate, Baker&McKenzie



Publicité comportementale : enjeux, risques et tendance

Pour les acteurs de l'écosystème actuel du marché de la communication en ligne (annonceurs, agences, régies publicitaires et éditeurs), la publicité personnalisée (publicité contextuelle, ciblage comportemental) fait partie des tendances clés des stratégies publicitaires car constituant une source de rémunération plus élevée.

Pour le consommateur, la publicité personnalisée répond à un désir de services pertinents et de qualité, susceptibles de lui faire gagner du temps et témoigne d'une attention dont le consommateur est en quête surtout à l'égard de sites régulièrement fréquentés.

L'exploitation des données personnelles qui en résulte peut néanmoins se révéler intrusive du fait de technologies de plus en plus innovantes permettant de tracer son comportement sur Internet et ce, de façon extrêmement fine.

On assiste ainsi à un phénomène étrange de « paradoxe de la vie privée » (*privacy paradox*) qui se traduit par une tendance naturelle à publier un volume croissant d'informations pour obtenir de meilleurs services, bénéficier de certains avantages, être reconnu à chaque visite, tout en craignant de dévoiler sa vie privée.

Ce phénomène n'est pas sans inquiéter les autorités de part et d'autre de l'Atlantique. Les rapports publiés en 2009, par la Federal Trade Commission (FTC) aux Etats-Unis et la Commission Européenne sur la mise en œuvre des pratiques de ciblage comportemental et leur impact sur le respect de la vie privée des internautes, ont réaffirmé l'application des principes protecteurs applicables en matière de données personnelles tels qu'ils résultent de la réglementation en vigueur. Cette tendance a également été confirmée par la récente étude de la Commission Nationale de l'Informatique et des Libertés (CNIL), et le rapport du Sénat¹ qui rappelle que les principes de la loi Informatique et Libertés sont universels et intemporels. Si la capacité des législations actuelles à appréhender la publicité comportementale est ainsi réaffirmée (1), cette approche visant à protéger un internaute passif, nécessite néanmoins des adaptations afin de tenir compte de l'évolution de son comportement de plus en plus interactif, en particulier dans le contexte de sites web 2.0 où il lui importe de mieux maîtriser les données qu'il communique (2).

¹ Rapport du Sénat sur « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information » du 27 mai 2009.

1. Capacité de la législation actuelle des Etats membres à appréhender la publicité comportementale

La CNIL définit la publicité comportementale comme celle « choisie en observant le comportement de l'internaute à travers le temps (...), laquelle étudie les caractéristiques de l'internaute par ses actions pour en déduire son profil et lui proposer des publicités adaptées »². Elle la distingue (i) de la publicité personnalisée, « choisie en fonction des caractéristiques connues de l'internaute (âge, sexe, localisation...) et qu'il a fournies en s'inscrivant à un service » sur un site et (ii) de la publicité contextuelle, « choisie en fonction du contenu immédiat » consulté ou du mot clé utilisé par l'internaute. En pratique, la CNIL reconnaît que la frontière entre ces différents modes de publicité est ténue.

Les principaux griefs adressés à la publicité comportementale sont les suivants :

- elle repose sur des profils qui, bien qu'élaborés à partir de données de navigation anonymes, permettent à travers des rapprochements d'opérer des discriminations commerciales. En effet, les informations collectées à des fins de ciblage peuvent révéler ce qu'un consommateur est prêt à payer pour obtenir un certain type de service, ses risques d'insolvabilité, sa propension à retourner le bien acheté etc. une telle analyse comportementale permet ainsi de traiter une même demande de manière différenciée.
- elle donne lieu à une collecte et un traitement de données à l'insu de l'internaute qui n'a pas toujours conscience :
 - o de l'ampleur des données collectées sur lui, ni de la finalité de ces traitements ;
 - o de la conservation excessive de ses données : la durée de conservation est un des facteurs permettant de gagner en précision dans le profilage, ce qui n'est pas sans risque en cas de défaillance des mesures de sécurité en place ;
 - o des destinataires de ses données : alors que la publicité sur site permet de limiter l'accès aux données personnelles des utilisateurs au seul site Internet choisi par l'annonceur, la publicité effectuée par les régies publicitaires repose sur la constitution de profils et l'agrégation de données à travers le temps et l'espace (collecte d'informations sur plusieurs mois et sur plusieurs sites visités) en coopération avec les fournisseurs de contenus.
- elle s'inscrit dans une démarche de plus en plus intrusive : les offres triple play caractérisées par la convergence des technologies (Internet, téléphone, télévision) permettent potentiellement à un même opérateur de collecter une quantité incroyable d'informations à travers celles volontairement communiquées par les internautes et celles issues de l'observation de son comportement sur les sites. Nul doute que grâce à un recoupement de ces informations, le même opérateur pourra à terme diffuser des publicités télévisuelles adaptées au profil de l'internaute et réciproquement sur Internet en relation avec les émissions télévisées ou les conversations téléphoniques.

