www.droit-ntic.com

MIEUX COMPRENDRE LES IMPLICATIONS JURIDIQUES DU PROGRES TECHNOLOGIQUE

REVUE D'ACTUALITE JURIDIQUE

DU DROIT DES

TECHNOLOGIES DE L'INFORMATION

ET DE LA COMMUNICATION

Aout 2003

SOMMAIRE

25/08/2003

Fermeture citoyenne de DROIT-NTIC le 27 aout !

- Auteur : **Julien Le Clainche** *Allocataire de recherche* .
- Domaine : PROPRIETE_INTELLECTUELLE
- Sous thème : Droit_des_marques_et_des_brevets
- Ordre juridique :

- Abstract :

Logiciel, brevet, innovation,

DROIT-NTIC fermera ses portes le mercredi 27 aout 2003 pour protester contre la directive "brevet de logiciel" qui sera présenté devant le Parlement européen le 1er septembre 2003. Nous espérons que vous comprendrez notre démarche qui ne vise pas à troubler votre navigation, mais à interpeller les internautes sur un vrai problème de société.

- Les brevets concernant des logiciels sont de nature a changerla fonction même de ce type de protection. En effet, le brevet est une protection initialement crée pour protéger et stimuler l'innovation. Pourtant, le brevet appliqué aux logciels est désormais utilisé dans le cadre d'une stratégie de blocage des concurrents qui freine l'innovation comme l'illustrent certaines études économiques.

Enfin, le logiciel se prête mal au droit des brevets qui s'en trouve dénaturé.

Pour plus d'infos consultez notamment *FFII: Brevets Logiciels en Europe*.

Afin de protester contre ces dérives dangereuses, une manifestation est organisée le mercredi 27 aout devant le parlement européen.

En signe de protestation, DROIT-NTIC.com fermera donc ses portes toute la journée du 27 aout.

Nous vous remercions de votre compréhension.

Auteur : : **Julien Le Clainche** *Allocataire de recherche* . | **Source : DROIT-NTIC** |

LIENS

- http://swpat.ffii.org/
- http://wiki.ael.be/index.php/BigDemo27aug

18/08/2003

Lorsque la sécurité appelle la surveillance : le vieux fantasme de la protection à tout prix

- Auteur : **Melle Joëlle Béderède** *Juriste* .
- Domaine : INFORMATIQUE_ET_LIBERTES
- Sous thème : Droits_de_la_personnalité
- Ordre juridique :

Si une surveillance systématique des individus permettait d'assurer un niveau de sécurité et de protection optimum, nul doute que les citoyens de ce Monde seraient sur le point d'entrer dans l'âge de la Tranquillité.

Seulement, lorsque les techniques de profilage des individus dégénèrent en moyen de surveillance systématique, liberticide par excellence sinon par essence, l'objectif de sécurité ne peut souffrir aucun échec.
L'arsenal de surveillance actuellement déployé sous la pression américaine n'amène cependant pas à la quiétude intellectuelle que l'on voudrait.

- Depuis le 11.09 un certain nombre de pays - dont la France - s'est pourvu d'instruments juridiques visant à faciliter les travaux d'investigation dans des situations à risques, en permettant notamment aux autorités compétentes un accès quasi-direct aux données personnelles d'individus suspects.
Les raisons alors invoquées, manifestement légitimes au regard des événements (quand les moyens employés n'emportaient pas l'adhésion) tendent cependant à devenir la légitimation d'un déploiement infernal de mesures de sécurité, tenant plus de la manie de la persécution que d'une réponse à des menaces probables.
Dans la tradition d'insulte à l'intelligence dont le Reste du Monde a dû s'accommoder, les Etats-Unis tentent actuellement de convaincre que le fichage systématique des voyageurs aériens à destination, en partance ou en transit sur leur territoire serait en mesure d'endiguer la probabilité d'événements imprévisibles, incertains et insaisissables.

La conquête du PNR, « Passenger Name Record »

L' « Aviation and Transportation Security Act » adopté le 19.11.2001 aux Etats-Unis et créant la « Transportation Security Administration », TSA, a d'abord fait obligation aux compagnies aériennes opérant des vols à destination des Etats-Unis de transmettre aux douanes américaines (US Customs) les données personnelles des passagers et membres d'équipage.
Par acte du 14 mai 2002, cette obligation était étendue au bénéfice du service de l'immigration (US Immigration and Naturalization Service).
Cependant que cette obligation rencontrait quelque résistance de la part des compagnies et contrevenait à la directive 95/46/CE relative à la protection des données personnelles, des pourparlers entre les Etats-Unis et la Commission étaient engagés.

