

8 Publicité ciblée et protection du consommateur en France, en Europe et aux États-Unis

Winston J. MAXWELL Thomas ZEGGANE et Sarah JACQUIER,

avocats chez Hogan & Hartson MNP

Principal mode de financement de l'Internet, la publicité tend à être ciblée pour être « au plus près » des goûts du consommateur. Elle présente alors des risques sur le plan des libertés et de la vie privée en ce qu'elle implique la collecte d'informations personnelles relatives au consommateur. Les autorités françaises, européennes et américaines, largement alertées sur la question des risques posés pour le consommateur et d'autant plus vigilantes que l'Internet est aujourd'hui généralisé, adoptent ou recommandent des mesures pour la protection du consommateur. Un consensus n'existe toutefois pas toujours entre ces autorités.

1 - Sans les revenus publicitaires, des outils formidables comme Google ou DailyMotion n'existeraient pas ou seraient payants. Qu'il s'agisse de moteurs de recherche, de sites communautaires ou d'autres services de l'Internet, tous ont pour mode de financement essentiel à ce jour les revenus publicitaires.

2 - Sur Internet, les annonceurs sont d'autant plus disposés à payer le prix fort que la publicité peut viser juste et précis : la publicité doit pouvoir toucher sa cible et s'afficher sur l'écran des personnes remplissant les caractéristiques définies à l'avance par l'annonceur.

3 - La publicité ciblée en ligne (« online behavioral advertising ») est permise par la collecte d'informations relatives au comportement du consommateur en ligne. Sa finalité est de délivrer des messages personnalisés en fonction des centres d'intérêts de l'internaute.

4 - Cette technologie commence à inquiéter les autorités françaises, européennes et américaines.

À côté des avantages pour l'internaute (une publicité ciblée, *a priori*, proche de ses goûts et intérêts), des menaces sur le plan des libertés et du respect de la vie privée de l'internaute sont également pressenties. À quelques mois d'intervalle, la Federal Trade Commission, l'agence Européenne pour la sécurité des réseaux ENISA, et le Groupe de travail Article 29 sur la protection des données (« Groupe Article 29 ») se sont intéressés à la publicité ciblée sous l'angle de la protection du consommateur. Leurs conclusions convergent sur plusieurs points : une meilleure information du consommateur sur les risques associés à la divulgation d'informations personnelles en ligne est nécessaire ; de meilleurs outils doivent être mis à la disposition du consommateur pour lui permettre de contrôler son environnement numérique et maîtriser le partage de données à caractère personnel. Quelques divergences existent entre les approches européennes et américaines, notamment sur la nature d'une adresse IP : est-ce une donnée à caractère personnel ? L'objectif de cet article est d'examiner les risques qui ont retenu l'attention des autorités américaines, européennes et françaises ainsi que les solutions préconisées.

1. Pratiques en matière de publicité ciblée

5 - La publicité en ligne peut prendre diverses formes telles que les bannières publicitaires, des *skycrapers* (qui sont des bannières

publicitaires consistant en une colonne disposée sur la hauteur de l'écran d'une taille de 120 × 600 ou 160 × 600 pixels, selon les standards préconisés par l'Interactive Advertising Bureau), des hyperliens, des liens contextuels (liens ciblés en fonction de la thématique de la page), des liens sponsorisés apparaissant en tête des pages de résultats de moteurs de recherche ou des *pops-up* (qui sont des fenêtres publicitaires apparaissant d'elles-mêmes en utilisant le système d'exploitation des logiciels) ¹.

6 - Ces modes de publicités sont d'autant plus efficaces pour les annonceurs qu'ils sont ciblés. Pour cela, la publicité doit pouvoir s'appuyer sur des données collectées « au plus près » de l'internaute. La question est alors de savoir quel degré de proximité est permis.

2. Données anonymes ou données à caractère personnel

7 - Les risques pour le consommateur naissent quand les données collectées pour la publicité se rattachent trop directement à lui.

8 - Dès lors que la publicité ciblée repose sur des goûts et comportements qui ne peuvent être rattachés à un individu déterminé, la publicité ne pose pas de danger en termes de protection des libertés individuelles. En revanche, les libertés individuelles peuvent être en danger dès lors que les données collectées sur les goûts et comportements peuvent être rattachées à un individu déterminé ou déterminable. Pour chaque type de données utilisées à des fins de publicité, la question est alors de savoir si les données collectées peuvent être considérées comme des données pouvant être rattachées à un individu déterminé ou déterminable ou si elles sont des données anonymes. Les données anonymes peuvent recouvrir des données sur des catégories de personnes et les comportements de ces catégories de personnes (ex : requêtes d'information sur des sujets sportifs faites par les jeunes hommes de 25 ans).

