



**« Une obligation de surveillance en quelque sorte particulière » (jugement rendu par la 8ème chambre du tribunal de commerce de Paris en date du 20 février 2008)**

par Géraldine Criqui

Par un jugement du 20 février 2008, le tribunal de commerce de Paris condamne les sociétés Google France et Google Inc en tant qu'hébergeurs pour la diffusion sur leur site, Google vidéo d'un contenu contrefaisant : le film « Le monde selon Bush » [1] .

En effet, ayant reçu notification du caractère illégal d'un contenu qu'il proposait, le service Google Vidéo n'a pourtant pas rendu sa diffusion définitivement impossible. Dès lors sa responsabilité est engagée sur le fondement de l'article L 6-I-2 de la loi pour la confiance dans l'économie numérique du 21 juin 2004 (LCEN).

Une décision sur la responsabilité d'un hébergeur du web 2.0, donc, dans la droite ligne de celles récemment rendues par le TGI de Paris, et notamment de deux décisions rendues par sa 3ème chambre civile : Nord-ouest production c/ Daily Motion [2], et Zadig production c/ Google Inc [3].

Des décisions qui ont fait l'objet de nombreux commentaires : les sites 2.0 d'hébergeurs devenaient de facto des éditeurs, tenus d'une obligation générale de surveillance, une nouvelle qualification naissait en dehors du cadre de la LCEN [4] .

C'est une analyse. Le jugement étudié en amène une différente. Il confirme qu'une autre grille de lecture des arrêts Daily Motion et Zadig production c/ Google Inc. est possible : il n'y a aucune création prétorienne du juge mais bien une application solide des règles de la LCEN.

Dans l'arrêt Dailymotion, le juge fait référence, dans le cadre de la discussion sur la qualité d'hébergeur ou d'éditeur du service, aux accords que ce dernier a passés avec des grandes majors de cinéma pour diffuser légalement leurs œuvres. Ce rappel n'est pas anecdotique. On serait plutôt tenté de penser que, par lui, le juge tient subtilement à souligner que l'hypocrisie dont font preuve de telles plate-forme, Dailymotion ou Google Vidéo entre autres, ne peut plus être. Ils ont conscience que des contenus pirates sont diffusés par leurs services.

Toutefois avoir conscience du caractère vicieux de leur modèle économique ne signifie pas que ces plates-formes puissent avoir connaissance de tout fait précis de

contrefaçon. Et contrairement à ce qu'on pourrait croire, c'est bien ce que dit le juge. Il n'impose pas d'obligation générale de surveillance à Dailymotion qu'il qualifie d'hébergeur. Il ne contredit pas l'article 6-I-7 de la LCEN.

En effet, la mise en œuvre de la responsabilité de l'hébergeur est conditionnée par l'existence d'une notification. Le juge n'élide pas cette étape et respecte les prescriptions de la LCEN.

Il est vrai toutefois que la formulation de la décision Dailymotion porte à confusion, il y est fait état d'un « contrôle a priori ». Mais celui-ci doit plutôt s'entendre comme un contrôle a priori de la réalisation de tout dommage qu'une nouvelle diffusion pourrait entraîner, dès lors que le contenu a été porté à la connaissance du service une première et unique fois.

Le tribunal, composé à l'identique, l'expose plus clairement dans le jugement Nord-ouest production /c Google Inc ; la responsabilité de l'hébergeur 2.0 s'entend ainsi : « informée du caractère illicite du contenu en cause par la première notification, il lui appartenait de mettre en œuvre tous les moyens nécessaires en vue d'éviter une nouvelle diffusion, ce qu'elle ne démontre pas avoir fait, le développement allégué de solutions techniques afin de prévenir et à tout le moins de limiter l'atteinte aux droits des tiers ayant manifestement été en l'espèce inopérant ».

Le tribunal de commerce de Paris suit le même raisonnement : « Attendu cependant qu'à compter de cette date il leur appartenait de rendre l'accès au film impossible [...] Attendu que les défenderesses ne peuvent donc faire valoir une quelconque impossibilité technique pour exercer cette surveillance, qu'elles ont développés dans leurs écritures et à la barre l'existence de moyens de plus en plus sophistiqués leur permettant d'identifier les contenus déclarés illicites, que ces moyens sont mis en œuvre pour éliminer les contenus à caractère pédophile, faisant l'apologie de crime contre l'humanité ou de l'incitation à la haine ».

On le voit l'obligation de surveillance après une première notification est justifiée par les moyens techniques dont disposent les hébergeurs pour tracer leurs contenus.

