l'Association canadienne du droit
des technologies de l'information

July 24, 2009/24 juillet 2009

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors Robert Currie, Chidi Oguamanam and Stephen Coughlan of the Law and Technology Institute of Dalhousie Law School. Part 2 of this newsletter is prepared by Professors Pierre Trudel and France Abran of the L.R. Wilson Chair in Information Technology and Electronic Commerce Law, Université de Montréal.

Les auteurs de la première partie du présent bulletin sont les professeurs Robert Currie, Chidi Oguamanam et Stephen Coughlan de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie. Les professeurs Pierre Trudel et France Abran de le Chaire en droit des technologies de l'information et du commerce électronique L.R. Wilson de la Faculté de droit de l'Université de Montréal ont rédigé la seconde partie du présent bulletin.

Part 1

Copyright Law Consultations

The federal government has announced public consultations regarding copyright laws.

The consultation period will run from July 20 to September 13, 2009.Sept. 13 and will include an online discussion forum, a centre for posting detailed submissions, and a number of round tables to be held across Canada. In addition, two "town hall" meetings (one in Toronto and one in Montreal) will be webcast on the consultation site.The government has indicated its intention to table new copyright laws in the fall of this year.

Downloading of Public Inquiry Exhibits to the Web

The Inquiry into the Death of Howard Hyde has concluded that video footage surveillance footage of the deceased while he was being held in custody will not be directly downloaded to the internet. Howard Hyde was a schizophrenic man who was arrested by police and in the course of that arrest was tasered. He was eventually taken to the Central Nova Scotia Correctional Facility and died some hours later while still in custody.Approximately 16 hours of video footage of Hyde existed, and much of it was to be introduced in evidence at the Inquiry.

The issue of whether to download the videos to the web arose in a somewhat unusual fashion.The Inquiry is being webcast, and so is available to anyone who wishes to watch it by live stream on the internet. Judge Derrick, who is conducting the Inquiry, observed that webcasting itself will:

a) enhance the public aspect of the Inquiry in keeping with the mandate conveyed by the Fatality Investigations Act;

b) promote public interest in and public discussion of important issues arising from the Inquiry, particularly the treatment of the mentally ill in the community and in the justice system;

c) allow persons to observe the hearings without being forced to travel to Halifax.

Because of this webcasting, the surveillance video could be seen by any member of the public who was watching when the footage was shown as part of the proceedings. However, the inquiry is not maintaining a website, and so that would have been the only way in which the video was accessible. No application for release of the video footage was made by a media organization or others: rather, the Nova Scotia Government Employees' Union (NSGEU), on behalf of the correctional workers who appeared in the footage, made an application for an order preventing the video from being directly downloaded. Judge Derrick noted that this action by the NSGEU "seems to suggest the existence of a presumption that the DVD should be directly downloaded to the internet in the normal course of the Inquiry process" and that "The parties that support direct downloading of the DVD regard internet access to be the only option consistent with the presumptive openness of judicial proceedings". Ultimately she concluded that this was not the case.

Judge Derrick worked on the presumption that media access to the surveillance footage and freedom of expression were live considerations in the case even in the absence of any direct application by

the media: it was obvious that they would wish to make us of the material if it were downloaded. She also noted that there was no question that the open court principle applied and that the proceedings had to be open and accessible. The issue, she held, was whether that led to the conclusion that exhibits which happened to exist in a digital form therefore had to be directly downloaded to the internet. The open court principle did not lead to that conclusion, she held:

> 37 If freedom of expression guarantees under section 2(b) of the *Charter* required internet downloading of court hearings so that the broadest possible access could be achieved, then courts would be obligated to webcast all their proceedings.

Accordingly, the NSGEU's application was granted, not so much because they had succeeded in justifying a departure from the norm, but because the norm did not require the thing which the NSGEU opposed.