9 - Les États-Unis et les États-membres de l'Union européenne n'utilisent pas la même terminologie pour qualifier les données pouvant être rattachées à un individu déterminé ou déterminable.

1. V. M. et J.-P. Jean-Baptiste, *Le marketing on line, guide pratique et juridique* : Eyrolles 2008

10 - Aux États-Unis, on parle « d'information personnellement identifiable » ou « d'information personnelle » (ensemble « IPI »). La directive n° 95/46/CE et la loi du 6 janvier 1978 utilisent le terme de « donnée à caractère personnel ». Plusieurs définitions coexistent au sein de législations spécifiques. En matière de protection de l'enfance, le « *Children's Online Privacy Protection Act* » de 1998 (« COPPA ») définit une IPI comme : « *une information individuellement identifiable à propos d'une personne collectée en ligne, y compris ses nom et prénom ; son domicile ou une adresse physique, y compris le nom d'une rue et d'une ville ou village ; une adresse de courrier électronique ; un numéro de téléphone ; un numéro de sécurité sociale ; tout autre identifiant que la Federal Trade Commission estime susceptible de permettre un contact physique ou virtuel avec une personne spécifique ; ou une information relative à un enfant ou aux parents de cet enfant que le site Internet collecte en ligne qui sont combinées à un identifiant mentionné ci-dessus* ».

11 - En France, on parle de « donnée à caractère personnel ». L'article 2 de la loi du 6 janvier 1978 dispose : « *Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* ».

12 - Au-delà de la différence sémantique, le point d'achoppement porte sur la question de savoir dans quelle mesure des données peuvent être rattachées de manière indirecte à une personne déterminée. Les débats relatifs à la qualification de l'adresse IP illustrent la complexité du débat.

A. - Difficulté de reconnaître une donnée rattachable à un individu : exemple de l'adresse IP

13 - Aux États-Unis, une adresse IP n'est pas considérée en soi comme une IPI. Ce n'est que dans la mesure où un identifiant personnel s'ajoute à cette adresse IP que le régime protecteur des données à caractère personnel s'appliquera.

14 - En droit européen, la plupart des autorités de protection des données considèrent que les adresses IP, en elles-mêmes, constituent des données à caractère personnel. L'idée est la suivante : il est possible, après des démarches judiciaires, d'identifier l'ordinateur qui a utilisé une adresse IP à un moment donné. Or, derrière l'ordinateur, se trouve l'abonné d'un fournisseur d'accès, et donc une personne déterminée. Certes, l'abonné peut ne pas être celui qui a utilisé la connexion permise par son abonnement (par exemple, parce qu'il aura prêté son ordinateur ou parce que l'abonné est une société mettant à disposition de plusieurs salariés une adresse IP). Cependant, la probabilité est quand même forte que l'abonné soit celui qui utilise la connexion Internet ou que, à défaut, il connaisse l'identité de celui qui utilise cette connexion.

15 - Dans un avis (n° 4/2007, 20 juin 2007) sur le concept de donnée à caractère personnel, le Groupe Article 29 a expliqué que la notion de donnée à caractère personnel est rattachée à l'existence de moyens raisonnables permettant d'associer ces données à une personne identifiée. Or, dans un environnement en ligne tel que l'Internet, il est possible dans la majorité des cas d'identifier un ordinateur à partir d'une adresse IP, bien que cela requière la coopération des fournisseurs d'accès Internet et des autorités judiciaires. Une question est donc de savoir si ce besoin de coopération des autorités judiciaires fait perdre l'adresse IP, prise de manière isolée, sa qualification de donnée à caractère personnel².

B. - Anonymisation et pseudonymisation : moyen de décorrélérer l'individu et la donnée

16 - La pseudonymisation est un procédé permettant de dissimuler l'identité de l'utilisateur tout en collectant des données permettant de remonter plus tard à cette identité. La pseudonymisation est souvent utilisée dans des essais cliniques. L'identité réelle du patient est gardée secrète mais peut être retrouvée en cas de besoin. À l'opposé, le terme anonymisation renvoie à un traitement en vertu duquel des données « *sont rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable* »³, de manière définitive.