Les juges exercent dès lors pleinement leur rôle : ils ne se placent pas en dehors du cadre législatif mais lui donne une relecture au travers du prisme des évolutions technologiques. Leur interprétation de la loi doit permettre au temps législatif, si ce n'est de rattraper le temps technologique, tout du moins de le serrer au plus près.

Des techniques de marquage des contenus sonores et vidéos voient le jour, sont commercialisées et achetées par les diffuseurs de vidéos en ligne [5]. Dès lors une nouvelle catégorie d'hébergeur naît avec « une obligation de surveillance en quelque sorte particulière ».

Une obligation de surveillance qui n'est pas générale, donc, puisqu'elle n'intervient qu'à partir de la première notification, qui techniquement permet de constituer l'empreinte digitale qui permettra le traçage futur de l'œuvre.

Et une catégorie nouvelle d'hébergeur et non pas une redéfinition du statut d'hébergeur dès lors que ce raisonnement ne semble s'adresser qu'aux services

permettant la mise en œuvre de ces techniques. Le raisonnement appliqué à Dailymotion et à Google Video n'est pas le même que celui appliqué à Wikimédia foundation [6]. Il convient de le préciser dès lors que bien souvent toutes ces décisions sont citées ensemble pour faire état de la responsabilité des hébergeurs du web 2.0, au risque de créer la confusion.

Enfin il faut rester mesuré et ne pas agiter le spectre d'une atteinte aux libertés individuelles, et à la liberté d'expression notamment. Les présentes affaires avaient la particularité de porter sur un délit de contrefaçon et non sur une atteinte à l'image ou à la vie privée. L'automatisme des techniques de marquage convenait dès lors d'autant mieux que le caractère manifestement illégal du contenu dans ces espèces ne pouvait être remis en cause.

Toutefois, il est vrai qu'il faut être vigilant quant à la généralisation de cette justification de la responsabilité des acteurs de l'internet par les techniques nouvelles. Ces dernières ne doivent pas suspendre la réflexion et figer le cadre normatif.

Rappelons, d'ailleurs, que nous sommes toujours en attente d'un décret précisant l'obligation d'identification des créateurs et contributeurs de contenus définie à l'article 6.II de la LCEN.

Les systèmes de filtrage ne sont pas une fin en soi et l'hébergeur sera toujours inquiété tant que ne lui sera pas imposée avec précision l'obligation d'identifier le véritable auteur de l'infraction : l'utilisateur éditeur de contenu.

Géraldine CRIQUI

---

[1] Jugement disponible sur [www.legalis.net](http://www.legalis.net)

[2] TGI Paris, 3ème ch. 2ème section, 13 juillet 2007 RG 07/05158

[3] TGI Paris, 3ème ch. 2ème section, 19 octobre 2007 RG 06/11874

[4] Lettre du Cejem n°37, Aurélien BAMDE Déclaration de guerre confirmée contre les hébergeurs de web 2.0 ; QUEMENER Myriam et Joël FERRY Cybercriminalité Défi mondial et réponses, Economica 2007, p.47.

[5] DUMONS Olivier, « Les diffuseurs de vidéos en ligne mettent en place des systèmes de filtrage », Le Monde du 24 juillet 2007.

[6] TGI Paris, réf., 29 oct. 2007 sous Com. THOUMYRE Lionel, Etudes n° 5 Communication Commerce Electronique, Février 2008.

## **L'avocat et internet ou la confrontation de la tradition au modernisme**

par Morgan Baglin

« Un avocat vous répond en ligne », « Conseil juridique en ligne », depuis un certain temps ces annonces fleurissent sur internet. Faire appel à un avocat en quelques clics apparaît désormais banal. Dans le prolongement de la directive sur le commerce électronique du 8 juin 2000 qui s'applique aux prestations en ligne dans le domaine de la consultation et de l'élaboration des actes juridiques, le Conseil national des barreaux a adopté, le 28 avril 2007, son règlement intérieur national. Ce dernier marque la volonté de la profession de travailler en adéquation avec son temps puisqu'il intègre des dispositions relatives à internet. En outre, dans la mouvance de l'e-administration, le 15 novembre 2007, un décret relatif à l'utilisation des nouvelles technologies au cours de la procédure pénale a été adopté. Ces perspectives de simplification de la procédure pénale par l'utilisation de nouveaux procédés méritent que l'on s'y attarde au regard des principes très traditionnels qui régissent la profession d'avocat et plus largement le fonctionnement de la justice.

