http://www.droit-ntic.com

# ACTUALITES JURIDIQUES

# AOUT 2002

## DROIT-NTIC

**Auteurs :**
Me Frédéric Dechamps, Julien Le Clainche, Me Martine Ricouard-Maillet, Nicolas Samarcq, Pamela Morinière, Me Caroline Parmentier, Nadjy Nackna Sadry

info@droit-ntic.com

# TABLE DES ARTICLES

# 29/08 --> Que faire en cas d'attaque contre son système informatique ?

| par Frédéric Dechamps |

Nul n'est à l'abri d'une attaque contre son système informatique… Sans être exhaustif, une attaque informatique peut prendre diverses formes : il peut s'agir d'une ingérence dans un système informatique en vue de modifier ou supprimer des données et/ ou des programmes, mais encore une violation des droits conférés à l'auteur d'un programme informatique.

Toute la question est bien entendu de déterminer dans quelle mesure la victime pourra espérer engager la responsabilité de l'auteur et, de ce fait, obtenir la réparation de son préjudice.

La plupart du temps, les sites web apposent un disclaimer visant à s'exonérer de diverses responsabilités.

Si ce disclaimer revêt un utilité relative pour d'autres aspects légaux liés à une présence sur le Net (propriété intellectuelle, qualité et pertinence des informations, etc.), il n'est cependant d'aucune utilité et d'aucun secours dans le cadre d'une attaque informatique.

En réalité, la victime d'une attaque informatique dispose de deux voies légales pour tenter d'obtenir réparation des conséquences, parfois catastrophiques, d'une attaque contre son système informatique.

Depuis une loi du 28 novembre 2000 sur la criminalité informatique, les dispositions pénales belges ont été modifiées et complétées pour intégrer les comportements des cybercriminels.

Le faux informatique ou l'intrusion et le maintien non autorisé dans un système informatique sont à présent des notions parfaitement ancrées dans notre arsenal juridique et peuvent donner lieu à des sanctions telles que l'emprisonnement ou une peine d'amende. En vertu de ces dispositions, la victime peut porter plainte et se constituer partie civile pour obtenir la réparation du préjudice subi.

Il faut également souligner l'existence d'un instrument à vocation internationale : la convention sur la Cybercriminalité du 23 novembre 2001 qui vise également à mettre en place des sanctions en cas de comportement informatique répréhensible.

D'autre part, la victime d'un acte de piratage peut engager la responsabilité civile de l'auteur.

Dans ce cadre, il faudra impérativement démontrer une faute, un dommage et un lien de causalité entre la faute et le dommage subi. La prudence s'impose : une faute de la victime peut, dans certains cas, être de nature à modaliser la responsabilité en cas de sinistre informatique.

Ainsi, le fait de ne pas mettre en place des mesures de protection suffisantes pourrait constituer une faute susceptible d'atténuer ou, plus grave encore, mettre en échec une éventuelle action judiciaire à l'encontre du pirate.

Le choix de l'action à entreprendre est donc avant tout une question d'appréciation qui paraît devoir être laissée aux professionnels du droit.

# 27/08 --> Doubleclick devant la justice américaine : Entre personnalisation et confiance ,

| par Julien Le Clainche |

Le 26 août 2002, le procureur général Eliot Spitzer a annoncé l'intervention d'un accord (*settlement*) entre la première société de vente d'espace publicitaire, Doubleclick.inc et plusieurs Etats américains [1]. Cet accord établit de nouveaux standards de protection de la vie privée [2] du consommateur en ligne.

Il s'agit d'une part de rendre les **traitements de données personnelles plus transparents** et d'autre part, de garantir un meilleur **droit d'accès** aux informations traitées. En outre, la société s'est engagée à se soumettre à une **vérification indépendante** de la conformité de sa politique avec l'accord. Elle a, par ailleurs, été **condamnée à verser 450.000$ aux Etats requérants** au titre des sommes mises en œuvre dans le cadre de l'investigation et de l'information des consommateurs.