² Communiqué de la CNIL sur « la publicité ciblée en ligne » présentée en séance plénière le 5 février 2009 et publiée le 27 mars 2009 sur son site Internet.

Une analyse comparée nous a permis de constater que ces différents risques sont appréhendés par la réglementation actuelle de la plupart des pays européens³ issue de la transposition de la directive européenne sur la protection des données personnelles (directive 95/46/CE) et celle relative à la vie privée et aux communications électroniques (directive 2002/58/CE), à travers les principes fondateurs suivants :

- 1.1. Une conception large de la notion de données personnelles
- 1.2. Une information claire, complète et loyale
- 1.3. La nécessité de veiller à la sécurité des données collectées et de limiter leur durée de conservation

1.1 Une conception large de la notion de « données personnelles » applicable à toute activité de profilage

Les techniques de traçage à des fins de profilage sont souvent considérées comme anonymes car visant à analyser le comportement des internautes sans toutefois véritablement les identifier. En effet, les profils (âge, sexe, localisation) issus d'analyses prédictives déduites des sites visités, publicités cliquées, mots clés recherchés, langue des sites consultés, sont souvent considérés comme incomplets et insuffisamment précis pour identifier un individu.

Précisant les définitions retenues par les directives et les législations nationales, le G29⁴ a rappelé dans son avis 4/2007 du 20 juin 2007 qu'une donnée personnelle repose sur « toute information » « concernant » « une personne physique », « identifiée ou identifiable ». L'avis précise que : « les données concernent une personne si elles ont trait à l'identité, aux caractéristiques ou au comportement d'une personne ou si cette information est utilisée pour déterminer ou influencer la façon dont cette personne est traitée ou évaluée ».

La FTC⁵ rejoint d'ailleurs cette approche en préconisant l'application de son projet de code de conduite à toutes données qu'elles soient « personnellement identifiables » ou non, dès lors que celles-ci sont « collectées à des fins de publicité comportementale en ligne qui pourraient raisonnablement être associées à un consommateur en particulier ou un ordinateur ou un appareil en particulier ».

Ces définitions permettent clairement d'appréhender toutes données permettant d'identifier une personne sans nécessairement connaître son identité : identifiants se trouvant dans les cookies, données de connexion, données de navigation, données servant à constituer des profils (âge, sexe, localisation, etc.), adresse IP⁶, etc.

³ Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et Loi pour la Confiance dans l'Économie Numérique du 21 juin 2004 (France) ; Loi en matière de protection des données à caractère personnel du 6 juillet 2000 et la décision du 7 mai 2004 relative aux services universels et aux intérêts des consommateurs finaux (Pays-Bas) ; Loi relative à la protection des données à caractère personnel de 1998 et réglementations en matière de vie privée et communications électroniques de 2003 (Royaume-Uni) ; Loi du 13 décembre 1999 et Décret Royal du 21 décembre 2007 en matière de protection des données à caractère personnel, Loi n°34-2002 relative au commerce électronique et aux services de la société d'information (Espagne) ; Loi du 29 août 2007 relative à la protection des données à caractère personnel et Loi du 18 juillet 2002 pour la fourniture de services électroniques (Pologne) ; Loi fédérale de protection des données à caractère personnel du 23 mai 2001, Loi Telemedia du 26 février 2007 (Allemagne).