Le règlement adopté par le Conseil national des Barreaux s'intéresse notamment aux relations entre l'avocat et ses clients ainsi qu'entre l'avocat et ses confrères. Au préalable, ce texte exige que l'avocat qui souhaite ouvrir ou modifier un site internet doit en informer l'Ordre, il en est de même pour la création de liens hypertextes. Aucun encart ou bannière publicitaire ne peut apparaître. Ces sites ne peuvent contenir aucun lien hypertexte permettant d'accéder directement ou indirectement à des sites dont le contenu serait contraire aux principes de la profession. L'avocat doit s'en assurer en visitant régulièrement son site. Principe phare de la profession : le secret professionnel, celui-ci doit être respecté quelque soit le support matériel ou immatériel (papier, télécopie, voie électronique...). Dans le même ordre d'idée, les échanges entre avocats, par nature confidentiels, doivent le rester quelque soit le support. La communication de pièces peut se faire par voie électronique, par la remise de tout support de stockage de données numériques (CD-rom, clé USB...), ou l'envoi d'un courrier électronique, s'il est justifié de sa réception. Cependant, le texte impose également et logiquement que les pièces soient numérotées, qu'elles portent le cachet de l'avocat et soient accompagnées d'un bordereau daté et signé par l'avocat. Cette dernière disposition risque d'être techniquement difficile à mettre en œuvre si les pièces sont transmises par voie électroniques surtout au niveau de leur numérotation et pour l'apposition du cachet. En outre, le règlement traite un pan croissant des modalités du travail de l'avocat : la prestation juridique en ligne définie comme un service personnalisé à un client. Le professionnel doit s'assurer de l'identité et des caractéristiques de la personne à laquelle il répond afin de respecter le secret professionnel, d'éviter le conflit d'intérêts et de fournir des informations adaptées à la situation de l'interrogateur. L'avocat qui répond doit toujours être identifiable et être en mesure d'entrer personnellement et directement en relation avec l'internaute pour lui poser les questions nécessaires ou lui faire des suggestions. En effet, il doit pouvoir s'assurer de l'identité de son client afin d'éviter de donner une consultation anonyme sans le savoir à l'un de ses adversaires. La création de tels sites appelle immédiatement des mesures concernant la publicité qui prend une dimension importante sur internet. La prestation peut être proposée mais doit respecter les prescriptions de l'article 15 du décret du 12 juillet 2005 relatif à la

publicité (l'information au public doit respecter les principes essentiels de la profession ; informations sur la nature des prestations de services proposées ; offre de service personnalisée adressée à un client potentiel est interdite). Sur ce point, il est à noter que la Cour de cassation a rendu un arrêt le 6 décembre 2007 approuvant l'achat d'encarts publicitaires sur le site internet des Pages Jaunes au motif que « le choix de ce mode de consultation de l'annuaire ne porte pas en lui-même atteinte aux obligations de discrétion et de dignité ». Le texte reprend également la célèbre jurisprudence Class Action dans laquelle la Cour d'appel concluait que l'offre de service proposée sur le site litigieux constituait un acte de démarchage illicite, prohibée par la loi du 31 décembre 1971. La Cour rejetait l'application à la cause de la loi pour la confiance dans l'économie numérique qui instaure un régime de liberté pour le commerce en ligne puisque l'article 16-I-2° de la LCEN exclut de son champ les activités de représentation et d'assistance en justice. Cette publicité doit donc être véridique, respectueuse du secret professionnel et mise en œuvre avec dignité et délicatesse. Elle est communiquée préalablement à l'Ordre. Traitant, quant à lui, des relations de l'avocat avec la justice, le décret du 15 novembre 2007 instaure la dématérialisation de la procédure pénale. Pour simplifier le travail des avocats et des juridictions, ce décret aménage le Code de procédure pénale, afin d'y inclure des dispositions relatives au recours aux nouvelles technologies. Ce texte adapte la procédure pénale au numérique en permettant l'envoi par un moyen de communication électronique des copies numérisées du dossier d'instruction, d'une plainte avec constitution de partie civile déposée par un avocat, d'un réquisitoire définitif du procureur de la République adressé au juge d'instruction, etc. Cependant, si dans les textes la volonté étatique ne fait pas de doute, en pratique, il convient d'émettre quelques réserves. En effet, il faudra que les moyens financiers et informatiques soient donnés aux juridictions et, surtout, assurer une confidentialité absolue de la procédure. Il est à noter que la dématérialisation des procédures civiles est, quant à elle, prévue pour 2009. Pour conclure, si la volonté de simplification des échanges, de la procédure apparaît tout à fait louable, il ne faut cependant pas oublier, dans un souci de précipitation, que les piliers du bon fonctionnement de la justice imposent un certain réalisme quant à la mise en œuvre pratique des nouvelles dispositions.