17 - Dans son avis sur les moteurs de recherche, le Groupe Article 29 marque sa préférence pour l'anonymisation des données⁴. Il estime que le procédé doit être « *totale et irréversible* »⁵ pour que la Directive 95/46/CE cesse d'être applicable à un tel traitement. Le Groupe Article 29 prend acte d'une pratique de certains moteurs de recherche supprimant les quatre derniers chiffres d'une adresse IP, mais considère que « *cela n'est pas nécessairement suffisant pour garantir l'anonymisation* »⁶.

18 - De manière générale, il faut retenir que l'anonymisation des données ne sera admise que de façon restrictive.

3. Comment assurer la protection du consommateur ?

19 - La protection du consommateur passe par un ensemble de mesures allant de l'information du consommateur jusqu'au recueil de son consentement explicite et éclairé ou encore l'interdiction de traiter certains types de données.

A. - Information de l'utilisateur

20 - Pour faire un choix éclairé, le consommateur doit comprendre l'usage réel qui est fait des données le concernant, que ces données soient fournies par lui de sa propre initiative (par exemple sur son profil sur un site communautaire) ou collectées sans intervention de sa part (par exemple par un moteur de recherche).

21 - Cette information est particulièrement importante en cas de regroupement d'informations portant sur une même personne. Le Groupe Article 29 considère à propos des moteurs de recherche que : « *en récupérant et regroupant des informations éparses et variées sur une même personne, les moteurs de recherche peuvent créer une représentation potentiellement plus dommageable pour la personne concernée que si chaque donnée mise en ligne demeure distincte* »⁷.

22 - Déjà, la Directive n° 2002/58/CE dite « Vie privée et communications électroniques » prévoyait des dispositions relatives à la collecte de données sur Internet et au besoin d'information corrélatif de l'internaute. Les fournisseurs de services de communications électroniques sont tenus d'informer l'utilisateur de la mise en place de témoins de connexions, les « cookies », qui collectent des informations relatives au comportement de l'utilisateur. L'information fournie doit être « *claire et complète* »⁸ quant à la finalité du traitement de données et la possibilité pour l'utilisateur de refuser le traitement (« opt-out »).

23 - De manière générale, la publicité en ligne doit être loyale et véridique, et les mentions lisibles et compréhensibles pour l'internaute. En France, le Code des pratiques loyales en matière de publicité de la chambre de commerce internationale (CCI) contient bon nombre de recommandations visant à assurer une parfaite

3. Cons. CE et Parlement, dir. n° 95/46/CE, 24 oct. 1995, consid. 26

4. Avis du Groupe Article 29 sur les moteurs de recherche, 4 avr. 2008, p. 18

5. *Idem*, p. 20

6. *Idem*

7. *Idem*, p. 5

8. Cons. CE et Parlement, dir. 2002/58/CE, 12 juill. 2002, art. 5.3

2. Sur cette question, V. CA Paris, 27 avr. et 15 mai 2007 : *legalis.net*

compréhension par le consommateur de la nature et du contenu du message publicitaire (exemple : ce code contient des recommandations en termes de durée d'exposition et de taille des caractères en fonction du format de la publicité).

24 - Récemment modifié par la loi n° 2008-3 du 3 janvier 2008, l'article L. 121-1 du Code de la consommation considère comme une pratique commerciale trompeuse la publicité qui repose sur des indications fausses ou de nature à induire en erreur et portant sur les caractéristiques essentielles d'un service ou sur le procédé mis en œuvre dans le cadre de la prestation de service.

25 - L'article L. 121-1, II du Code de la consommation proscribit l'omission d'information ou la fourniture d'informations substantielles « de façon inintelligible, ambiguë ou à contretemps ». En clair, cette disposition peut remettre en cause la validité des conditions générales d'utilisation des sites communautaires qui sont lues seulement – si jamais elles sont lues – au moment de l'inscription de l'internaute au site. Cela signifierait qu'une information claire et efficace du consommateur devrait s'ajouter à celle fournie par les conditions générales du site et devrait être présentée au moment où elle serait la plus pertinente (par exemple, au moment où l'internaute souscrit à un nouveau service ou décide de changer la politique d'accès à ses données par les autres internautes).

26 - À noter que ce devoir d'information à l'égard du consommateur s'applique même si le service est gratuit pour le consommateur. En effet, le droit de la consommation s'applique dès lors qu'est en cause une relation professionnel/consommateur, et ce indépendamment du point de savoir si un prix est versé ou non. À titre d'exemple, la Commission des clauses abusives en France n'hésite pas à interdire des clauses jugées non conformes au droit de la consommation stipulées dans le cadre de contrats d'accès à Internet gratuits⁹.