Doubleclick étant devenu au fil du temps une figure emblématique des traitements de données à l'insu des internautes, notamment par le recours à des cookies attribuant un identifiant unique, plus d'une dizaine d'Etats américains ont décidé de mener une action à forte connotation symbolique. Cet accord fait suite à celui intervenu en mai 2002 qui avait alors condamné la société à verser 1.800.000 $ [3]

Le système mis en œuvre par Doubleclick.inc et ses partenaires permet d'identifier la plupart des ordinateurs accédant à Internet. L'identification de la machine couplée à la collecte d'une adresse électronique est de nature à justifier une information des personnes et un plus grand respect quant aux droits individuels. Les deux axes de l'accord sont ainsi :
. Plus de transparence
. Un meilleur accès aux informations collectées.

**Plus de transparence**
La plupart des collectes de données sur les réseaux étant invisibles, Doubleclick s'engage à apporter une plus grande information aux consommateurs. En pratique, un site partenaire de Doubleclick devra le signaler et exposer la nature des activités de cette société. En cas d'évolution de la politique de traitements des données de Doubleclick, la société s'engage à prévenir les personnes concernées...

**Un meilleur accès aux profils**
. Un vérificateur indépendant aura la charge de suivre le comportement de Doubleclick durant les quatre prochaines années. Au terme de trois interventions, il devra déterminer et informer les consommateurs sur l'évolution de la gestion des données personnelles.
. En outre, Doubleclick travaille actuellement à une solution technique permettant à la personne, sur la machine de laquelle un cookie est implanté, d'accéder directement à son profil, de le contrôler,... ou de le préciser.

Cet accord est symptomatique de l'inlassable quête de confiance indispensable au décollage du commerce électronique. Il ne s'agit pas essentiellement de protéger la vie privée des personnes, mais plus, de permettre le développement du commerce électronique. Le fondement de la protection de la vie privée semble donc en évolution Outre-Atlantique. Les Etats, comme les entreprises, commencent à comprendre qu'une politique de traitement des données personnelles claire, transparente et rationalisée est indispensable au développement économique.

Ainsi Don Peppers et Martha Rogers, pionniers renommés du marketing One to One plaident désormais pour un plus grand respect de la privacy et s'élèvent contre le souci

“*de vendre plus*” , “*ce qui est important, c'est la création de valeur pour le consommateur, l'augmentation des ventes en dépend.*”.
Cet accord ouvre une nouvelle voie dans laquelle le souci de personnalisation se fait aussi dans la recherche de la confiance du consommateur. Nous restons toutefois très en dessous des exigences minimales du droit européen.

1 New York, Arizona, californie, Connecticut, Massachusetts, Michigan, New Jersey, Nouveau Mexqiue, Vermont et Washington

2 Vie privée doit s'entendre, dans le cadre de cet article au sens américain du terme et fait référence aux concepts de la Privacy.

3 Voir : Doubleclick devant la justice américaine, une démonstration efficace :

http://www.droit-ntic.com/MyNews1.2/read_comment.php3?id_news=60

# 20/08 --> Les nouvelles obligations des prestataires de services internet ,

| par Me. Martine Ricouart-Maillet & Nicolas Samarcq |

• Le projet de loi d'Orientation et de programmation de la sécurité intérieure voté en première lecture, selon la procédure d'urgence, par les députés et les sénateurs les 17 et 31 juillet dernier est un texte devant permettre « *aux officiers de police judiciaire, agissant dans le cadre d'une enquête judiciaire, sur autorisation d'un magistrat, d'accéder directement à des fichiers informatiques et de saisir à distance par la voie télématique ou informatique, les renseignements qui paraîtraient nécessaires à la manifestation de la vérité* » (Annexe I – Rapport sur les orientations de la politique de sécurité intérieure).

Selon le Forum des droits sur l'internet ( http://www.foruminternet.org ), cette proposition imposerait aux prestataires de services internet l'obligation d'assurer aux autorités judiciaires l'accès direct et en ligne aux adresses IP pour identifier, dans des délais raisonnables, les auteurs d'infractions commises sur le réseau.

Cette procédure devra être strictement encadrée par des mesures garantissant la sécurité des données personnelles archivées par les prestataires de services internet.

En effet, aménager un accès direct et en ligne de ces données sensibles suppose la mise en oeuvre d'un haut niveau de sécurité technique et juridique apte à empêcher toutes consultations abusives par des personnes non autorisées.

A ce titre l'association IRIS (Imaginons un Réseau Internet Solidaire) rappelle que de tels abus ont été constatés pour le fichier de police judiciaire STIC (Système de traitement des infractions constatées).