Morgan Baglin

---

## **La Directive « Services de Médias audiovisuels » et les communications commerciales**

par Ludovic Bottallo

La directive 2007/65/CE du Parlement européen et du Conseil, dite Services de Médias Audiovisuels (SMA), a été adoptée le 11 décembre 2007. Elle révisé la directive 89/552/CEE du Conseil du 3 octobre 1989, modifiée une première fois par la directive 97/36/CE du Parlement européen et du Conseil, visant à la coordination de certaines dispositions législatives, réglementaires et administratives des Etats membres relatives à l'exercice d'activités de radiodiffusion télévisuelle.

La principale évolution induite par le texte concerne l'élargissement du champ d'application de la directive TVSF. Si, jusqu'à présent, cette dernière ne couvrait que les services audiovisuels traditionnels et principalement la radiodiffusion télévisuelle, elle s'applique

dorénavant aux services dits non linéaires tels que, notamment, les services à la demande. Désormais, aux côtés des services traditionnels, la directive encadre à minima « les services de médias audiovisuels fournis par un fournisseur de services de médias pour le visionnage de programmes au moment choisi par l'utilisateur et sur demande individuelle sur la base d'un catalogue de programmes sélectionnés par le fournisseur de services de médias ».

S'agissant de la publicité, la directive SMA introduit une nouvelle terminologie en insérant la définition de la « communication commerciale audiovisuelle ». Selon l'article 1.h, ces messages publicitaires sont « des images, combinées ou non à du son, qui sont conçues pour promouvoir, directement ou indirectement, les marchandises, les services ou l'image d'une personne physique ou morale qui exerce une activité économique. Ces images accompagnent un programme ou y sont insérées moyennant paiement ou autre contrepartie, ou à des fins d'autopromotion ». Dès lors, toutes les formes de publicités sont regroupées sous cette dénomination puisque la communication commerciale « revêt notamment les formes suivantes : publicité télévisée, parrainage, téléachat et placement de produits ». A la suite de cette définition générale, chacune des formes désignées est définie individuellement.

L'encadrement des communications commerciales a été pensé de façon à ne pas entraver le marché. Ainsi, s'il met en place un régime commun aux services linéaires (traditionnels) et aux services non linéaires (à la demande) (I), il propose, par ailleurs, d'assouplir les règles relatives à la publicité télévisée traditionnelle (II).

#### I/ Elaboration d'un régime commun à tous les services audiovisuels

La directive SMA a mis en place un régime souple pour l'ensemble des services de médias audiovisuels, qu'ils soient linéaires ou non linéaires. En effet, l'encadrement ne porte pas sur la programmation ou sur la durée des spots publicitaires, mais uniquement sur l'identification de ces contenus et sur certaines restrictions traditionnelles. Ainsi, l'article 3 sexies impose notamment aux communications commerciales d'être facilement reconnaissables, de ne pas utiliser de techniques subliminales, de ne pas porter atteinte à la dignité humaine ou encore de ne pas comporter de discrimination « fondée sur le sexe, l'origine raciale ou ethnique, la nationalité, la religion ou les convictions, l'âge ou l'orientation sexuelle ».

L'article 3 septies énonce également toute une série de restrictions pour les services de médias audiovisuels parrainés. Ces derniers doivent ainsi répondre aux exigences suivantes : « leurs contenus ne doivent pas porter atteinte à la responsabilité et à l'indépendance éditoriale (...) ; ne doivent pas inciter directement à l'achat ou à la location de services, notamment en faisant des références promotionnelles spécifiques à ces produits ou services » et doivent « être clairement identifiés ».

Par ailleurs, il convient de relever que la directive introduit une nouvelle forme de publicité désignée sous le terme de « placements de produits », défini comme « Toute forme de communication commerciale audiovisuelle consistant à inclure un produit, un service, ou leur marque, ou à y faire référence, en l'insérant dans un programme, moyennant paiement ou contrepartie ». Or, à suivre la rédaction du point n°1 de l'article 3 octies, « le placement de produit est interdit ». Cela étant, cette interdiction est uniquement théorique. En effet, dès le point n°2 de l'article, il est indiqué que le placement de produit est admissible « dans les œuvres cinématographiques, films et séries réalisés pour des services de médias audiovisuels, ainsi que pour des programmes sportifs et de divertissement (...) ». Ainsi, contrairement à ce qu'indique le premier point de l'article, le placement de produits est autorisé pour tous les contenus sauf pour les « programmes pour enfants ».