27 - De l'avis de plusieurs organismes français, internationaux et américains, les moteurs de recherche et sites Internet ne satisfont encore que de manière incomplète aux exigences de clarté et d'intelligibilité des mentions et publicités pour les internautes.

28 - Le rapport ENISA juge que les informations fournies par certains sites communautaires sont insuffisantes : « L'utilisateur n'a pas toujours conscience de l'ampleur de l'audience ayant accès au contenu qu'il divulgue. L'apparence d'intimité résultant de l'entourage d'« amis » donne souvent lieu à des révélations inopportunes ou dommageables »¹⁰. Par ailleurs, l'ENISA recommande des campagnes de sensibilisation et d'éducation de l'opinion à l'usage des sites communautaires, ainsi que la fourniture d'informations contextuelles au sein de la structure même des sites afin d'éduquer les utilisateurs en temps réel. L'ENISA encourage par ailleurs les sites communautaires à adopter les configurations par défaut les plus sûres possibles et à les accompagner de guides pédagogiques plutôt que des conditions générales souvent rébarbatives et difficilement compréhensibles.

29 - Le Groupe Article 29 adresse des observations et des recommandations similaires dans son avis concernant les moteurs de recherche : « la plupart des utilisateurs internet n'ont pas conscience de la quantité significative des données relatives aux comportements lors des recherches qui font l'objet d'un traitement et des finalités de ce traitement »¹¹. Le Groupe Article 29 estime également que les moteurs de recherche de manière générale ne fournissent pas une vue d'ensemble complète des différentes finalités pour lesquelles sont mis en place des traitements de données. Il juge que des finalités telles que « l'amélioration du service » ou « l'offre de publicité personnalisée » sont « définies de façon trop large pour permettre d'apprécier de manière satisfaisante la légi-

imité d'une telle finalité »¹². Enfin, du fait que le réglage par défaut des navigateurs Internet autorise le plus souvent la mise en place de cookies, le Groupe Article 29 affirme que « l'information devrait être mise en avant de manière plus importante qu'une simple inclusion dans la politique de confidentialité d'un moteur de recherche qui n'est pas immédiatement apparente »¹³.

30 - Aux États-Unis, la FTC recommande que chaque site internet qui procède à la collecte de données à des fins de publicité ciblée fournisse une déclaration claire, concise et conviviale précisant que « des données relatives à l'activité du consommateur sur Internet sont collectées sur ce site afin de fournir des publicités ciblées de produits et services personnalisés en fonction des intérêts de chaque consommateur »¹⁴.

31 - En pratique, les sites communautaires majeurs proposent des « outils de management de l'identité et de contrôle d'accès pour le contenu créé par l'utilisateur, permettant à ce dernier de contrôler son audience (ce que les blogs ne permettent pas par exemple) »¹⁵. Ces outils sophistiqués contribuent à une meilleure protection de la vie privée par rapport à des sites internet traditionnels et permettent aux utilisateurs de contrôler réellement les données le concernant.

B. - Recueil du consentement de l'utilisateur

32 - « La publicité au moyen de pop-up est à la navigation sur Internet ce que le spam est à l'e-mail » a déclaré le président d'Overstock, société de commerce en ligne¹⁶.

33 - Or, on sait qu'en vertu de l'article 13, § 1 de la Directive 2002/58/CE dite « Vie privée et communications électroniques », l'envoi de courriers électroniques à des fins de prospection directe est soumis au principe de l'opt-in (c'est-à-dire qu'un consentement préalable de l'internaute est requis)¹⁷. En droit français, le principe de l'opt-in pour des courriers électroniques à des fins de prospection directe est consacré dans des termes très similaires à l'article L. 34-5 du Code des postes et communications électroniques.

34 - Faudrait-il dès lors soumettre les *pops-up* au principe de l'opt-in ? En l'état du droit européen, répondre par l'affirmative à cette question suppose de qualifier le *pop-up* de courrier électronique. Interrogée dans le cadre d'une question écrite, la Commission européenne a répondu par la négative, considérant que la définition de courrier électronique donnée par la Directive « Vie privée et communications électroniques » « ne couvre que les messages pouvant être stockés dans un équipement terminal jusqu'à ce qu'ils soient relevés par leur destinataire. Les messages qui s'affichent quand le destinataire est en ligne et disparaissent quand ce n'est pas le cas ne sont pas couverts par la définition du courrier électronique »¹⁸. Rappelons que la Directive « Vie privée et communications électroniques » définit le courrier électronique comme « tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère »¹⁹.

