Le phishing dans les mailles du filet de la contrefaçon de marque

Par Xavier Jorelle

E-mail : xav.jorelle@wanadoo.fr

Le *Forum des Droits sur l'Internet* a récemment mis en ligne un article[1] traitant des différentes menaces informatiques dans le cyberespace. Parmi ces cas figure le *phishing*. Le Forum a une fois de plus traité un sujet important, puisque le *phishing* demeure au cœur des préoccupations. Le géant américain du logiciel *Microsoft* a d'ailleurs intégré un « *filtre anti-hameçonnage* » à la toute dernière version de son navigateur Internet censée rattraper le retard accusé sur son concurrent de la fondation *Mozilla*. C'est donc l'occasion d'approfondir le sujet et de voir comment le droit, et spécialement le droit des marques, peut se saisir d'une telle hypothèse de « cyber-escroquerie ».

Le mot *phishing* est la contraction des mots anglais *fishing*, « pêche » en français, et *phreaking*, désignant le piratage de lignes téléphoniques. Il a longtemps été traduit en français par le terme « hameçonnage ». La *Commission Générale de Terminologie et de Néologie* lui a ensuite donné la traduction officielle de « filoutage ». Certains peuvent regretter l'interférence avec la notion de filouterie déjà bien connue du Code pénal (art. L.313-5), car la ressemblance étymologique ne doit pas induire en erreur sur des notions qui sont loin d'être aussi voisines. Cet organisme a en outre donné une définition du filoutage : c'est une « *technique de fraude visant à obtenir des informations confidentielles, telles que des mots de passe ou des numéros de cartes de crédit, au moyen de messages ou de sites usurpant l'identité d'institutions financières ou d'entreprises commerciales* ».

Plus précisément, le filoutage n'est pas une menace informatique comme les autres, car il consiste à exploiter non pas une faille informatique, mais la faille humaine. C'est donc une technique d'ingénierie sociale employée dans le cadre des nouvelles technologies d'information et de communication. La démarche est la suivante : le pirate va duper les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, le plus souvent une banque, un site de commerce électronique ou encore de sites web hébergeant des pages personnelles et autres blogs. Le corps du message reprendra donc dans cette optique les signes distinctifs de celle-ci. Ce mail est envoyé en masse à des milliers de destinataires dont l'adresse électronique a été récupérée au hasard sur Internet. Le destinataire n'est donc souvent pas client de l'établissement duquel le courrier semble provenir et ne se laissera pas piéger. Mais sur la quantité de messages envoyés, il arrive que le destinataire soit effectivement client de l'entreprise ciblée. Il obtempèrera donc en toute confiance aux directives données dans le message. Ce courrier se présente sous la forme d'une invitation à se connecter par le biais d'un lien hypertexte afin de mettre à jour les informations le concernant dans un formulaire d'un site web contrefait, copie conforme du site original (voire même jusqu'à son nom de domaine similaire). Le prétexte est assez facile à trouver, et les pirates ne font pas souvent preuve d'une grande originalité : une mise à jour du service, une intervention du support technique, etc. C'est par le biais de ce formulaire que les pirates réussissent à obtenir des informations personnelles ou bancaires des internautes tels que des numéros de comptes bancaires, identifiants et mots de passe en tous genres. Ces données leur permettront ultérieurement de réaliser des transactions frauduleuses, comme transférer directement de l'argent sur un autre compte.

Le *Forum des Droits sur l'Internet* précise que ces agissements peuvent tomber sous le coup de plusieurs qualifications pénales, et bien évidemment engager la responsabilité civile de leur auteur (1382s. C.civ.). Le *Forum* recense l'escroquerie (L.313-1s. C.pén.), l'abus de confiance (L.314-1s. C.pén.), l'usurpation d'identité (L.434-23 C.pén.), et spécialement l'atteinte à un système de traitement automatisé de données (L.323-1s. C.pén.). De manière plus hétéroclite, l'infraction de contrefaçon de marques (L.713-1s. CPI) fait aussi partie de l'arsenal juridique susceptible de trouver application à de tels faits de filoutage.

[1] Forum des Droits sur l'Internet, "De quelques dangers en « ing »", *foruminternet.org*, 28/09/2006 <http://www.foruminternet.org/actualites/lire.phtml?id=1112>.

Le groupe de travail a pu s'appuyer sur un jugement du Tribunal de grande instance de Paris[2] afin de préconiser l'application du droit des marques à la technique du *phishing*. En l'espèce, les juges ont condamné en contrefaçon d'œuvres protégées par le droit d'auteur (le graphisme et la présentation générale du site cible) ainsi qu'en contrefaçon de marques (reproduites sur les pages web factices) un individu s'étant livré à des faits de filoutage. Les magistrats ont simplement relevé la copie servile des marques pour entrer en condamnation.