Enfin, le régime des publicités interdites est étendu à toutes les communications commerciales audiovisuelles. Ainsi, d'après le considérant 55, la directive 2003/33/CE du

Parlement européen et du Conseil du 23 mai 2003, qui interdit la publicité et le parrainage en faveur des cigarettes et des autres produits du tabac et la directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001, qui interdit la publicité auprès du public faite à l'égard de certains médicaments, s'appliquent. Ces interdictions sont ainsi applicables aux communications commerciales audiovisuelles (article 3 sexies), au parrainage de services de médias audiovisuels (article 3 septies) ainsi qu'au placement de produits (article 3 octies).

## II/ Un assouplissement des règles relatives à la publicité télévisée

La directive SMA procède à un assouplissement législatif des dispositions relatives au temps de diffusion des écrans publicitaires. Jusqu'à présent, la directive TVSF imposait aux éditeurs de services de diffuser ces contenus en respectant un intervalle de 45 minutes. Or, à l'occasion de la révision de la directive, les autorités communautaires ont réduit ce délai à 30 minutes. Ainsi, selon l'article 11.2, « La diffusion de films conçus pour la télévision (à l'exclusion des séries, feuilletons et documentaires), des œuvres cinématographiques et des journaux télévisés peut être interrompue par de la publicité télévisée et/ou du téléachat une fois par tranche programmée de trente minutes au moins ». En revanche, l'article 18.1 conserve la référence classique de 12 minutes de publicité par heure d'horloge.

Cet assouplissement paraît être justifié par deux considérants. Selon le considérant 57, « compte tenu des moyens accrus dont dispose les téléspectateurs pour éviter la publicité grâce au recours aux nouvelles technologies, telles que les enregistreurs vidéos numériques personnels, et de l'élargissement de la palette des canaux disponibles, le maintien d'une réglementation détaillée en matière d'insertion des spots publicitaires en vue de protéger les téléspectateurs ne se justifie plus ». A cette explication, nous pouvons également relever que le considérant 55 invoque l'objectif de proportionnalité à « l'intérêt général » pour justifier cet assouplissement.

A l'inverse, Emmanuel DERIEUX, que nous rejoignons sur ce point, considère que « les aspects techniques et économiques semblent ainsi fortement privilégiés, au détriment des quelques éléments de spécificité du cadre européen en ce qui concerne la réglementation de la publicité et le placement de produits notamment » (CCE n°6, juin 2007, p.13 et s.). En effet, sous couvert de modernisation et d'adaptation de la réglementation aux nouvelles technologies, la directive SMA semble davantage avoir profité aux opérateurs économiques qu'à l'identité culturelle européenne et à la création.

Ludovic Bottallo

---

## De la fragmentation de l'internet

par Aurélien BAMDE

Parce que l'internet fascine autant qu'il dérange, bien des croyances se sont cristallisées autour de sa nature. Et si nombreuses sont celles qui se contredisent d'une communauté à l'autre, il en est une qui est universelle chez les internautes : aux yeux de tous, l'internet a été élaboré selon une architecture complètement décentralisée pour que les réseaux de télécommunications ne soient pas touchés en cas d'attaque nucléaire inopinée.

Mais, en réalité, deux systèmes sont à distinguer : l'un gouverne la communication au sein du réseau, l'autre son adressage. Dès lors, s'il est incontestable que le premier répond à une logique décentralisée en ce que les paquets IP sont libres d'emprunter la voie la moins encombrée, le second quant à lui répond plutôt à une logique centralisée en ce que toutes

les adresses utilisées sont inscrites dans une seule et même base de données. En effet, afin que la communication entre les utilisateurs soit facilitée, les architectes du réseau ont imaginé dans les années soixante-dix, un système permettant de nommer les ordinateurs par des caractères alphanumériques, de sorte qu'il n'ait pas besoin de taper leur adresse IP pour y accéder. Pour ce faire, c'est un gigantesque annuaire numérique qui a été créé, lequel est constitué d'une liste unique de correspondances entre toutes les adresses IP des machines connectées au réseau et les noms qui leur sont attribués. Ainsi cette liste constitue-t-elle l'ensemble de l'espace de nommage.