12. *Idem*, p. 16

13. *Idem*, p. 20

14. FTC, communiqué sur la publicité ciblée, p. 3 : <http://www.ftc.gov/opa/2007/12/principles.shtml>

15. Rapp. ENISA, p. 6

16. Propos reproduits par M. et P. Jean-Baptiste dans leur ouvrage « marketing en ligne » : Eyrolles

17. Cons. CE et Parlement, dir. n° 2002/58/CE, préc., art. 13, § 1 : « l'utilisation de systèmes automatisés d'appel sans intervention humaine (automates d'appel), de télécopieurs ou de courrier électronique à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable ».

18. Quest. écrite A. Thors, n° E-3392/02 à la Commission sur les fenêtres publicitaires indésirables dans Windows et protection des données personnelles au sein des réseaux de télécommunication.

19. Dir. n° 2002/58, préc., art. 2, h. La définition donnée par le droit français du courrier électronique est quasi identique (définition introduite par l'article 1 de la loi n° 2004-575 sur la confiance dans l'économie numérique).

9. Recommandation n° 03-01, 31 janv. 2003

10. ENISA Position Paper n° 1 « security issues and recommendations for Online social network : Giles Hogben, oct. 2007 (traduction libre), p. 6

11. Avis du Groupe, Article 29 sur les moteurs de recherche, p. 22

35 - Toutefois, en Allemagne, le tribunal régional de Dusseldorf a jugé illicite la pratique de *pop-up* non autorisée au préalable par l'internaute²⁰. Pour ce faire, il a considéré que cette pratique était dans une certaine mesure comparable au spam²¹. La condamnation s'est fondée sur le droit de la concurrence, le tribunal considérant que le *pop-up* constituait une pratique immorale favorisant les entreprises qui y recourent au détriment de celles qui s'obligent à obtenir l'accord de l'internaute avant l'envoi de publicité. Dans le même sens, en Belgique, une proposition de loi du 12 juillet 2007 vise à soumettre les *pops-up* au régime de l'*opt-in*. Pour ce faire, les parlementaires expliquent que les *pops-up* rentrent dans la notion de « communications non sollicitées » visée au § 3 de l'article 13 de la Directive « Vie privée et communications électroniques » (cette notion de communications non sollicitées étant jugée plus large que celle de courrier électronique²²). Et ils proposent, comme les y autorise la Directive, de soumettre ces communications non sollicitées au principe de l'*opt-in*.

36 - Dans les cas où le législateur entend réserver la possibilité à l'internaute de refuser une pratique (on est alors dans le cadre d'un « *opt-out* » et non plus d'un *opt-in* car un consentement n'est pas requis), la FTC recommande que les sites Internet proposent au consommateur une « méthode claire, accessible et facile d'utilisation pour mettre en œuvre l'*opt-out* »²³. Cette recommandation va dans le même sens que la réglementation européenne applicable aux *cookies* aux termes de laquelle les utilisateurs doivent être informés de façon claire de l'utilisation de *cookies* et de la possibilité de refuser un tel traitement.

37 - Conformément à la législation européenne, les fournisseurs de services de communications électroniques peuvent conditionner l'accès au service à l'acceptation « en pleine connaissance de cause »²⁴ d'un *cookie* ou d'un dispositif analogue si celui-ci est utilisé à des fins légitimes. Le consentement peut être donné « selon toute modalité appropriée permettant à l'utilisateur d'indiquer ses souhaits librement, de manière spécifique et informée, y compris en cochant une case lorsqu'il visite un site Internet »²⁵.

38 - Dans son avis sur les moteurs de recherche, le Groupe Article 29 affirme que les informations relatives aux recherches sont le plus souvent stockées dans des *cookies* persistants dont la durée peut dépasser plusieurs années sans que l'utilisateur en ait parfaitement conscience notamment du fait du réglage par défaut de son navigateur. En conséquence, le Groupe Article 29 refuse que « la responsabilité pour ces traitements de données soit réduite à la responsabilité pour l'utilisateur de prendre les précautions nécessaires dans la configuration de son navigateur »²⁶.