• Ce texte constituera le bras armé de la loi « Sécurité quotidienne » (LSQ) du 15 novembre 2001 promulguée également selon la procédure d'urgence à la suite des événements du 11 septembre.

Pour mémoire cette loi a introduit trois mesures sécuritaires spécifiques à internet dont notamment **la conservation, pendant une durée maximale d'un an, des données relatives à une communication**.

Elle a donc posé le principe de rétention de ces données « pour les besoins de la recherche, de la constatation et de la poursuites des infractions » (article 29).

Cette disposition sera juridiquement opérationnelle après adoption du décret d'application.

Le décret devra déterminer les catégories de données visées et la durée de leur conservation selon l'activité des opérateurs et la nature des communications, ainsi que

les modalités de compensation.

Pour les prestataires de services internet, il s'agira vraisemblablement des données de connexion qui enregistrent les adresses IP, les adresses e-mails des messages envoyés ou reçus (à l'exclusion de leur contenu) ainsi que les adresses des sites visités.

Ce texte réglementaire devra également définir une procédure précise ne permettant pas la mise en œuvre d'une surveillance générale des réseaux afin de respecter la vie privée des citoyens dans une société démocratique, conformément au droit communautaire et à la Convention européenne des droits de l'homme.

Dès la publication du décret, le stockage de ces données sera obligatoire pour les prestataires de services internet.

D'ailleurs, les fournisseurs d'accès internet conservent d'ores et déjà les données de connexion, généralement pendant une période de trois mois voire six mois pour certains.

Cette pratique répond aux exigences de la loi du 1er août 2000, qui imposent aux fournisseurs d'accès internet et aux hébergeurs « *de détenir et de conserver des données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu dont elles sont prestataires.* » (article 43-9).

Ces derniers engagent en effet leur responsabilité en cas d'incapacité à fournir ces données dans le cadre d'une procédure judiciaire d'identification.

• • •

Au sein de l'Union européenne, la démarche sécuritaire française n'est pas isolée, loin s'en faut.

Depuis le 1er août dernier, les fournisseurs d'accès internet britanniques sont dans l'obligation d'assurer l'accès aux données de connexion de leurs abonnés dans un délai d'un jour ouvrable à compter de la réception d'un mandat policier (Regulation of Investigatory Powers Act).

L'*Information Commissioner* (équivalent de la CNIL outre-manche) considère que cette loi risque fortement d'être contraire à l'Human Rights Act qui intègre en droit interne les Conventions internationales sur les droits de l'homme et la vie privée (10 juillet 2002, http://www.dataprotection.gov.uk ).

Certes il ne sera pas facile pour les PSI de naviguer entre respect des données personnelles et de la vie privée et nouvelles exigences sécuritaires.

Le décret d'application de l'article 29 de la LSQ est donc à la fois attendu et redouté par les professionnels.

---

# 14/08 --> Greenpeace France relance le débat de la parodie sur internet ,

| par Me Martine Ricouart-Maillet & Nicolas Samarcq |

Après l'épisode DANONE du 4 juillet 2001, qui s'est conclu par la condamnation du titulaire des sites « *jeboycottedanone.com* » et « *jeboycottedanone.net* » pour contrefaçon des marques semi-figuratives du groupe agro-alimentaire, Greenpeace France relance le débat juridique opposant le droit des marques à la liberté d'expression et d'information sur internet et notamment le droit à la parodie.

Dans deux affaires distinctes, le géant pétrolier ESSO d'une part, AREVA1 d'autre part, ont assigné en référé l'association de défense de l'environnement pour usage et imitation de leurs marques dénominatives et semi-figuratives dans le cadre de deux campagnes diffusées sur le site internet « greenpeace.fr ».

• La première concernait le réchauffement de la planète où Greenpeace dénonçait le lobbying exercé par le pétrolier américain contre la ratification du protocole de Kyoto.

L'association illustrait ses propos en reproduisant la marque dénominative et semi-figurative ESSO modifiée : les lettres « S » de la marque ayant été remplacées par le symbole du dollar.

En défense Greenpeace France invoquait le droit à la parodie2 en précisant que l'imitation de la marque obéissait à la nécessité d'informer le public.