Judge Derrick noted that two further questions arose: whether she should provide access to the footage once it was an exhibit for the purpose of direct downloading to the internet; and whether the fact that the video surveillance would be filmed as part of the webcasting of the Inquiry removed the argument against direct downloading (since the images would be streamed to the internet in any event). She took account of a number of other considerations in deciding that these issues did not affect her conclusion. She noted that the correctional officers in the footage had a privacy interest which had been asserted on their behalf, and would be compromised if the footage were made generally available on the internet. She noted as well that there were many other prisoners in the facility who were visible in the footage, that most of them would by this time have been released and would be trying to get on with their lives, and that they too had a privacy interest. Further, the surveillance video had no accompanying sound, and its presentation at the Inquiry would include witnesses explaining what was going on at each point. Noting that context was crucial, Judge Derrick held:

> Filming of the Inquiry0edings will capture the witnesses' testimony about the video surveillance and any submissions that will be made on what inferences should be drawn from it. Direct downloading of the images will not. Directly downloading the video surveillance will send images to the internet without any context. (para 67).

She concluded that direct downloading would potentially distort the facts, and would also make it impossible to impose any practical limits on the use to which the footage was put. These further factors reinforced her conclusion, that:

> the existence of technology that permits direct downloading does not create a constitutional right for the general public or the media to have that technology employed for the purpose of providing access to the evidence in the same format that it is presented to the Inquiry. (para 78)

Making Child Pornography

The Manitoba Provincial Court has found an accused guilty of a charge of making child pornography by taking digital images. What makes the case somewhat unusual is that the digital images themselves were not found and were not entered into evidence: the convicted was based on the testimony of the child who reported that the accused had taken pictures of her, and considerable circumstantial evidence gleaned from his digital camera and computer.

The accused was charged after a six year old girl, a neighbour who had been playing with the accused's daughter, reported to her mother that she had taken a shower at the accused's house and that he had taken pictures of her. She told police (and adopted the statement in her testimony) that he had told her to pose in particular ways and that she had seen the flash of his camera go off five or six times. The police executed a search warrant at the accused's house the next day: the accused did not answer the door, and after two minutes of knocking and yelling the police forced the door open. They found the accused coming upstairs from the basement. The subsequent search discovered a computer power cord plugged into an outlet in the kitchen and an HP laptop (that was normally kept in the kitchen) on the top shelf of the downstairs cold storage room underneath the floor joists. In addition, computers, hard drives and

optical disks that were reported to be used only by the accused were found in the basement; an IBM laptop said to belong to the accused was found in a number-locked briefcase behind the passenger seat in the accused's truck in the detached garage, and; a digital camera was found in a camera case with three SD cards located behind the passenger seat in C.M.'s truck in the detached garage.

Police were able to examine data on the computers, the camera, and the SD cards. The trial judge relied on this "overwhelming" forensic evidence as supportive of the claims made by the girl, even though no pornographic images of her were found. What the evidence did show was the following:

> The SD cards contained images, deleted images that could still be viewed, and a series of images that had been wiped clean by a software program (PGP) and could not be viewed;
>
> The PGP program had been used on the SD card on the date in question between 8:27 p.m. and 9:14 p.m.. Six minutes prior to this, pictures from the camera had been uploaded to the HP laptop. Each image had been wiped five times;
>
> Approximately two minutes after the last time the PGP program was run, a series of images of a black room was taken within a three minute time span from 9:16 p.m. to 9:19 p.m.. Evidence was given that that simply deleting images allows them to be retrieved later, while wiping images clean and overwriting them means that they can never be retrieved or viewed;
>
> Nine digital images taken with the camera on the date in question between 8:16:39 p.m. and 8:18:24 p.m. had been uploaded to the HP laptop between 8:21:19 p.m. and 8:21:30 p.m. (six minutes before the SD card was wiped). These photographs were taken in the accused's residence and showed the girl with wet hair. These photos were not found on any of the SD cards;
>
> A series of other images had been uploaded to encrypted files on the HP laptop, and the R.C.M.P. had not been able to crack the password and view the files. However, it was possible to determine that five of those images were taken on the day in question between 7:21 p.m. and 7:30 p.m., were uploaded between 7:41 p.m. and 7:42 p.m., and were opened between 7:43 and 7:56 p.m.. One of these images was then copied at 8:46 p.m. to an encrypted file entitled "PROMO_PGP_G T: Porno Mine 2005-05-11 Best ";
>
> At the time when the search warrant was being executed, a wave file was activated on the HP laptop. This typically means that hardware such as a power cord, mouse or thumbstick has been disconnected from the laptop. Also at that time the computer entered hibernation mode, which was probably as a result of a command or closing the lid.