Si le droit pénal et la responsabilité civile envers l'internaute victime de cette escroquerie sont le mieux à même de sanctionner ce type de délinquance, les titulaires de marques pourront trouver un moyen de réparer ce type d'atteintes à leurs signes distinctifs par le biais des dispositions du livre VII du Code de la propriété intellectuelle. Ce titulaire ciblé par le pirate va en effet subir un préjudice du fait des pertes subséquentes de fiabilité et de crédibilité auprès de sa clientèle.

Mais une telle application du droit des marques aux hypothèses de *phishing* est-elle si évidente ? Car toute utilisation d'un signe enregistré à titre de marque n'est pas susceptible de tomber dans le monopole de son titulaire[3]. L'utilisation par un tiers d'un signe couvert par un droit de marque attirera les foudres de la contrefaçon à son auteur seulement si elle entre dans le cadre général de l'atteinte aux droits détenus sur la marque, autrement dit si une telle utilisation était réservée à son titulaire. A défaut, elle éloigne donc l'application du droit des marques. Ce cadre général n'est autre que celui de la vie des affaires. La notion est visée par l'article 5.1 de la directive communautaire du 21 décembre 1988 *rapprochant les législations des États membres sur les marques*. Selon J. Passa, « *la précision est justifiée car un signe qui n'est pas utilisé dans la vie des affaires ne joue pas le rôle d'une marque, se trouve comme tel inapte à compromettre les fonctions de la marque (…) et ne peut dès lors justifier l'exercice d'un droit tendant précisément à la préservation de ces fonctions* »[4]. Ainsi le droit des marques ne viendrait uniquement sanctionner un usage par un tiers non autorisé du signe, si et seulement si cet usage venait à compromettre l'une des fonctions de la marque que sont principalement l'organisation de la concurrence et la fonction de garantie d'origine. Cet usage s'inscrirait par là dans la vie des affaires. La notion a déjà été explicitée par la CJCE dans son arrêt *Arsenal* du 12 novembre 2002. Il y est précisé qu'un usage relève de la vie des affaires « *dès lors qu'il se situe dans le contexte d'une activité commerciale visant un avantage économique et non dans le domaine privé* ».

Il faut donc qualifier les faits de filoutage en atteinte à la marque au regard de ce critère d'usage dans la vie des affaires afin de pouvoir conclure à une utilisation contrefaisante du signe distinctif. Il est clair que le « cyber-délinquant » n'inscrit pas à proprement parler son utilisation du signe de la cible dans la vie des affaires, puisqu'il n'évolue bien évidemment pas dans le cadre d'une activité commerciale. L'usage du signe qu'il réalise n'a pour unique but d'induire en erreur ses victimes afin d'obtenir des informations personnelles. La reproduction du signe de l'entreprise ciblée est donc asservie aux besoins de l'escroquerie en elle-même. La marque a donc été instrumentalisée au service d'un délit étranger à la vie des affaires. Cette utilisation de la marque a tenu place dans un simulacre de vie des affaires, à défaut du cadre authentique, puisque le pirate est venu parasiter les relations électroniques entreprise / client en usurpant l'identité de la première.

Plus juridiquement, l'applicabilité du droit des marques semblerait surtout pouvoir se justifier par le fait que l'usage du signe réalisé par le pirate vient bien compromettre une fonction essentielle jouée par la marque. Elle a notamment pour fonction d'indiquer et de garantir l'origine, l'identité de l'entreprise ayant émis le produit ou le service qu'elle accompagne. C'est la fonction de garantie d'origine de la marque. Dans l'hypothèse du filoutage, c'est bien cette fonction de garantie d'origine de la marque qui est atteinte, ce qui justifie donc une condamnation fondée sur les articles L.713-1s. CPI.

---

[2] TGI Paris, 31ème ch., 21 septembre 2005, Robin B c/ Sté Microsoft Corporation : *Juriscom.net*, <http://www.juriscom.net/jpt/visu.php?ID=759>.

[3] Voir notamment à ce sujet toute la problématique de l'usage d'une marque à des fins polémiques, utilisation ressortissant de la liberté d'expression et hors de portée du monopole du titulaire de la marque sur son signe. Particulièrement démonstratif, voir l'arrêt CA Paris, 16 novembre 2005, Esso c/ Greenpeace France : *Juriscom.net,* <http://www.juriscom.net/jpt/visu.php?ID=769>.

[4] J. Passa, "Les conditions générales d'atteinte au droit sur une marque", *Propr. Ind.,* février 2005, p. 8.

L'application du droit des marques aux faits de filoutage peut être un facteur de sévérité supplémentaire dans la répression de la cyber-délinquance. Cette fermeté reste de rigueur dans la politique jurisprudentielle de répression des comportements délictueux dans l'espace virtuel. Peut-être serait-il opportun de renforcer l'arsenal juridique afin de mieux protéger les intérêts des entreprises ciblées. Car il faut bien garder à l'esprit que la technique du *phishing* ne fait pas uniquement le destinataire du courrier électronique comme victime. Les entreprises ciblées sont indiscutablement les premières victimes du filoutage : sans même remplir leur objectif de collecte de données personnelles, les campagnes de *phishing* occasionnent de graves préjudices pour ces agents économiques.

X.J.