Les juges refusèrent d'appliquer cette exception au droit d'auteur aux motifs que l'association ne prouvait pas « *sérieusement s'être placée, lorsqu'elle s'est approprié la marque, sur le terrain de la création artistique* ».

La question qui se posait alors aux juges était de savoir s'il existait un risque de confusion dans l'esprit du public à raison de la notoriété de la marque ESSO ? (Article L. 713-3 b du Code de la Propriété Intellectuelle).

Le Tribunal a estimé « *que la substitution du symbole du dollar aux lettres S du mot Esso, seul ou inclus dans le logo, a pour objet de capter l'attention de l'internaute moyennement informé, alors que la marque semi-figurative est reproduite à l'identique, tant sur le plan graphique que des couleurs (…) ; que de ce fait, la première perception du logo comme de la marque verbale si légèrement modifiée évoque immanquablement les produits et services offerts par cette marque notoire* ».

Il en a déduit que cette imitation, de par « la terminologie adoptée3 » a porté atteinte à l'image d'ESSO et par conséquent a détourné le public de cette dernière.

Dès lors, les juges ont considéré que l'imitation des marques ESSO « *ne participe pas exclusivement de la nécessité de communiquer les opinions de l'association (…)* », et qu'il existe un risque de confusion dans l'esprit du public caractérisant l'atteinte portée à la demanderesse.

Ce jugement du Tribunal de Grande Instance de Paris du 8 juillet dernier confirme le seul précédent en la matière (affaire « jeboycottedanone »).

• Dans la seconde affaire opposant Greenpeace France au groupe AREVA, le Tribunal de Grande Instance de Paris était saisi d'une action en contrefaçon des marques semi-figuratives AREVA composée de la lettre A soulignée par l'élément dénominatif AREVA et de la lettre A stylisée.

En l'occurrence, Greenpeace France avait notamment reproduit la « *marque « A » stylisée avec une ombre reproduisant une tête de mort associée au slogan « STOP PLUTONIUM-L'ARRET VA DE SOI* » (…) ».

Dans un premier temps , le tribunal a refusé de retenir la contrefaçon sur le fondement de l'article L. 713-2 du Code de la Propriété Intellectuelle qui interdit la reproduction d'une marque sans l'autorisation de son titulaire aux motifs « *que les reproductions incriminées ne sont pas à l'identique des marques opposées car elles comportent toutes l'adjonction d'autres éléments* ».

Sur le grief d'imitation au visa de l'article L. 713-3 b qui nécessite la démonstration d'un risque de confusion, le Tribunal a considéré que « *la finalité des imitations de Greenpeace ne se situe pas sur le terrain commercial mais sur le terrain de la liberté d'expression dans le cadre du droit à la critique et à la caricature et que d'autre part [concernant] le risque de confusion, l'internaute compte tenu de la notoriété de l'éditeur du site ne pouv[ait] croire que les informations diffusées proviennent du titulaire des marques ou d'entreprises qui lui sont liées (…)* » (Tribunal de Grande Instance de Paris, ordonnance de référé, 02 août 2002).

Par ailleurs en imitant les marques en cause, Greenpeace France ne désigne pas les produits de la classe 38.

Ainsi le Tribunal n'a t'il pas abordé comme le lui suggérait Greenpeace les notions de caricature et de parodie, mais s'est limité à examiner la demande au regard des principes classiques du droit des marques :

- imitation ou usage des signes entraînant un risque de confusion,

- désignation de produits ou services identiques ou similaires.

Sur ce seul fondement le groupe AREVA a été débouté.

1. Nom commercial du regroupement des activités des sociétés CEA INDUSTRIE, COGEMA, FCI, FRAMATOME ANP et TECHNICATOME.
2. Article L. 122-5-4° du Code de la Propriété Intellectuelle.
3. E$$O, STOP E$$O

# 07/08 --> Deep linking and the possible liability of search engines ,

| par Pamela Morinière |

The Munich oberlandesgeright court has recently ruled that using a search engine to locate stories on newspapers' web sites violated the Directive 96/9/EC on the legal protection of databases. The present case involved the German newspaper Mainpost and the German search service Newsclub.

This decision could significantly challenge the level of information that many European search engines aim to provide their users with.