The trial judge noted that this evidence showed that at least five missing images were taken at the time that the girl testified five or six nude photographs were taken of her. It showed that five images were saved in an encrypted file, and that a series of pictures taken at this time were wiped clean from the camera. This encryption and wiping of pictures was indicative of someone who wanted to hide the pictures, the trial judge noted, particularly when contrasted to the other pictures on the SD cards and computer that were not treated in the same way. In addition the forensic evidence made it appear that the laptop had been taken from the kitchen and hidden in the floor joists of the basement at the moment the police arrived to execute a search warrant. In the circumstances the trial judge concluded that the accused had taken photographs of the girl which met the definition of child pornography, and therefore was guilty of the charge of making child pornography.

Privacy and Social Networking

The Privacy Commissioner of Canada has rendered decisions with regard to a number of complaints against Facebook Inc. under the Personal Information Protection and Electronic Documents Act (PIPEDA). The complaints were brought by the Canadian Internet Policy and Public Interest Clinic (CIPPIC), and concerned various policies, including default privacy settings, collection and use of users' personal information for advertising purposes, disclosure of users' personal information to third-

party application developers, and collection and use of non-users' personal information. In particular issues of knowledge and consent, data retention, and security safeguards were crucial. The Commissioner concluded that some of the complaints were not well-founded, while others were well-founded but were adequately resolved by corrective measures proposed by Facebook. With regard to the areas of third-party applications, account deactivation and deletion, accounts of deceased users, and non-users' personal information, the Commissioner found that the complaints were well-founded, and there remained unresolved issues where Facebook had not as yet accepted the Commissioner's recommendations for corrective measures.

One of the complaints concerned Facebook's practice of collecting the date of birth of users. The Commissioner concluded that Facebook's reasons for doing so – to enforce the site's minimum age in order to protect the safety of minors, and to ensure that users used their real identities on the site so as to lessen the incidence of inappropriate content and behaviour and promote a safe and respectful environment for all users – were legitimate. As a result, Facebook was entitled to require users to provide this information. However, the Commissioner found that Facebook was not sufficiently open with users about the use of that data, which was something especially valued by identity thieves. In particular, although users could choose not to make their date of birth public, it was not clear that this only meant that the information would not appear on the user's profile. Users would be led to believe that opting out would mean that their date of birth would not be among the information provided to targeted advertisers: in fact that was not the case. Accordingly Facebook was in contravention of PIPEDA in this regard. Facebook did agree to implement changes to better notify users in this regard.

A further complaint dealt with Facebook's use of default privacy settings, which CIPPIC in effect argued steered users in particular directions. For the most part the Commissioner had no objection to Facebook's practice, rejecting the analogy to an "opt-out" approach. She noted that the Facebook context was unlike most other situations, because "Facebook users proactively and voluntarily upload their personal information to the Facebook site for the express purpose of sharing it with others (para 88)". She suggested that although the ideal would require users to make their own selections while registering, rather than there being preselected choices, the sheer number of settings could make that impractical and serve as a disincentive to users to register. Accordingly, she held that it was acceptable for Facebook to preselect choices, so long as those choices met the reasonable expectations of users and users were reasonably informed how their data would be used in accordance with the settings. For the most part, she concluded, that was the case, with two exceptions. First, the default setting for sharing photographs was to share them with everyone, which she held was inconsistent with other default settings. Second, the default privacy setting for search engines was to allow users to be searchable, but there was no evidence this matched user's expectations. Facebook also proposed corrective measures in this regard, which would allow users to select a low, medium or high privacy setting and would make it easier for users to configure privacy settings.

The Commissioner also found it reasonable for Facebook to require that users receive ads as a condition of joining, since Facebook needed revenue to run the site, which was free to users. However, the Commissioner found that Facebook was not transparent enough with users, in particular in not informing them that there were certain types of advertising it was not possible to opt out of. Once again Facebook proposed adequate corrective measures.