Faisant visiblement fi des interminables efforts de négociation déployés dans le cadre du « Safe Harbor », une déclaration commune est adoptée en février 2003, qui autorise les douanes américaines à avoir accès depuis le 5 mars 2003 aux « Passenger Name Records », base de données de réservation des compagnies aériennes basées sur le territoire de l'Union et effectuant des vols à destination, en partance ou via les Etats-Unis.

Au-delà du caractère peu diplomatique que revêt cette décision américaine tombée comme une injonction – qui pourrait-on abuser par ce semblant de concertation bilatérale ? – de nombreuses inquiétudes existent. Les douanes américaines ne seraient pas les seuls destinataires des ces mines d'information : les autorités fédérales américaines y auraient accès, pour des motifs d'ordre public et ainsi qu'il a été souligné par Me Wery, « les données seront partagées […] et ne bénéficieront plus d'une protection spécifique » . En outre, ces flux de données, en dehors de tout cadre légal, contreviendraient à l'économie générale de la directive, à toutes les initiatives de l'Union visant à protéger l'intimité des individus. Quant aux données sensibles, les douanes américaines se seraient engagées (FAQ N°7) à ne pas les utiliser pour identifier des individus à la frontière. Une procédure spécifique devrait être suivie avant que lesdites données ne soient communiquées à d'autres autorités américaines. Quant à la consultation par d'autres organismes, elle relève en droit américain du « Freedom of Information Act », qui autorise l'accès public aux registres d'une agence fédérale américaine sauf dérogation spéciale prévue par le FOI Act. Cependant, et sous réserve d'exception, les douanes s'engagent à ne pas appliquer l'obligation de divulgation inscrite dans le FOI Act à ce type de données (FAQ n°12).
Autrement dit, il faut donner l'accès à des données de toutes sortes mais dormez tranquille, les autorités américaines s'engagent à en faire bon usage. Elles réclament le transfert de données sensibles pour lutter contre le terrorisme, mais elles s'engagent à ne pas les utiliser dans l'enceinte des aéroports et à les transmettre très rigoureusement aux autorités compétentes. Quelque chose dans l'air ne permet pas d'adhérer gaiement à ces engagements…

« No fly list » et « Selectee list »

Ceci étant, suite au refus de la TSA de répondre à une requête déposée par l'EPIC (Electronic Privacy Information Center) dans le cadre de son droit à l'information, l'EPIC a poursuivi la TSA. Le procès a permis de révéler (après dénégation publique de la TSA) que cette administration avait dressé des listes discriminatoires de passagers suspects de présenter « un risque de piratage aérien, un risque terroriste, ou une menace pour la sécurité aérienne ou des passagers ».
Ainsi ont été dressées une « no fly list » et une « selectee list » qui empêcheraient certains passagers de voyager via ou à destination des Etats-Unis et qui en soumettraient d'autres à des examens intensifs.
Selon les informations accessibles sur le site de l'EPIC, les noms des passagers sont fournis aux transporteurs aériens par des « directives de sécurité » ou des « amendements d'urgence », stockés sur leurs systèmes et permettant de ce fait de retenir un individu dont le nom correspond avec celui stocké par les transporteurs. Un nom présent sur la « no fly list » impose à l'agent de contacter immédiatement un officier, qui procédera à la détention et au questionnement du passager. Dans l'hypothèse d'un nom figurant sur la « selectee list », la carte d'embarquement est marquée d'un « S » ou d'un caractère spécial et le passager fait l'objet de contrôles poussés lors de l'embarquement.

Ce système de listing a été crée en 1990, afin de repérer les individus « déterminés à poser une menace sérieuse pour l'aviation civile américaine ». Administrées par le FBI, ces listes sont depuis novembre 2001 placées sous la responsabilité de la TSA et n'ont de cesse de s'allonger, la TSA ayant été intégrée au ministère des affaires intérieures (Office of Homeland Security).