Malheureusement, très rapidement, cet espace est devenu trop petit pour satisfaire la demande en adresses numériques de l'ensemble de la communauté. C'est la raison pour laquelle un nouveau système a été façonné, système connu sous le nom de DNS (Domain Name System). Concrètement ce système d'adressage consiste en la division de l'espace de nommage en « sous-espaces », appelés zones, de sorte que la base de données contenue à l'époque dans un seul fichier (host.txt), s'est vue divisée en autant de fichiers qu'il y a de zones. Les fondateurs du DNS ont alors pu édifier une architecture dans laquelle chaque zone est associée à un ordinateur hôte faisant office de serveur, un logiciel de résolution de noms et un fichier-zone à l'intérieur duquel on retrouve le binôme : adresse IP-nom alphanumérique. De la sorte, tout comme pour une adresse postale composée d'un nom de pays, d'un code postal, d'un nom de ville, d'un nom de rue et enfin d'un numéro, à chaque zone est affectée une partie de l'adresse numérique. Il en résulte que, chacune des différentes zones entretient un rapport hiérarchique avec la zone qui lui est inférieure ou supérieure, l'ensemble des zones réunies formant une arborescence.

Jon Postel, fondateur de cet ouvrage use d'ailleurs de la métaphore d'arbre inversé pour décrire son système, arbre inversé au sommet duquel se trouve une zone unique appelée racine, laquelle est reliée à des zones inférieures appelées haut niveau (Top Level Domain), lesquelles sont à leur tour reliées à des sous-zones, appelées deuxième niveau etc. Ainsi apparaît-il que le système DNS repose sur une architecture complètement centralisée vers un point : la racine.

Dès lors inévitablement tout un chacun se posera la question de savoir ce qui se passerait si cette dernière était amenée à disparaître, notamment en cas d'attaque nucléaire comme cela était redouté. Assurément, sans qu'il soit besoin de s'étendre, c'est tout le système d'adressage qui serait anéanti. Or sans un tel système l'internet ne pourrait plus fonctionner. Manifestement, si cette menace n'est pas à négliger, notamment en raison du contexte géopolitique créé à la suite des attentats du 11 septembre 2001, il en est une autre plus pressante qui est née, jusqu'alors encore insoupçonnée. Et contrairement à ce que l'on pourrait penser, celle-ci ne réside pas dans la disparition de la racine mais dans sa duplication, voire sa multiplication. En effet, une telle entreprise conduirait indéniablement à empêcher des utilisateurs appartenant à deux espaces de nommage différents de communiquer. Pis, c'est l'internet tout entier qui s'en trouverait fragmenté. De la sorte, au lieu d'avoir un réseau de réseau comme cela l'a été imaginé, l'internet deviendrait un réseau parmi les réseaux. Autrement dit, cela reviendrait à nier purement et simplement sa spécificité.

Telle est pourtant, semble-t-il, la voie dans laquelle s'est engagée la Chine, celle-ci s'étant vraisemblablement dotée depuis mars 2004 d'un serveur racine. Officiellement le gouvernement chinois justifie cette initiative en affirmant qu'elle est uniquement motivée par la volonté de permettre à ses nationaux d'utiliser des idéogrammes dans leurs navigateurs.

Mais en réalité, nombreux sont ceux qui n'hésitent pas à avancer que cette mesure n'a d'autre finalité que d'isoler un peu plus l'empire du milieu du reste de la société de l'information. Effectivement en disposant d'un espace de nommage qui lui est propre, ses dirigeants peuvent en toute liberté délimiter un périmètre de l'internet au-delà duquel les



chinois ne peuvent pas aller, sauf pour les plus expérimentés à emprunter des voies détournées. Ainsi, étrangement ces derniers n'ont pas accès à la désormais très célèbre encyclopédie Wikipédia. De la même façon, le site du journal Libération est inaccessible. Dès lors, si comme le souligne Reporters Sans Frontières il serait excessif d'affirmer que nous nous trouvons face à un « début de balkanisation d'internet », ce phénomène n'en est pas moins dangereux en ce qu'il constitue tant une restriction à l'accès universel du savoir qu'à la liberté d'expression. Malheureusement, il semble que la chine n'a pas l'intention de s'arrêter là, puisqu'elle a pour dessein de renforcer toujours plus les mesures de filtrage entreprises depuis quelques années déjà, lesquelles s'inscrivent dans le cadre du « grand pare-feu chinois » (Great Firewall). D'ailleurs, l'illustration nous a été donnée, lorsque la société Google a accepté de collaborer avec les autorités nationales, quant à filtrer les résultats des requêtes faites dans la version chinoise du moteur de recherche. Et si le moteur de recherche, qui au demeurant n'est pas la seule entreprise à s'adonner à de telles pratiques, justifie sa démarche en affirmant qu'elle doit se plier aux lois locales, il ne s'en rend pas moins complice d'une violation de la liberté d'expression, valeur pourtant reconnue par la Déclaration universelle des droits de l'homme et inscrite dans la Constitution chinoise.