⁴ Le Groupe 29 est constitué des autorités de protection des données de tous les pays de l'UE.

⁵ Rapport de la Federal Trade Commission du 7 février 2009 sur la publicité comportementale.

⁶ Rapport du Sénat du 27 mai 2009 confirme que l'adresse IP est une donnée personnelle.

Si cette conception extensive des données personnelles est parfois considérée comme excessive parce qu'il s'agit de données qui, en elles-mêmes, ne permettent aucune identification, force est de constater que la tendance est à affirmer que ces données sont personnelles et donc soumises à la réglementation protectrice en la matière, dès lors qu'elles permettent de reconstituer la personnalité d'un individu et de lui attribuer des décisions en fonction de ses choix et préférences.

On constate, à ce titre, une position harmonisée des autorités de régulation nationale des différents Etats Membres.

1.2 Une information claire, complète et loyale

Les techniques de profilage et de collecte des données sont généralement peu transparentes.

Or, l'internaute doit être clairement informé, non seulement lorsqu'il fournit ses données volontairement en remplissant un formulaire de collecte (profil explicite), mais également en cas de collecte non visible lors de la constitution de profils par étude du comportement de l'internaute sur le site (profil prédictif - analyse de la navigation, des achats, etc.). Cette information indiquera les conditions et moyens de collecte (utilisation d'un cookie et les possibilités de le désactiver), les finalités (l'envoi d'une publicité personnalisée), les catégories de destinataires, l'existence d'un partage de catégories de données avec des tiers (régie publicitaire, annonceurs, etc.). L'internaute devra pouvoir s'opposer de manière effective à cette collecte ou y consentir expressément dans le cas d'envoi de publicité par courriel (opt-in). Ces droits s'exerceront sans affecter le consommateur dans le déroulement de son processus d'achat.

La mise en œuvre de cette obligation d'information demeure toutefois insuffisante puisque :

- traditionnellement reflétée par la mise en ligne de « charte de protection des données personnelles », ces chartes ou « *privacy policy* » sont aujourd'hui considérées comme inadaptées car très peu lues par l'internaute.
- si l'internaute a en principe la maîtrise de l'installation de cookies sur son ordinateur et la possibilité de s'y opposer, cette maîtrise s'avère illusoire car opter pour une réelle politique de contrôle des cookies est difficile à gérer parce qu'elle aboutit à une impossibilité de consulter le site, ou pénalise la navigation par l'envoi répété de messages.
- une absence d'information claire sur la manière de faire valoir ses droits, notamment de rectification et d'opposition, rend peu efficace la politique d'opt-out préconisée par les systèmes de publicité comportementale.

Ces obstacles conduisent donc à devoir repenser les modes d'information, point que nous aborderons par la suite.

Outre l'information préalable, il conviendra d'obtenir le consentement de l'internaute, et notamment:

- lorsque la collecte et le traitement portent sur des données sensibles (données de santé, ou relatives à la vie sexuelle, origines raciales ou ethniques, opinions religieuses ou philosophiques, appartenance syndicale). En principe, ces données ne doivent en aucun cas être exploitées à des fins commerciales, sauf respect de toutes les exigences requises par la loi (consentement exprès de la personne concernée, respect des principes de loyauté, proportionnalité, pertinence et caractère non excessif des données, obligation de sécurité et conservation limitée)⁷.
- de même, tout recoupement d'informations ou enrichissement d'un profil émanant de sources autres que l'internaute lui-même doit être soumis au consentement exprès de l'intéressé.

La CNIL et les autorités européennes⁸ préconisent un principe de consentement exprès (opt-in) à la collecte de données et à leur utilisation à des fins de publicité comportementale. Toutefois, la CNIL reconnaît le caractère illusoire de ce principe, susceptible de freiner les possibilités de traçage des internautes et donc le développement de ce modèle publicitaire.