Not all well-founded complaints were satisfactorily resolved. One of the complaints was that Facebook allowed third party application developers potentially unlimited access to personal information, including making all of a user's personal information accessible to third parties. Facebook denied that this was so, claiming that developers had a limited ability to access data. The Commissioner noted that the only limits which appeared to be imposed were contractual ones rather than technological ones. She held that Facebook ought to have safeguards in place that would not merely forbid but would prevent developers gaining access to personal information they did not need. She also raised the question of how much personal information an application typically would need to run, which suggested that Facebook was in any case giving developers more

information than they required. The Commissioner found, therefore, that the safeguards Facebook regarded as adequate were not sufficient, and encouraged them to reconsider.

Similarly Facebook had not immediately chosen to comply with the Commissioner's recommendations with regard to deactivated accounts. Although Facebook provided users with the option of deactivating an account, the data in such accounts was retained indefinitely. Facebook defended this practice on the basis that a majority of deactivating users reactivated their account within weeks. The Commissioner noted that this argument did not require the indefinite retention of data and encouraged Facebook to reconsider her recommendation.

Not all complaints were considered well-founded in the first place. For example, one complaint was that Facebook was not notifying users of new purposes for which their personal information would be collected, used, or disclosed. However, there was no evidence that Facebook had failed to inform its users of new uses of their personal information, and so this complaint was not well-founded. Similarly the Commissioner found no evidence that Facebook was willfully misleading or deceiving users about the purposes for which it collected information or was obtaining consent through deception.

Other aspects of the complaint dealt with collection of personal information from sources other than Facebook, accounts of deceased users, and personal information of non-users, among other issues.

2ième partie

Interdiction judiciaire de diffuser des images intimes sur Internet

Le tribunal a accordé plus de 40,000$ en dommages intérêts à une personne qui se plaignait que son ex ami avait diffusé sur Internet des séquences de ses ébats sexuels. Des photos et des vidéos de la jeune femme la montrant nue ou en train d'avoir des rapports sexuels avec le défendeur s'étaient retrouvés sur des sites Internet après qu'elle eut mis fin à leur relation amoureuse. Le tribunal qualifie ces gestes d'ignobles et exprime son indignation. Le jugement ordonne au défendeur de ne pas créer de site Internet et d'adresse de courrier électronique au sujet de la demanderesse ou portant le nom de cette dernière. Il lui interdit d'écrire, diffuser ou transmettre sur tout site Internet quelque information, commentaire ou photographie que ce soit de la demanderesse ou se rapportant à cette dernière.

Le jugement ordonne en outre au défendeur de ne pas diffuser, reproduire, communiquer et/ou transmettre par quelque moyen que ce soit, y compris par Internet, messagerie-texte, courrier ou autrement toute photographie, tout vidéo et tout courriel concernant la demanderesse; de remettre à la demanderesse toute photographie de la demanderesse sur support papier, qui est à caractère sexuel, comportant de la nudité ou montrant la demanderesse en sous-vêtements et de ne pas détenir, en format électronique, papier ou autre, toute photographie et tout vidéo de la demanderesse à caractère sexuel, comportant de la nudité ou montrant la demanderesse en sous-vêtements. Il est aussi ordonné que les photographies, CD-ROM et clé USB déposées dans le cadre de ce recours demeurent sous scellés pour qu'elles ne puissent être consultées que sur autorisation d'un juge de la Cour supérieure.

- *J.G c. M.B.* Cour supérieure, 2009 QCCS 2765 (CanLII), 19 Juin 2009.