Finalement, il en résulte que ce qui est à redouter, ce n'est pas tant que l'internet d'un pays soit anéanti par l'arme nucléaire, c'est que l'internet devienne pour un pays une arme aussi puissante que le nucléaire.

Aurélien BAMDE

---

## Facebook et vie privée

par Géraldine Criqui

Faut-il encore présenter « Facebook » ? Ce réseau social est le site phénomène de l'année 2007. Ouvert au public le 24 mai dernier, il compte aujourd'hui plus de 60 millions de membres dont près d'un million de français [1].

Pas un média qui n'ait relaté la success-story de ce site crée à l'origine par un étudiant de Harvard, Mark Zuckerberg, pour mettre en relation les étudiants de son campus. Pas un média non plus n'a cependant manqué de faire état des craintes des utilisateurs de ce site, qui, de par son développement, est désormais bien plus qu'un simple trombinoscope étudiant.

Le principe même d'un réseau social est de dévoiler ses données personnelles. La question est de savoir si, une fois inscrit, l'utilisateur reste maître de ces dernières. L'interface Facebook permet-elle un niveau de protection adéquat des données personnelles et le respect de la vie privée ?

La problématique ainsi formulée sous-tend une culture juridique française ou encore européenne. Vient à l'esprit l'article 1er de la loi informatique et libertés [2] : « L'informatique doit être au service de chaque citoyen. [...] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

Cependant le site Facebook est une société américaine et la première question à se poser est donc bien celle-là : la législation européenne plus protectrice des données personnelles que celle en vigueur aux Etats-Unis, et notamment la loi informatique et libertés française, peut-elle s'appliquer au site ?

On peut donner à cette question une réponse positive, le site étant accessible en France. La collecte de données est réalisée sur le territoire français. Dès lors les conditions de l'article 5

de la loi informatique et libertés sont remplies, et la législation française doit donc s'appliquer.

Toutefois, les conditions d'utilisation (terms of use) de Facebook précisent que l'utilisateur consent à voir ses données personnelles traitées et transférées aux Etats-Unis [3]. La logique est alors autre. Le site pour être en règle avec la législation européenne [4] doit présenter un niveau de protection adéquat. Facebook, pour ce faire, a adhéré au « Safe Harbor », un accord entre la commission européenne et les autorités américaines signé en 2000 [5].

La question reste complexe et illustre la nécessité d'un texte international contraignant. Toujours est-il que Facebook doit donc au minimum respecter des principes de protection des données personnelles basés sur ceux de la directive européenne de 1995, principes qui guident également la législation française.

Les données doivent être traitées en toute loyauté et de manière transparente. L'utilisateur doit être informé de la finalité du traitement et de l'usage qui est fait de ses données. Il doit pouvoir y avoir accès pour les rectifier ou demander leur suppression. Facebook respecte-il ces principes ?

Le profil d'un individu sur le réseau consiste au minimum en ses noms et prénoms (qui peuvent être fantaisistes-l'usurpation d'identité est dès lors possible - ou consister en un pseudonyme-au détriment cependant de sa visibilité sur le réseau) et sa date de naissance.

Les paramètres par défaut ne permettent pas à tous les utilisateurs de Facebook de visualiser ce profil. Il est accessible uniquement aux amis de l'utilisateur, que ce dernier les ait invités ou ait répondu à une invitation. Invitation rendue possible, dès lors que l'inscription au réseau vous inclue automatiquement dans son moteur de recherche interne. Il est cependant possible de modifier ce paramètre en cliquant sur l'onglet « privacy ».

Tout l'art de protéger sa vie privée sur Facebook est là, dans la capacité à savoir paramétrer son profil. Tout est paramétrable. Encore faut-il comprendre les fonctionnalités d'un site totalement rédigé en anglais. « L'utilisateur ne maîtrise pas assez ces nouveaux outils et il apprend trop souvent à s'en servir à ses dépens » nous dit la CNIL dans une brève publiée sur son site le 16 janvier 2008 intitulée « Facebook et vie privée, face à face » [6].