Fait plus curieux sinon inquiétant, les noms sont approuvés sur la base de critères secrets.

Les documents mis à la disposition de l'EPIC ne permettent pas de déterminer s'il existe effectivement un processus d'approbation formel des noms, dans lequel leur vérification serait assurée par un organisme tiers indépendant. Il n'existe par ailleurs aucune référence au « Privacy Act » de 1974, ni aucune mention du droit des individus fichés, notamment pour ce qui concerne le droit d'accès et de rectification. Apparemment en cas de plainte, la TSA dirigerait l'individu vers le bureau FBI le plus proche. Quid d'un non - Américain ?

Dans le cadre de ce procès, l'EPIC a reçu des douzaines de plaintes de passagers irrités, ayant possiblement été confondus avec d'authentiques terroristes.

La TSA souhaite également améliorer le système CAPPS I de profilage des passagers aériens, utilisé à des fins provisoires en 1996 pour assister à la détection des bagages.
Ce CAPPS II (Enhanced Computer Assisted Passenger Pre-screening System), deviendrait un instrument de profilage plus attentatoire encore à la vie privée des individus ; il distinguerait notamment entre un statut « red light » et un statut « orange light » selon le type de passager.

Dans le même esprit, le nouveau projet de l'administration Bush nommé Total Information Awareness puis Terrorism Information Awareness permettrait de croiser différentes bases de données, publiques et privées, de manière à esquisser un profil précis de chaque individu. Il viserait à « fouiller dans les archives gouvernementales et des entreprises ».

Ce projet partage les caractéristiques de CAPPS II. Au-delà de la question fondamentale de l'intrusion dans la vie privée des individus, la question de l'utilité et de l'efficacité de tels procédés est évidente. La pertinence des informations contenues dans le PNR au regard des déclarations des autorités américaines et des buts affichés de lutte anti-terroriste n'est pas, loin s'en faut, avérée. Ces mesures de surveillance jouent peut-être le rôle de la dissuasion ? Mais lorsque les risques sont inconnus, lorsque que les efforts sont concentrés sur l'individu et ses milliards de confrères en tant que danger potentiel, la surveillance démesurée dégénère en oppression et la sécurité n'en tire que peu de profit. De quel droit un Etat, aussi imbu soit-il de son importance, aurait-il la mainmise sur l'intimité du reste du Monde ?
Le besoin est urgent de soulever un débat public.
Le groupe de travail de l'article 29 appelle de tous ses vœux à une révision du compromis dans le sens d'une plus grande protection des données… qui sont d'ores et déjà communiquées en dehors de l'UE. Des associations regroupées notamment au sein de European Digital Rights, dont IRIS est le relais en France, ont entamé une campagne contre le transfert illégal de ces données personnelles. L'EPIC réclame plus de transparence, alors que la TSA s'apprête à expérimenter ses systèmes de profilage dans des aéroports de taille moyenne et prévoit la généralisation sur l'ensemble du territoire pour

l'été 2004.

A quand le passeport numérisé contenant nos données ?

« A compter du 1er Octobre 2003, toutes les personnes, y compris les enfants, quel que soit leur âge, qui souhaitent se rendre aux Etats-Unis sans visa, devront présenter un passeport individuel à lecture optique » (texte en ligne sur le site de l'ambassade des Etats-Unis en France).

Entre exigence de protection, efficacité accrue et vent paranoïaque, tout va pour le mieux dans le meilleur des mondes.

http://www.epic.org/privacy/airtravel/
http://solutions.journaldunet.com/0307/030729_securiteus.shtml
http://www.zdnet.fr/actualites/technologie/0,39020809,2137890,00.htm
http://www.liberation.com/page.php?Article=125448
http://www.zdnet.fr/actualites/technologie/0,39020809,2136957,00.htm
http://www.transfert.net/a9051
http://www.transfert.net/a8987
http://www.zdnet.fr/common/homepage/0,39021853,2135205,00.htm
http://www.liberation.com/page.php?Article=112858
http://www.transfert.net/a8763
http://www.iris.sgdg.org/les-iris/lbi/lbi-050503.html
http://www.transfert.net/a8688
http://www.transfert.net/a8634
http://www.privacy.org
http://www.zdnet.fr/actualites/internet/0,39020774,2132989,00.htm
http://www.droit-technologie.org/1_2.asp?actu_id=731
http://europa.eu.int/comm/internal_market/privacy/index_en.htm
http://www.statewatch.org/news/2003/mar/02usdata.htm