1.3 Obligation de sécurité et conservation limitée des données

Etant donné la richesse des informations résultant des activités de profilage, toute faille de sécurité peut s'avérer extrêmement préjudiciable à l'internaute. Il est donc indispensable de veiller à prendre toutes précautions utiles pour préserver la sécurité des données aussi bien au moment de leur collecte que de leur traitement, afin qu'elles ne soient pas déformées, endommagées, ou que des tiers non autorisés y aient accès. Il s'agit là d'une obligation légale : en cas de défaillance, la responsabilité de l'entité ayant collecté et traité les données pourra être engagée.

A cet égard, il est intéressant de noter quelques similarités dans les mesures préconisées en Europe et aux Etats-Unis :

- Tout comme la réglementation européenne, la FTC recommande la mise en place de mesures de sécurité « *en fonction de la sensibilité des données, de la nature de l'activité de la société, des types de risques auxquels elle peut être confrontée et les moyens raisonnables de protection qui lui sont accessibles* ».
- Tout comme la législation de nombreux Etats américains, le G29 souligne l'importance d'informer toutes les personnes concernées, lorsque leurs données personnelles sont compromises ou risquent de l'être⁹. Egalement en projet, l'obligation de notifier toute faille de sécurité à la CNIL afin de compléter le dispositif actuel.

L'obligation de limiter la durée de conservation participe aussi à la politique de sécurité des données. Les données collectées à des fins de publicité comportementale devront donc être conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui ne doit pas excéder la durée nécessaire à la finalité commerciale recherchée.

⁷ Avis du Groupe 29 du 12 juin 2009 sur les réseaux sociaux.

⁸ Procédure d'infraction de la Commission Européenne contre le Royaume-Uni pour l'utilisation par des fournisseurs d'accès à Internet d'un outil de ciblage comportemental à l'insu des internautes.

⁹ Avis du G29 du 15 mai 2008 sur la révision de la Directive vie privée et communication électronique.

Dans son avis du 4 avril 2008, le G29 rappelle que la conservation des données personnelles et le délai correspondant doivent toujours être justifiés et réduits au minimum, pour plus de transparence et pour garantir la légitimité et la proportionnalité du traitement avec sa finalité. Pour les délais supérieurs à 6 mois, les professionnels doivent démontrer que celui-ci est strictement nécessaire au service.

Ainsi des méthodes d'anonymisation doivent être mises en œuvre de manière effective au-delà de la durée de 6 mois ainsi préconisée.

Si les principes fondateurs ainsi évoqués sont toujours d'actualité en matière de ciblage comportemental, force est de constater que l'évolution du comportement de l'internaute nécessite des adaptations dans la manière d'appréhender ces principes.

2. Promouvoir une démarche permettant une meilleure maîtrise individuelle des données personnelles

2.1 Une adaptation nécessaire à l'évolution du comportement des internautes

Le développement du ciblage comportemental permet de dégager les grandes tendances économiques (enjeux financiers, besoins de consommation) propres à chacun des protagonistes concernés¹⁰ :

- Les consommateurs sont demandeurs d'une reconnaissance accrue et d'une meilleure compréhension de la part des professionnels de leurs besoins réels.

Le développement des réseaux sociaux et blogs témoigne ainsi de la volonté de dévoiler des données privatives et de les partager avec son cercle de connaissances. Il en résulte sur le plan économique une croissance du SIM (Social Influence Marketing) : le consommateur est influencé par les choix des personnes de son réseau, la recommandation d'un proche demeure un facteur clé d'incitation à l'achat.

Une étude menée sur une population internationale de 13-30 ans révèle que 50% des jeunes consommateurs sont parfaitement disposés à livrer des informations sur leur vie privée dans le but d'obtenir un produit répondant à leurs besoins¹¹.

- Pour les fournisseurs, la préoccupation est de singulariser l'internaute en traçant son comportement. L'atout du ciblage comportemental serait ainsi de fournir aux internautes des messages marketing plus élaborés et qualitatifs (en fonction des besoins, goûts et centres d'intérêts exprimés à travers des profils explicites ou prédictifs) au détriment de bannières publicitaires polluantes.