Le site doit donc améliorer l'information des utilisateurs pour que le droit d'accès et de rectification soit pleinement effectif. Il doit ensuite, et c'est ce que lui a demandé la CNIL qui a rencontré ses responsables cet automne, préciser sa position sur les deux points sensibles de tout traitement de données : la durée de conservation et l'usage des données.

Beaucoup d'inquiétudes en effet naissent à la lecture de la politique de respect de la vie privée (privacy policy) [7] du site quant à la durée de conservation des données ; le droit à l'oubli étant une notion absente ou presque de cette dernière.

Ainsi il est indiqué à plusieurs reprises que toute modification du profil n'est pas définitive, l'ancienne version étant conservée « for a reasonable period » par le site dans ses archives ou en cache. Une photo par exemple, même supprimée, vient donc gonfler les archives du site ; photo, dont il faut le rappeler, la mise en ligne vous a engagé à en céder la licence perpétuelle à Facebook.

De même il est précisé que la fermeture d'un compte n'entraîne pas, là encore, sa suppression définitive. Les données sont conservées et le compte pourra être réactivé par l'utilisateur. A tout moment ? Non. La « privacy policy » le précise bien : les données du compte inactif sont conservées « for a reasonable period ».

Cela manque toutefois de précisions, et le sentiment d'une conservation longue des données qui permet à l'utilisateur de réactiver son compte à tout moment est bien là.

Ce flou est d'autant plus préoccupant au regard de la masse des données collectées et de l'usage que le site en fait.

Rappelons d'abord que le site conserve les données personnelles que l'utilisateur a souhaité dévoiler mais également les adresses e-mail des personnes qu'il a voulu inviter que celles-ci aient répondu ou non à l'invitation. Autrement dit, le site détient des données personnelles d'individus qui ne sont même pas inscrits sur le site.

Le site précise également, toujours dans sa « privacy policy » qu'il peut utiliser d'autres sources comme des journaux, des blogs ou des logiciels de messagerie instantanée pour récolter d'autres informations sur ses utilisateurs.

Or récemment, Facebook a dévoilé son intention d'utiliser les données collectées à des fins commerciales. Cette patrimonialisation des données personnelles doit être encadrée et reposer sur le consentement des utilisateurs.

Consentement qui devra être clairement demandé. Il convient de préciser cette exigence de clarté dès lors qu'elle n'est pas toujours remplie par le site. En effet, actuellement, Facebook propose une multitude d'applications, qui font l'intérêt du site, ou tout du moins, qui sont plébiscitées par ses utilisateurs. Elles permettent par exemple de comparer ses goûts cinématographiques avec ses amis, ou de jouer au poker en ligne avec eux.

Ces applications sont proposées par des sites tiers et lorsque l'utilisateur les installe, il accepte de permettre l'accès des informations données à Facebook à ces derniers qui ont leur propre politique de traitement de données. Cette acceptation se fait automatiquement dès lors que la case « Allow this application to know who i am and access my information » est déjà cochée. L'utilisateur ne lit pas les conditions et clique simplement sur ajouter cette application. On ne peut que regretter cette passivité.

Ainsi, Facebook est une gigantesque arborescence, dont la plupart des utilisateurs ignore l'étendue. La vigilance des autorités compétentes mais aussi l'information du plus grand nombre s'imposent donc.

Géraldine CRIQUI

---

[1] SANZ Didier « Ce qu'il faut retenir de 2007 et attendre de 2008 », Le figaro.fr, le 2 janvier 2008

[2] Loi n°2004-801 du 6 Août 2004, JO n°182 du 7 Août 2004, p.14063

[3] Conditions d'utilisation disponibles à cette adresse : [www.facebook.com/terms.php](http://www.facebook.com/terms.php)

[4] Dir. 95/46/CE du 24 octobre 1995, JOCE n° L 281 du 23 novembre 1995, p.0031-0050

[5] Safe harbor privacy principles issued by the US dept. of commerce on july 21, 2000 disponibles à cette adresse : [www.export.gov/safeharbor/SH\\_Privacy.asp](http://www.export.gov/safeharbor/SH_Privacy.asp)

[6] Brève disponible sur la page d'accueil du site de la CNIL : [www.cnil.fr](http://www.cnil.fr)

[7] « Privacy policy » disponible à cette adresse : [www.facebook.com/policy.php](http://www.facebook.com/policy.php)