Auteur : : Melle Joëlle Béderède ***Juriste*** **. | Source : |**

01/08/2003

Comment ne pas être poursuivi par la RIAA pour partage de fichiers.
(et autres idées pour éviter d'être traité comme un criminel)

Auteur : **Electronic Frontier Fondation EFF** *Association* et **Julien Le Clainche** *Allocataire de recherche*.
Domaine : PROPRIETE_INTELLECTUELLE
Sous thème : Criminalité_informatique
Ordre juridique :

Abstract :
paratge de fichier / file sharing - Société de gestion collectives des droits d'auteur / RIAA -

Ce texte est a destination du public américain. Il a été traduit en français à titre purement informatif. L'objet de ce document est d'expliquer au public américain comment se prémunir contre la politique agressive de la société de gestion collective des droits d'auteur américaine, la « Recording Industry Association of America » (RIAA).

La « Recording Industry Association of America » (RIAA) a annoncé le 25 juin 2003, qu'elle allait introduire des actions en justice contre les utilisateurs des systèmes de partage de fichiers « Peer to Peer » (P2P). Conformément à son annonce, la RIAA cible les utilisateurs qui mettent en ligne ou qui partagent un nombre « substantiel » de morceaux de musique soumis au Copyright. La RIAA a établi qu'elle allait choisir qui poursuivre en scannant les dossiers partagés des utilisateurs, puis elle identifiera le fournisseur d'accès Internet (FAI) de chaque utilisateur. Alors, en vertu de Digital Millenium Copyright Act (DMCA), la RIAA mettra en demeure le FAI de lui communiquer le nom de l'utilisateur, son adresse, et d'autres informations personnelles dans le but de le poursuivre.

Pour savoir si votre nom à été demandé auprès d'un FAI consultez cette page :

Plus d'informations sur les procès de la RIAA et leur issue, consultez RIAA v. the People page :
http://eff.org/IP/P2P/riaa-v-thepeople.php

Alors qu'il n'y a aucun moyen de connaître exactement ce que s'apprête à faire la RIAA, qui sont les personnes qu'elle va poursuivre, ou même la quantité de musique qui est qualifiée de « substantielle », les utilisateurs des réseaux P2P peuvent prendre les mesures suivantes pour réduire le risque de poursuite.

1.
a. Assurez vous de l'absence de fichiers susceptibles de vous mettre en infraction dans vos dossiers partagés. Cela signifie que le dossier partagé contiendra environ un fichier 1) qui est dans le domaine public, 2) que vous

avez la permission de partager, ou 3) ou qui est disponible sous les licences « pro partage de fichiers », spécialement, la « Creative Commons license » (http://www.creativecommons.org/) ou d'autre licences « Open media », et b. Enlevez de votre dossier partagé tous les noms fallacieux susceptibles de prêter à confusion (http://news.com.com/2100-1025-1001319.html)avec des titres ou des artistes dont les droits sont gérés par la RIAA (par exemple « Usher », ou « Madonna »).
c. Ou désactivez les fonctions « paratage » ou « upload » de votre application P2P qui permettent aux autres utilisateurs d'obtenir une copie des fichiers qui sont sur votre ordinateur, ou de scanner votre dossier musique. Nous ne supportons pas l'idée cette option, mais il apparaît qu'elle réduit le risque de devenir dès à présent une cible de la RIAA. Pour consulter les instructions propres à chaque application, EFF suggère (mais ne peut garantir) les liens suivants :

Groskers
http://www.grokster.com/helpfaq.html#Stop%20Sharing%20files
http://www.oit.duke.edu/helpdesk/filesharing/grokster.html

Morpheus
http://www.oit.duke.edu/helpdesk/filesharing/morpheus.html
http://penguin.cc.edu/peer/peer2peer.html#morpheus

KaZaA
http://www.oit.duke.edu/helpdesk/filesharing/kazaa.html
http://penguin.cc.edu/peer/peer2peer.html#kazaa