Injonction interdisant la diffusion de « propos diffamatoires » sur Internet

En mai 2005, le défendeur-intimé a inauguré un site Internet qui loge à l'adresse rawdon-qc.net. Ce site Internet abrite un forum de discussion sur lequel des citoyens commentent l'actualité municipale de Rawdon. Le tribunal estime que les propos rapportés à la requête introductive d'instance en injonction et en diffamation « constituent une apparence de droit claire à l'effet que nous sommes en présence d'atteintes sérieuses à la réputation. » Les auteurs de ces propos utilisent des pseudonymes qui ont été identifiés par une firme d'experts, grâce aux informations découlant d'une l'ordonnance d'injonction de type Anton Piller rendue dans le présent dossier. Ce qui amène le tribunal à conclure que l'on a démontré une apparence à l'effet que le forum de discussion sur Internet est devenu, en l'espèce, le moteur de l'excès et de la démesure, l'accélérateur et l'amplificateur de la diffamation contre les personnes physiques et contre la municipalité demanderesses. Dans son appréciation, le Tribunal a pris en compte « le contexte particulier et notamment la taille relativement petite de la Municipalité de Rawdon ainsi que l'impact et la grande force de frappe d'une attaque pernicieuse sur l'Internet, dans un milieu aussi restreint, pour ne pas dire en vase clos ». En plus, la juge est d'avis que l'utilisation de l'Internet comme moyen de diffusion de la diffamation rend pratiquement impossible la correction de l'impression négative laissée par les propos diffamatoires. Quant aux propos diffamants qui visent ou englobent la Municipalité de Rawdon, le jugement affirme que cela constitue une attaque à la stabilité de l'administration municipale et une attaque à la démocratie.

Le jugement prononce une série d'interdictions comme celle de « cesser immédiatement de diffuser, publier, reproduire ou faire circuler les propos diffamatoires, en tout ou en partie, sur le forum de discussion du site Internet qui loge à l'adresse rawdon-qc.net ou sous tout autre médium, verbalement ou par écrit ». Il ordonne de ne pas tenir de propos diffamatoires contre les demandeurs sur un forum de discussion ou en tant qu'administrateur, hébergeur ou modérateur de forums de discussion sur tout autre site Internet. Les défendeurs sont

enjoints de désactiver et de retirer du réseau Internet, dans les douze heures de l'ordonnance obtenue, le forum de discussion sur le site Internet qui loge à l'adresse rawdon-qc.net et de retirer du réseau de l'Internet tout document ou texte reproduisant les propos diffamatoires, en tout ou en partie, dudit site Internet. Le jugement ordonne en outre de respecter l'interdiction de prononcer à l'endroit des demandeurs-requérants des propos diffamatoires, tant verbalement que par écrit et sous toute forme que ce soit. Il est pareillement interdit d'émettre à l'endroit des demandeurs-requérants et de tenir à propos des demandeurs-requérants des propos diffamatoires ou injurieux.

- *Rawdon (Municipalité de) c. Leblanc (Solo)*, 2009 QCCS 3151 (CanLII), 9 juillet 2009.

Validité d'un constat d'infraction et exigences de signature

Il s'agit d'une requête verbale en rejet du constat au motif que le constat d'infraction produit en preuve est invalide parce qu'il n'est pas signé, et ne fait que mentionner le nom du policier (« GAGNON PASCAL »). Le tribunal invoque l'article 75 de la *Loi concernant le cadre juridique des technologies de l'information* qui dispose que : « Lorsque la loi prévoit qu'une signature peut être gravée ou imprimée ou apposée au moyen d'un fac-similé gravé, imprimé ou lithographié ou qu'une marque peut l'être au moyen d'une griffe, d'un appareil ou d'un procédé mécanique ou automatique, elle doit être interprétée comme permettant, sur support papier, d'apposer la signature autrement que de façon manuscrite ou de faire apposer la marque personnelle par quelqu'un d'autre. Une telle disposition n'empêche pas de recourir à un autre mode de signature approprié à un document, lorsque ce dernier n'est pas sur support papier.»

Étant donné qu'aucune preuve selon laquelle il y aurait eu atteinte à l'intégrité du document de constat d'infraction produit à la Cour n'a été présentée, le tribunal se déclare dans l'impossibilité de conclure que le constat d'infraction ne rencontre pas les exigences de la loi et des règlements.

- Montréal (Ville de) c. Bolduc, Cour municipale Montréal, 2009 CanLII 30774 (QC C.M.), 12 juin 2009.