The Database Directive entered into force in January 1998. The text states in its recital 13 that it “protects collections, sometimes called 'compilations`, of works, data or other materials which are arranged, stored and accessed by means which include electronic, electromagnetic or electro-optical processes or analogous processes”. The Directive provides the author of a database with a sui generis right which entitles him to “prevent the unauthorized extraction and/or re-utilization of the contents of a database”. Therefore, the author of a database shall authorize or prohibit “ temporary or permanent reproduction by any means and in any form, in whole or in part”(article 5).

According to the Munich court the activity of search engines would fall into the category of temporary reproduction of the content of a database. Unlike the Copyright Directive, however, no exception exist as to temporary reproduction of a content in the Database directive.

From January 1998 onwards, and every 3 years thereafter, the European Commission shall present a report on the implementation of the Directive in Member States. One of the task of the European Commission is specifically to check whether the application of the sui generis right has led to abuse of a dominant position or other interference with free competition.

The European Commission's first report on the implementation of the Database Directive should be presented to the European Council and the European Parliament in 2003.

# 05/08 --> Spamming : L'Europe approuve le système de l'opt-in ,

## 05/08 --> Spamming : L'Europe approuve le système de l'opt-in ,

| par Caroline Parmentier et Martine RICOUART-MAILLET Avocats |

En adoptant le 12 juillet dernier la proposition de directive sur la protection des données personnelles dans le secteur des télécommunications électroniques, le Conseil des ministres européens impose désormais aux Etats membres le système de l'opt-in pour les e-mails, fax et systèmes d'appel automatique, obligeant ainsi les professionnels du marketing direct à recueillir le consentement préalable des consommateurs avant tout envoi d'e-mail commerciaux.

Cette directive devra être transposée par les Etats membres de l'Union européenne avant le 31 octobre 2003.

**Définitions :**

- **Spam** : la CNIL définit le spam comme l'envoi massif et parfois répété de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact, et dont il a capté l'adresse électronique dans des espaces publics de l'Internet : forum de discussion, listes de diffusion, annuaires électroniques, sites web… .

- **«Opt-in »** : le système de l'«opt-in» réside dans l'autorisation préalable du destinataire à l'envoi à son adresse des courriers électroniques promotionnels.

- **«Opt-out»** : le système de l'«opt-out» consiste à l'inverse, à obliger le prestataire à permettre au destinataire de pouvoir retirer son adresse de la liste d'envoi de l'annonceur (généralement en cochant une case).

L'intérêt du spam pour les entreprises qui y ont recours est principalement économique dans la mesure où les coûts à leur charge sont bien moindres que par rapport à tout autre procédé de communication (courrier postal, fax…). Le spam permet ainsi aux entreprises du marketing en ligne d'atteindre rapidement, directement et massivement les consommateurs par le biais de leur boîte aux lettres électroniques et de réduire ainsi les frais qu'ils auraient dû engager.

En revanche, si le spam présente de nombreux atouts pour les entreprises du marketing, il a un coût pour les internautes qui voient leur boîte aux lettres envahies de messages

non souhaités, augmentant le temps de téléchargement de leur boîte de réception. Ces derniers supportent non seulement le coût lors des connexions au réseau téléphonique, mais perdent également du temps à lire ou tout au moins à supprimer ces messages. Ainsi, selon une étude commandée par la Commission européenne, les abonnés à Internet payent à leur insu un montant de 10 milliards d'euros par an en frais de connexion juste pour recevoir des messages non-sollicités.

La pratique du spamming est prohibée par la Nétiquette.

Elle est très encadrée dans le cadre de l'Union Européenne et notamment en France. Une telle pratique suppose en effet, que les entreprises aient préalablement collecté les adresses auxquelles elles envoient ces courriers non sollicités conformément aux nombreuses dispositions de protection des données. L'adresse électronique constitue en effet une donnée personnelle.

Ainsi la directive CE du 24 octobre 1995 relative à la protection des données personnelles reprenant certaines dispositions de la loi « Informatique et Libertés » du 6 janvier 1978 impose que les données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités. Pour être légitime, le traitement de données doit être nécessaire au but légitime poursuivi par son responsable, et la personne doit avoir donné son consentement.