Aimster/Madster
* Windows
http://www.oit.duke.edu/helpdesk/filesharing/aimster.html
* Mac OS
http://www.oit.duke.edu/helpdesk/filesharing/aimster_mac.html

Gnutella
* Mactella
http://www.oit.duke.edu/helpdesk/filesharing/mactella.html
* Gnucleus
http://www.oit.duke.edu/helpdesk/filesharing/gnucleus.html
* Gnotella
http://www.oit.duke.edu/helpdesk/filesharing/gnotella.html

LimeWire
* MacOS
http://www.oit.duke.edu/helpdesk/filesharing/limewiremac.html
* Windows
http://www.oit.duke.edu/helpdesk/filesharing/limewirewin.html
http://penguin.cc.edu/peer/peer2peer.html#limewire

BearShare
http://www.oit.duke.edu/helpdesk/filesharing/bearshare.html
http://penguin.cc.edu/peer/peer2peer.html#bearshare

iMesh
http://www.oit.duke.edu/helpdesk/filesharing/imesh.html

WinMX
http://www.oit.duke.edu/helpdesk/filesharing/winmx.html
http://penguin.cc.edu/peer/peer2peer.html#winmx

2.
La RIAA semble inquiéter les utilisateurs qui permettent à leur ordinateur d'être « Supernodes » sur le bandes haut débit des systèmes P2P (utilisé pour le moment par KaZaA et Morpheus). Afin de limiter les risques, assurez que votre ordinateur n'est pas utilsé comme « Supernode ». Pour en apprendre d'avantage, consultez ces pages :
http://www.whtvcable.com/fasttrack et
http://helpdesk.princeton.edu/kb/display.plx?ID=9245. Voir aussi « Disabling the Supernode function with KaZaA » (PDF 331k).

3. Si vous recevez un courrier vous informant que votre FAI à été mis en demeure de communiquer vos données personnelles, vous pouvez contacter http://www.subpoenadefense.org site sur lequel vous pourrez trouver des informations sur les moyens de protection de votre « Privacy » ainsi qu'une liste des avocats susceptibles de vous venir en aide. Contactez votre Fai pour lui demander de vos informer immédiatement si vous faisiez éventuellement l'objet d'une telle requête.
4. Si vous recevez une mise en demeure de cesser vos téléchargements, adressée par la RIAA, considérez qu'il vous est possible de contacter « Chilling Effect » (http://www.chillingeffects.org/). Dans cet esprit, EFF et quelques écoles de droit créent une galerie de modèles de lettres de réclamation et mettent à votre disposition des informations sur vos droits et sur les moyens de les faire respecter.

Vous n'aimez pas l'idée de mettre fin au partage de fichier ou changer le nom des fichiers afin de flouer les stupides robot ou les employés de la RIAA confondent vos fichiers avec des œuvres protégées ?

Nous non plus !
Rejoignez la campagne EFF pour rendre légal le partage de fichier tout en rémunérant les artistes :

1. Contactez votre représentant au Congrès des Etats-Unis (http://action.eff.org/action/index.asp?step=2&item=2713) et demandez un débat sur les moyens de sauver le P2P et de rémunérer les artistes.
2. Apprenez en plus quant aux alternatives possibles. La page P2P de EFF rassemble parmi les meilleures idées et décrit comment les évolutions technologiques ont été gérées par le passé. http://www.eff.org/share/
3. Informez votre entourage, ou même des inconnus sur les dangers que fait peser la RIAA sur l'internet , l'innovation, et le choix des consommateurs. Il y a plus de 57 millions d'américains qui utilise le partage de fichiers – Plus que le nombre de gens qui ont votrés pour le président Bush – Et de millions de plus à travers le monde – Il y a de bonnes chance que la personne assise devant vous dans le bus, que vous croisez dans la rue ou qui conduit la voiture à coté de la votre pratique le P2P lui aussi. Entammez la

conversation.
4. rejoignez l'EFF et supporter leur effort de protection du partage de fichiers.

Auteur : : **Electronic Frontier Fondation EFF** ***Association*** **et Julien Le Clainche** ***Allocataire de recherche*****. | Source : Electronic Frontier Foundation |**

NOTES

Texte traduit de l'anglais par Julien Le Clainche.

LIENS

- http://www.eff.org
- http://www.eff.org/IP/P2P/howto-notgetsued.php