39 - Il n'est pas certain que le dispositif légal européen relatif aux *cookies* soit applicable en l'état aux outils de traçage des sites communautaires comme il peut l'être pour les moteurs de recherche. Il apparaît cependant clair que les autorités américaines comme européennes entendent que l'utilisateur ait la possibilité de s'exprimer de manière spécifique quant à l'utilisation de données dans le cadre de la publicité ciblée. Dans le futur, cela pourrait vouloir dire que l'utilisateur doit avoir l'opportunité de refuser le traitement (*opt-out*) en cochant une case spéciale.

20. Décis. 26 mars 2003, en l'espèce, une succession de *pops-up* empêchait l'internaute de quitter le site web concerné sans devoir fermer avant le système d'exploitation.

21. Une différence est toutefois relevée par le tribunal dans le sens où, dans le cadre des *pops-up*, l'internaute s'est initialement délibérément rendu sur le site concerné, ce qui ne se produit pas dans le cadre de *spams*.

22. Par « communication », la directive vise « toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public ».

23. FTC, communiqué, p. 3

24. Dir. n° 2002/58/CE, consid. 25

25. Dir. n° 2002/58/CE, consid. 17

26. Avis du Groupe Article 29 sur les moteurs de recherche, p. 20

C. - Données sensibles

40 - La loi du 6 janvier 1978 définit les données sensibles comme les « données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci »²⁷. Les définitions de la FTC en la matière sont plus floues, l'autorité souhaitant encore recueillir des commentaires sur le type de données qui devrait être qualifié de sensible.

41 - La loi française pose le principe de l'interdiction de la collecte de données sensibles. Des exceptions sont prévues quand la finalité du traitement exige une telle collecte, mais les modalités de mise en œuvre d'un tel traitement sont soumises au contrôle strict de la CNIL.

42 - La FTC étudie actuellement l'opportunité d'imposer un consentement exprès du consommateur ou même d'interdire entièrement l'utilisation de données sensibles dans le cadre de publicités ciblées. La FTC a cependant noté que dans certaines hypothèses, les consommateurs pourraient apprécier de recevoir des publicités ciblées relatives, entre autres à des problèmes de santé, dans la mesure où ces consommateurs sont convenablement et préalablement informés d'un tel traitement et peuvent décider de ne pas en autoriser la mise en œuvre.

4. Durée de conservation des données et sécurité de stockage, accès, rectification, et destruction de données

43 - Les modalités selon lesquelles les traitements de données sont mis en œuvre sont essentielles pour garantir la protection du consommateur.

A. - Conservation des données

44 - La FTC recommande que les données utilisées dans le cadre de la publicité ciblée ne soient conservées qu'aussi longtemps qu'il est nécessaire pour répondre légitimement à un besoin commercial ou à une obligation légale. Cela coïncide avec les principes européens en la matière.

45 - L'ENISA a identifié un risque dans le contexte des sites communautaires lié à la difficulté d'effacer totalement un compte : « les utilisateurs désirent effacer leur compte découvrent qu'il est quasiment impossible de retirer les informations secondaires associés à leur profil tel que les commentaires publics présents sur d'autres profils »²⁸. Les sites communautaires tentent de répondre aux inquiétudes des consommateurs. Facebook a modifié sa page d'aide le 11 février dernier et propose dorénavant aux utilisateurs de procéder, à leur demande, à l'effacement permanent de leur compte. Le site ne permet cependant pas à l'utilisateur de procéder à cet effacement d'un simple clic, invoquant le nombre important de réactivations de comptes. Une alternative pourrait être de promouvoir la portabilité des profils, permettant ainsi à l'utilisateur de transférer les informations de son profil vers une autre plateforme.

46 - Pour les moteurs de recherche, le Groupe Article 29 met l'accent sur les risques attachés à la mise en mémoire « cache » de données présentes sur des sites internet et qui peuvent s'avérer erronées ou dommageables en raison de leur persistance sur le site. Il estime que « lorsque la publication originale a été modifiée, par exemple pour retirer des données à caractère personnel erronées, le responsable de la copie cache devrait immédiatement déferer à

27. L. n° 78-17, 6 janv. 1978, art. 8

28. Rapp. ENISA, Threat SN.6, p. 3

toute requête demandant la mise à jour de la copie cache ou le blocage temporaire de cette copie jusqu'à ce que le site Internet soit revisité par le moteur de recherche »²⁹. Il se prononce par ailleurs, dans tous les cas, pour une durée souhaitable de conservation des données qui ne devrait pas dépasser 6 mois.