Face à cette évolution du comportement d'achat, il importe donc de donner une marge de manœuvre plus importante à l'internaute dans sa stratégie d'achat (quand, comment et quelles données fournir), ce qui suppose une plus grande transparence à son égard.

¹⁰ Rapport de la Commission Européenne du 5 mars 2009 (« *Data collection, Targeting and Profiling of Consumers for Commercial Purposes in Online Environments* »), §4.4.

¹¹ Le nouveau paysage des données personnelles: quelles conséquences sur les droits des individus ? – FING Identités actives.net.

2.2 Les moyens permettant à l'internaute d'influer sur l'utilisation de ses données

Les réflexions en cours au niveau européen ou même international mettent l'accent sur la nécessité pour le responsable de traitement, qu'il soit fournisseur de contenus, régie publicitaire ou annonceur, de mettre en œuvre des technologies plus respectueuses de la protection des données des internautes.

2.2.1 Le droit pour l'internaute de fournir ses données selon les usages recherchés

Il est encore possible dans le monde physique de faire les boutiques, flâner ou effectuer des achats sans pour autant s'identifier et laisser des traces. Transposés au monde numérique, les mêmes actes sur Internet résultant de la navigation de l'internaute sont enregistrés pour être exploités à des fins commerciales.

Or la personnalisation d'un service ne nécessite pas toujours d'identifier l'internaute. Ainsi, il est possible de se contenter d'une connaissance des habitudes d'achat sans pour autant avoir d'information sur le nom ou l'adresse de l'internaute. Les « cookies traceurs » ou les « cartes de fidélité blanche » qui tracent les achats d'un client sans l'identifier en témoignent¹².

Selon les usages, l'internaute bénéficie des options suivantes : (i) utiliser un pseudonyme sans recoupement avec l'état civil (par exemple pour émettre des critiques sur un bien), (ii) recourir à l'anonymisation lorsque le service ne requiert pas d'identification ou (iii) s'identifier lorsque le service nécessite un certain niveau d'identification (notamment en cas de livraison à domicile).

Pour opérer un choix éclairé, il importe d'informer l'internaute en toute transparence non seulement sur les conditions de collecte de ses données à des fins de ciblage comportemental avec l'option de s'y opposer, mais également sur les moyens de dissimuler ses habitudes de navigation (vider le cache, rejeter les cookies inutiles, lire la charte de protection des données personnelles, etc.).

2.2.2 Une meilleure information sur les outils permettant de protéger sa vie privée

L'inefficacité des chartes de protection des données impose une approche plus proactive de l'information de l'internaute en amont :

- par une information contextuelle claire et complète dès la collecte des données, laquelle a le mérite d'être pédagogique, accessible à tous et davantage lue. Il s'agit de favoriser une plus grande transparence et interactivité des notices d'information avec l'internaute en jouant sur leur présentation et affichage. Cette information préalable servira de guide à l'internaute dans son processus de décision (identification, anonymat, pseudonymat, opposition à la collecte).
- par une information compréhensible sur le fonctionnement des cookies et l'utilisation d'outils de gestion des cookies aux fins de blocage, d'effacement des cookies en fin de session de navigation ou de tri (conserver actifs les seuls cookies renseignés par l'internaute et garder intact ses préférences en matière d'opt-in ou d'opt-out par exemple).
- par une meilleure information sur les solutions comportant des technologies de protection de la vie privée (PETs – Privacy-Enhancing Technologies).

¹² Voir note 11.

L'intérêt de ces solutions (système i-cartes de cardspace, carte électronique sécurisée, projet Higgins, etc.) est de permettre à l'internaute de réaliser une transaction en contrôlant le contenu et le type de données transmises au fournisseur. Ces outils permettront à l'internaute de créer différents profils (anonyme, pseudonyme ou identifiant) que l'internaute peut dévoiler tour à tour selon les usages envisagés.

Fortement encouragée par les autorités européennes et nationales, l'utilisation de ces outils en est encore à ses balbutiements et l'information s'y rapportant pratiquement inexistante.