Recommandation « Commerce électronique et procédure collective » – France

Dans un avis rendu à l'issue d'une consultation menée par l'un de ses groupes de travail, le Forum des droits sur l'Internet recommande de tenir compte de la variété des modèles du commerce en ligne, ce qui nécessite une connaissance des spécificités de cet univers par les administrateurs et les liquidateurs judiciaires. Par exemple, sur Internet, un cybermarchand peut être présent sur les plates-formes de mise en relation, sans posséder son propre site de vente en ligne. Les comparateurs de prix, très prisés par les consommateurs, renvoient quant à eux vers des cybermarchands. Dans ce contexte, le Forum a répertorié les actions suivantes à mener par les professionnels comme de vérifier l'existence de tous les canaux de distribution du marchand : en ligne et hors ligne afin de pouvoir agir sur l'ensemble de ceux-ci. Le Forum recommande aussi de désactiver le site marchand, ou au minimum, fermer la page de validation de la commande en cas de liquidation, sauf en cas de poursuite exceptionnelle de l'activité. Le Rapport conseille aussi de contacter par courrier électronique les clients du cybermarchand pour les prévenir de la mise en liquidation judiciaire. Le Forum estime qu'il est de bonne pratique d'obtenir les éléments techniques du site (code d'accès, code source…) permettant au liquidateur d'intervenir sur celui-ci, et notamment de poster les messages d'information dans toutes les langues de la clientèle visée. Enfin, il est recommandé de prendre contact avec les plates-formes et les comparateurs de prix pour demander le déréférencement du cybermarchand en liquidation , et indiquer la situation de liquidation du cybermarchand à côté de la notation en cas de poursuite de l'activité.

- Tiré de Forum des droits sur l'Internet, *Redressement et liquidation des cybermarchands : pour un dispositif proportionné et adapté au monde numérique*, communiqué de presse, 16 juillet 2009.
- Forum des droits sur l'Internet, *Recommandation – Commerce électronique et procédure collective*, 15 juillet 2009.

Une mise en demeure constitue un moyen adéquat de notifier un hébergeur de faits litigieux – France

Le Tribunal de grande instance de Paris a estimé dans un jugement du 10 juillet 2009 qu'une mise en demeure peut constituer une notification suffisante à un hébergeur afin de lui permettre d'acquérir connaissance du caractère illicite de contenus hébergés. En l'espèce, les juges ont conclu que la mise en demeure avait permis à YouTube d'avoir une connaissance effective des faits litigieux « dès lors que l'identification des vidéogrammes [concernés] était rendue possible par la seule saisie (...) des termes Petit Ours Brun et ne présentait pour l'hébergeur aucune difficulté de nature technique ». En négligeant de procéder au retrait des vidéos litigieuses à la réception de ce courrier, la plateforme avait engagé sa responsabilité d'hébergeur et porté atteinte aux droits d'auteur des entreprises demanderesses.

- *Bayard Presse c. YouTube LLC*, Tribunal de grande instance de Paris 3ème chambre, 2ème section, 10 juillet 2009.

26 000 signalements de contenus illicites transmis à la police – France

Depuis janvier 2009, la nouvelle version du service accessible sur Internet-signalement.gouv.fr est ouverte à tout type de crimes et délits : escroquerie, incitation à la haine raciale, etc. Résultat : le nombre de signalements a explosé, avec ce *« portail officiel des contenus illicites de l'Internet ».* En six mois, la police, dont 01net. s'est procuré les chiffres officiels, a enregistré 26 222 signalements, quand, sur toute l'année 2008, elle en avait reçu près de 13 000. Selon la police, ce sont chaque semaine autour de 900 sites qui lui sont signalés.

- Arnaud DEVILLARD, « 26 000 signalements de contenus illicites transmis à la police », *01net.*, 6 juillet 2009.