B. - Sécurité des traitements

47 - La FTC recommande que des mesures de sécurité raisonnables soient prises en matière de publicité ciblée en fonction « de la sensibilité des données, la nature de l'activité de la société, les types de risques auxquels elle doit faire face et les moyens raisonnables de protection qui lui sont accessibles »³⁰. Ce standard est presque identique à la réglementation européenne qui requiert la mise en place de mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel. Le niveau de sécurité doit être adapté aux risques présentés par le traitement et la nature des données à protéger, tout en prenant en considération l'état de l'art et les coûts afférents à son implémentation³¹.

48 - Des dispositions légales spécifiques en matière de failles de sécurité relatives aux données voient le jour tant aux États-Unis qu'en Europe. La Californie a adopté la première loi imposant une obligation de notification en cas de faille de sécurité qui est entrée en vigueur le 1^{er} juillet 2003. Par la suite, près de 39 autres États fédérés ont mis en place des dispositions similaires. En Europe, la Commission a indiqué de façon appuyée sa volonté de mettre en place de telles mesures dès 2006. Une proposition formelle a été présentée par la Commission le 13 novembre 2007 dans le cadre d'une proposition de modification de la directive 2002/58/CE et de la directive 2002/22/CE dite « service universel ».

5. Qui est responsable ?

49 - Le droit européen sur la protection des données à caractère personnel est fondé sur la notion de « responsable du traitement », à savoir la personne qui détermine les finalités et les moyens du traitement de données à caractère personnel. Dans un environnement de sites communautaires ou de moteurs de recherche, la détermination du responsable du traitement ne va pas de soi. Dans son avis sur les moteurs de recherche, le Groupe Article 29 reconnaît la difficulté d'appliquer cette notion à des entités qui sont principalement des « intermédiaires de triage »³². Il estime que les moteurs de recherche agissant purement comme intermédiaire ne peuvent être qualifiés de responsable du traitement que de manière accessoire, l'étendue de leur contrôle se limitant à la possibilité d'effacer les données de leurs serveurs. En revanche, dans le cadre de « services à valeur ajoutée » ou de « vente de publicité ciblée en fonction de données à caractère personnel telles que le nom d'une personne », le Groupe Article 29 estime que les moteurs de recherche sont alors « pleinement responsables en vertu de la réglementation protectrice du contenu résultant du traitement de données »³³.

50 - La situation est différente pour les sites communautaires. Pour ces acteurs, il existe trois sortes de données. **Premièrement** les informations que l'utilisateur fournit au site communautaire dans le cadre de son inscription (telles que les nom et prénom de l'utilisateur et son adresse de courrier électronique). **Ensuite** certaines informations que l'utilisateur fournit à la plateforme sur ses goûts dans le cadre de champs pré-établis (exemple : « j'aime le ski », « mon chanteur préféré est Bob Dylan »). **Enfin**, les données que l'utilisateur met en ligne à sa discrétion et de sa seule initiative sur son profil, telles que des photos de vacances. Pour la première

catégorie de données (données d'inscription), le site communautaire est clairement le responsable du traitement, car c'est le site qui détermine les finalités et les moyens du traitement de ces informations qu'il garde généralement confidentielles.

51 - Pour la deuxième catégorie de données (goûts de l'utilisateur), ces données sont collectées dans l'objectif de faciliter les contacts entre utilisateurs du site ou de les utiliser à des fins de publicité. Pour cette catégorie aussi, on peut dire que le responsable du traitement est le site communautaire lui-même car il influe sur le type de données collectées. Pour la troisième catégorie de données (photos de vacances), le site n'est généralement pas le responsable du traitement, car le site n'a aucun contrôle sur ces informations. Seul l'utilisateur décide avec qui ces informations seront partagées, et, à notre connaissance, le site n'utilise pas ces données pour fournir des services de publicité. Dans le cas contraire (le site analyse et utilise les données fournies par les utilisateurs), leur rôle de responsable du traitement serait établi, à supposer toutefois que les données n'aient pas été anonymisées.

52 - Centrale dans le cadre de la réglementation sur les données personnelles, la question du « responsable du traitement » perd de son importance si la pratique en cause constitue une publicité trompeuse au sens de l'article L. 121-1 du Code de la consommation. La responsabilité du fournisseur du service pourra être retenue s'il est établi qu'il a commis une pratique trompeuse en dissimulant ou en communiquant de manière inintelligible une information substantielle sur le service. Les conditions dans lesquelles les données des internautes peuvent être utilisées à des fins de publicité ciblée pourraient, le cas échéant, être qualifiées d'informations substantielles.