Des projets sont en cours afin de tester l'accueil de ces outils par les usagers : il résulterait de leur développement une meilleure information de l'internaute sur l'usage de ses données ainsi qu'une meilleure maîtrise des attributs qu'il choisira de divulguer.

En complément de la réglementation applicable se dessinent des initiatives visant à promouvoir les voies de l'autorégulation ou de la labellisation pour offrir des solutions pratiques.

3 Autorégulation et Labellisation

3.1. L'autorégulation ou l'adoption d'une éthique de conduite sectorielle

La voie de l'autorégulation est privilégiée aussi bien par les grandes instances régulatrices, comme la FTC aux États-Unis ou la Commission Européenne et les autorités européennes de protection des données personnelles que les acteurs concernés. Ces efforts de co-régulation sont menés dans l'optique de mettre en place de règles plus adaptées et de prendre un certain nombre d'engagements fermes.

Des codes de conduite sont en cours de rédaction, dont l'objet est de veiller notamment au respect des intérêts des consommateurs les plus vulnérables comme les mineurs ou encore à l'exclusion de collecte des données sensibles au titre de la publicité ciblée.

Dans son étude, la CNIL insiste sur la nécessité pour les sites Internet de mettre en place des pratiques transparentes et respectueuses des droits des personnes. Afin d'améliorer la qualité de l'information des internautes, l'adoption de codes de bonnes pratiques par les professionnels ainsi que l'insertion de mentions types rédigées par la CNIL pourraient être envisagées. La CNIL met également l'accent sur les mesures de sensibilisation et d'accompagnement des internautes en préconisant le développement en ligne d'outils pédagogiques sous la forme de conseils pratiques. L'idée de coordonner ses efforts aux côtés d'autres associations, telle que le Forum des droits sur l'Internet, est avancée par la CNIL pour toucher le plus grand nombre.

En Grande-Bretagne, l'*Internet Advertising Bureau* (« IAB ») a publié en mars 2009 un ensemble de principes et bonnes pratiques (« Principes ») en matière de ciblage comportemental en ligne à destination des membres signataires professionnels.¹³ Ces Principes autorégulateurs, ayant vocation à compléter ou suppléer les dispositions applicables de droit anglais, seront mis en œuvre à compter du 4 septembre 2009. Ils s'articulent autour de (i) l'information claire et non équivoque des internautes sur la collecte et l'utilisation de leurs données, (ii) le consentement préalable de l'internaute, et (iii) l'accès aux informations utiles afin de sensibiliser l'internaute sur ces pratiques publicitaires. En outre, les enfants âgés de moins de 13 ans sont exclus comme cible.

¹³ IAB Good Practice Principles for Online Behavioural Advertising(www.iabuk.net)

3.2. *La labellisation ou la transparence vis-à-vis des internautes*

La labellisation des produits ou services est non seulement un gage de confiance pour l'internaute dans les modalités de collecte et traitement de ses données personnelles, mais également un véritable facteur d'amélioration de l'image de l'entreprise concernée dans un univers fortement compétitif où chacun des protagonistes est soucieux des effets liés aux politiques de communication en place.

En France, si la CNIL dispose d'un pouvoir de labellisation depuis 2004, son exercice reste soumis à la mise en œuvre de mesures réglementaires d'application.

La Commission Européenne s'est engagée depuis 2007 dans un projet de certification intitulé EuroPrise ou « European Privacy Seal » fondé sur le succès remporté par un modèle de certification régional allemand¹⁴. Ce label repose sur l'évaluation de produits ou services rendue par un collège d'experts en droit et nouvelles technologies, et la validation d'un rapport. La délivrance d'un label atteste de leur qualité en termes de protection des données personnelles. Ce label est remis par un corps indépendant composé par les autorités de protection des données personnelles de 9 États Membres, y compris la CNIL.

L'apposition de ce label permet aux entreprises de témoigner auprès des internautes de leurs agissements en conformité avec les principes édictés par les directives européennes en la matière. Il s'agit également d'un remarquable outil de communication commerciale pour capter la confiance des consommateurs. La régie publicitaire WunderLoop, spécialisée dans la publicité comportementale, a obtenu la certification EuroPrise pour la protection des données personnelles en septembre 2008¹⁵.