Par ailleurs, le caractère facultatif de la collecte doit être rappelé, de même que le destinataire des données collectées, l'existence d'un droit d'accès et de rectification, l'existence d'un droit gratuit et sur demande de s'opposer au traitement de ces données à des fins de prospection et la possibilité de refuser toute communication ou toute utilisation de ces données par des tiers.

En plus de ces obligations, les professionnels devront désormais recueillir le consentement préalable des consommateurs avant tout envoi d'e-mail commerciaux.

Toutefois, lorsque les coordonnées électroniques ont été obtenues lors de la vente d'un produit ou d'un service, le professionnel pourra les exploiter à des fins de prospection directe pour des produits et services analogues. Si le commerçant veut présenter d'autres produits par mail, il devra demander l'accord préalable du client.

En imposant l'«opt-in », les instances européennes ont ainsi manifesté leur volonté de mettre fin aux pratiques abusives des spammeurs, qui n'hésitent pas à envahir nos boîtes aux lettres électroniques.

De son côté, la jurisprudence fait également preuve de sévérité. Ainsi, un internaute pratiquant le spamming qui s'était vu supprimer l'accès à Internet par ses deux fournisseurs d'accès et qui les avait assigné afin d'obtenir le rétablissement de son accès internet ainsi que des dommages et intérêts, a été condamné par le Tribunal de Grande Instance de Paris dans une ordonnance du 15 janvier 2002. Le Tribunal a estimé que la pratique du spamming est une pratique déloyale et gravement perturbatrice

Notons néanmoins que le problème des e-mail envoyés par des spammeurs situés en dehors de l'Union Européenne reste entier.

**Spam et CNIL :**

Le 10 juillet dernier, la CNIL a présenté son 22ème rapport annuel d'activité. A cette occasion, la CNIL a annoncé une action d'envergure de lutte contre les pratiques de spamming.

La CNIL a créé une adresse e-mail destinée aux particuliers victimes d'e-mails non sollicités. Cette adresse est destinée à recueillir tous les messages non sollicités reçus par les particuliers. Dotée d'un instrument d'analyse, la CNIL pourra ensuite repérer les messages qui contreviennent effectivement aux dispositions en vigueur et prendre les mesures adéquates.

Cette nouvelle boîte aux lettres est opérationnelle à l'adresse : spam@cnil.fr, on peut supposer qu'elle connaisse un grand succès dans la mesure où elle constitue un moyen simple et efficace pour tout internaute de faire constater une action de spamming.

Cet article est publié par le cabinet BRM Avocats :

http://www.brmavocats.com

# 02/08 --> Noms de domaine: Volvo cale au STOP ,

| par Nadjy Nackna |

Une décision rendue le 15 juillet par le Centre d'arbitrage et de médiation de l'OMPI met de nouveau en lumière une des limites les plus importantes de la procédure STOP applicable au « .biz ».

Le nom de domaine en cause est « volvocars.biz ». L'expert relève que le constructeur automobile est bien propriétaire de la marque « Volvo » aux Etats-Unis et dans de nombreux autres pays. Néanmoins il ajoute que, même si l'adjonction du terme « cars » ne réduit pas le risque de confusion entre le domaine et la marque, il n'y a pas identité entre les deux.

La procédure STOP (Start-up Trademark Opposition Policy), destinée à protéger les titulaires de marques contre le dépôt indu de noms de domaine en .biz est, sur de nombreux points, très proche de la procédure URDP.

Cependant, alors que l'article 4(a)(i) des règles de l'URDP s'applique lorsque le nom de domaine est « identique ou semblable au point de prêter à confusion avec une marque de produits ou de services sur laquelle le requérant a des droits », l'article 4(a)(i) des règles applicables à la procédure STOP ne concerne que l'identité et n'inclut pas la similarité.

Cet argument a conduit au rejet de la demande de transfert de Volvo, sans que les autres critères –cumulatifs- n'aient été examinés. A n'en pas douter, l'absence d'intérêt légitime ou de droit sur le nom, ainsi que la mauvaise foi auraient pu être prouvés par le requérant.

Le système mis en place pour l'attribution et le règlement des litiges concernant les noms de domaine en .biz devait corriger les errements qui avaient existé pour les autres TLD. Pourtant, avec des critères aussi restrictifs, le cybersquatting trouve un allié objectif plutôt inattendu.

---