6. Quelle loi s'applique ?

53 - En droit de la consommation, les lois s'appliqueront à toute plateforme visant un public français même si le fournisseur est établi en dehors de la France.

54 - S'agissant de la législation sur les données personnelles, l'applicabilité des lois française et européenne obéit à des règles différentes. La loi applicable est déterminée selon le lieu d'établissement du responsable du traitement. Si le responsable du traitement est établi dans un pays membre de l'Espace économique européen, c'est la loi du pays de l'établissement qui s'appliquera. Le « lieu d'établissement » signifie un lieu où une activité est poursuivie par des « arrangements stables », la structure juridique important peu. Selon le Groupe Article 29, un établissement peut exister si le bureau local s'occupe de relations avec des utilisateurs finaux, ou si le bureau s'occupe de la vente de publicité, ou si le bureau répond à des demandes d'autorités de police en ce qui concerne l'accès aux données.

55 - Si la plateforme (qu'il s'agisse d'un moteur de recherche ou d'un site communautaire) n'a pas d'établissement en Europe, la loi française s'appliquera si le site utilise des moyens techniques situés sur le territoire français. Selon le Groupe Article 29, des cookies situés dans l'ordinateur de l'utilisateur peuvent constituer des moyens conduisant à l'applicabilité de la loi locale.

7. Conclusion

56 - Trouver une solution équilibrée entre une offre ajustée aux besoins du consommateur et permettant le financement de l'Internet et une préservation des libertés individuelles du consommateur : tel est le défi posé à la publicité ciblée à ce jour.

57 - Le projet est ambitieux et essentiel, sous peine de ralentir le développement de l'Internet. Les fournisseurs de services doivent trouver une rémunération pour la fourniture de leurs services mais la recherche de profits ne doit pas se faire au détriment de la liberté et de la vie privée des internautes. Les autorités en charge de la protection de la vie privée et du consommateur deviennent de plus

29. Avis du Groupe Article 29 sur les moteurs de recherche, p. 15

30. FTC, Communiqué, p. 4

31. Dir. n° 95/46/CE, art. 17

32. Avis du Groupe Article 29 sur les moteurs de recherche, p. 13

33. Idem, p. 14

en plus vigilantes compte tenu de la généralisation de l'Internet comme moyen de communication.

58 - La concertation entre les différentes parties prenantes est déterminante, pour aboutir à des règles efficaces, largement acceptées et gérables techniquement. Par exemple, dans le cas d'un écran d'ordinateur ou d'un téléphone portable, il sera difficile d'assurer l'information parfaite du consommateur. L'article L. 121-1, II du Code de la consommation recommande d'ailleurs de tenir

compte « des limites propres au moyen de communication utilisé ». La définition de lignes directrices et de recommandations par des organismes tels que l'IAB et le Forum des droits de l'Internet sont très clairement à encourager. ■

Mots-Clés : Protection des consommateurs - Publicité - Publicité en ligne ciblée

JurisClasseur Conférences

COMMENT S'INSCRIRE ?

✉ COURRIER LexisNexis SA
Service Formations et Conférences
141, rue de Javel
75747 Paris cedex 15

☎ FAX 01 45 58 94 35

✉ E-MAIL formations@lexisnexus.fr

RENSEIGNEMENTS

🌐 SITE <http://formations.lexisnexus.fr>

☎ 0 821 200 700

0,112 € puis 0,59 €/min à partir d'un poste fixe

Journée d'étude JurisClasseur

Mardi 8 juillet 2008 - Paris

LOI DE MODERNISATION DE L'ÉCONOMIE

Soyez les premiers à bénéficier d'une analyse des points clés de la future loi :

- La transmission d'entreprise
- La réforme du statut de l'entrepreneur individuel
- La nouvelle négociabilité des contrats commerciaux
- La réduction des délais de paiement
- Urbanisme commercial : les nouvelles règles

Des experts de chaque matière débattront avec vous et répondront à vos questions.

ÉCONOMISEZ 50€
Inscrivez-vous avant
le 30 mai 2008

Sous la direction scientifique de Stéphane TORCK
Professeur agrégé, Université de Rouen

Avec les interventions de

Damien DUTRIEUX
Consultant associé au CRIDON Nord-Est, Maître de conférences à l'Université de Valenciennes

Henri HOVASSE
Professeur à la Faculté de droit de Rennes

Dominique FERRÉ
Avocat associé, Cabinet Fidal, Directeur du département distribution concurrence

Téléchargez le programme et le bulletin d'inscription sur

<http://formations.lexisnexus.fr>