Pour identifier les segments des utilisateurs, celle-ci utilise les données associées au surf des utilisateurs (requêtes saisies, liens cliqués) et les informations issues des opt-in selon les normes EuroPrise (uniquement les données déclaratives non personnelles, ce qui exclut l'adresse IP, le nom, l'adresse, etc).¹⁶

Les efforts menés dans une optique d'autorégulation et de labellisation traduisent une réelle prise de conscience des acteurs concernés et des autorités de régulation nationales dans la mise en œuvre du ciblage comportemental.

Néanmoins, les exemples suivants montrent que cette prise de conscience reste limitée :

- malgré la priorité donnée à la voie de l'autorégulation, la FTC vient de lancer un dernier avertissement à certains acteurs de l'Internet afin qu'ils informent de façon adéquate les consommateurs de leurs nouvelles pratiques, à défaut de quoi il reviendra au législateur d'imposer ses règles d'application contraignante¹⁷.
- le 14 avril 2009, consécutivement à des plaintes d'internautes britanniques, la Commission Européenne a ouvert une procédure d'infraction à l'encontre du Royaume-Uni concernant

¹⁴ Il s'agit du modèle de certification intitulé « Gütesiegel » mis en œuvre dans l'Etat de Schleswig-Holstein en République Fédérale d'Allemagne.

¹⁵ Journal du Net, Wunderloop certifié pour la protection de ses données, 25 septembre 2008 (<http://www.journaldunet.com/breve/international/31751/wunderloop-certifie-pour-la-protection-des-donnees.shtml>)

¹⁶ Zdnet, E-Marketing 2009 : La publicité sera comportementale ou ne sera pas !, 27 janvier 2009

(<http://www.zdnet.fr/blogs/2009/01/27/e-marketing-2009-publicite-comportementale-online-multi-canal/>)

¹⁷ Article du 27 avril 2009 intitulé « FTC says Internet firms near 'last chance' ». Source : Reuters.

l'utilisation d'une technologie de publicité comportementale « *Phorm* »¹⁸ allant à l'encontre des règles communautaires de confidentialité des communications électroniques qui interdisent leur interception et leur surveillance sans le consentement de l'internaute¹⁹.

Conclusion

Face aux nombreux enjeux et risques soulevés par le ciblage comportemental, les organes représentatifs des professionnels du secteur et les instances régulatrices sont encouragés à adapter le cadre juridique actuel pour le rendre plus souple et réactif. Sont ainsi prises en compte les nouvelles technologies permettant une meilleure maîtrise des données et les bonnes pratiques issues des démarches d'autorégulation et de labellisation.

Ces adaptations supposent que les professionnels jouent également le jeu en veillant à respecter le cadre juridique en place par des engagements fermes qui permettent de rassurer l'internaute face aux risques soulevés par des pratiques publicitaires qui s'affinent et des enjeux juridiques qui se complexifient.

Denise Lebeau-Marianna** & Eve-Christie Vermynck** Avocats à la Cour
Département Technologie de l'Information et de la Communication Baker & McKenzie

*** Nous remercions nos confrères européens pour leur participation à cette analyse comparée : Robert Boekhorst (Pays-Bas), Alexander Haines (Allemagne), Norman Heckh (Espagne), Steve Holmes (Royaume-Uni) et Tomasz Koryzma (Pologne)*

¹⁸ « Cette technologie permet d'analyser de manière constante les habitudes de navigation des internautes afin de déterminer leurs intérêts et de leur présenter des publicités ciblées lorsqu'ils consultent certains sites Internet » (Définition donnée par la Commission Européenne dans son article).

¹⁹ Article publié le 14 avril 2009 sur le site officiel de la Commission Européenne intitulé « Télécommunications : la Commission ouvre une procédure d'infraction à l'encontre du Royaume-Uni au sujet de la protection de la vie privée et des données à caractère personnel ».