Un agrégateur de flux RSS n'est pas responsable des contenus – France

Un jugement au fond rendu le 25 juin 2009 par le Tribunal de grande instance de Nanterre s'est prononcé sans ambiguïté pour la qualification d'hébergeur des agrégateurs de flux RSS. Le site Wikio.fr avait relayé une information sur la supposée liaison entre Olivier Dahan, réalisateur du film *La môme*, et Sharon Stone, à partir d'un flux RSS de Gala.fr. L'internaute avait ainsi accès au titre et à la brève et il pouvait aussi se rendre d'un clic sur le site source de l'information pour lire le même article illustré d'une photo. Les demandeurs considéraient que Wikio.fr était éditeur du site et donc responsable de l'atteinte au droit à sa vie privée. Le tribunal a plutôt estimé que Wikio se limite à regrouper sur une même page différents flux RSS émis par les sites auxquels il est abonné. Ce sont ces derniers qui ont la maîtrise du contenu de leur flux. Wikio n'effectue aucune intervention sur les textes mis en ligne. C'est pourquoi le tribunal conclut que le site *« ne peut être considéré comme un éditeur au sens de la loi pour la confiance dans l'économie numérique, mais comme un agrégateur de flux RSS dont la responsabilité ne peut relever que du seul régime applicable aux hébergeurs ; étant, relevé que l'automaticité de la réception des flux RSS rend quasiment impossible un filtrage de contenus illicites. ».*

- *Olivier D. c. Wikio*, Tribunal de grande instance de Nanterre, 1ère chambre, 25 juin 2009, *Legalis.net*.
- Hélène PUEL, « Un agrégateur de flux RSS n'est pas responsable des contenus » , *01net.*, 8 juillet 2009.
- « L'agrégateur de flux RSS hébergeur », *Legalis.net*, 7 juillet 2009.

L'adresse IP qualifiée de « donnée personnelle identifiante » – France

Selon un jugement rendu le 24 juin 2009 par le Tribunal de grande instance de Paris (TGI), l'adresse IP est une donnée personnelle qui permet de

retrouver la personne physique qui a mis en ligne un contenu. Selon le tribunal, *« Au regard de la technique existante, cette adresse apparaît être le seul élément permettant de retrouver la personne physique ayant mis en ligne le contenu »*. Dans cette affaire, un humoriste avait reproché à Google de ne pas avoir retiré promptement les films contrefaisants de son site de partage Google videos, d'avoir remis en ligne les contenus et de n'avoir pas collecté les données d'identification de ceux à l'origine de leur mise en ligne. En tant qu'hébergeur, Google videos avait l'obligation de faire cesser la diffusion illicite des œuvres concernées. Pour cela, le demandeur aurait dû notifier les faits litigieux de manière conforme aux exigences de la Loi. Comme il n'a pas communiqué d'indications précises des titres et de la localisation des films à retirer, le TGI a jugé que Google ne pouvait pas voir sa responsabilité engagée. Il ne pouvait pas davantage être poursuivi pour leur remise en ligne. Pour le tribunal, *« la société Google n'étant pas soumise à une obligation générale de surveillance, ne peut être poursuivie pour la remise en ligne de contenus illicites identiques dès lors que les demandeurs n'ont pas fait droit à sa proposition de prise d'empreintes sur leurs oeuvres pour éviter la récidive ni n'ont utilisé l'outil logiciel mis à leur disposition pour dénoncer les nouveaux contenus illicites »*.

- Tiré de « L'adresse IP est une donnée personnelle identifiante », *Legalis.net*, 9 juillet 2009.
- *Jean-Yves Lafesse et autres c. Google et autres*, Tribunal de grande instance de Paris, 3ème chambre, 3ème section, Jugement du 24 juin 2009, *Legalis.net*.

À signaler

- Serge KABLAN et Arthur OULAÏ, « L'essence des approches du droit cyberspatial et l'opportunité de la co-régulation », (2009) 39 R.G.D. 5-49.
- *Lafontaine c. Vidéotron*, 2009 QCCS 3189 (CanLII), 14 juillet 2009. Le tribunal autorise l'exercice d'un recours collectif, soit une action en dommages-intérêts contre Vidéotron Ltée, pour avoir facturé l'intégralité des frais relatifs à des forfaits de services Internet alors que ces services n'ont pas été entièrement dispensés et pour avoir causé des dommages en privant les abonnés du service auquel ils étaient en droit de s'attendre.