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

November 13, 2008/13 novembre 2008

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

Criminal Law: E-Mail Fraud

The Ontario Court of Justice has delivered its ruling in *R. v. Asmelash*. In this case, the accused is charged with one account of defrauding Katherine Brown, a deaf American and staffer of social security office in Kentucky via e-mail fraud. Ms. Brown received an e-mail in her workplace in August 2004 which solicited some help. The e-mail was written by a "Mary Jones" who claimed to be writing from Kuwait. Mary Jones was dying of cancer and wanted someone to assist her to distribute to the needy and deserving the sum of $8.6m bequeathed to her by her late husband. From then on, Ms. Brown became involved in an exchange of e-mails after agreeing to receive the money to do Mary Jones' bidding. She was directed also to correspond with an intermediary company and linked to the latter professional website. The company was to assist her to access the funds. Ms. Brown was required to set up an account with the intermediary company (International Payment House) which has a Toronto location address. As matters progressed, Ms entertained a barrage of demands for payment of diverse fees including, among others, $7,500 for setting up and activating of the account, $6,250 for non-residence tax, $5, 850 for stamp duties, etc. For each demand, she was given the name of an individual and details of the account numbers and wiring information for the lodgment of the funds in Canadian Banks, including CIBC and Desjardins Credit Union in Toronto. At a point, she was promised the sum of $100, 000 for herself. Then, when Ms Brown got a demand for $25,000 for "drug/anti-terrorist certificate", it became clear to her that she was the victim of a scam. According to the court, "This was a fraudulent scheme sent out via e-mail in a general way with the hope of finding someone gullible, desperate, or greedy enough to take the bait. Unfortunately for Ms. Brown, she did" (para 66).

Police investigation linked the two Toronto Accounts with CIBC and Desjardins Credit Union to the accused, an erstwhile employee of Royal Bank of Canada. The accused defence hinged on the theory that she also was a victim of the scam. She testified that her two bank accounts were used without her knowledge to carry out the fraud on the complainant. Upon reviewing her testimony, the court concluded that she lacked credibility as she was mostly evasive and inconsistent, self-serving. Essentially, "her testimony was given in the attempt to fit the facts that existed rather than following the path of a reliable and honest recollection" (para 61). The court evaluated the patterns of withdrawal of the monies transferred into the accounts, and noted that since the bank did not notify customers of payment of monies, Ms. Asmelash's withdrawals suggested she knew of payments being made at specific dates. Also, the nature of information required to be supplied for the complainant to deposit the funds and the information required for anybody to withdraw them from the accused's account were not likely to be obtained by third parties involved in the theft of the accused's identity. In the court's view if the relevant information were available to persons other than the accused, they may have as well set up entirely different accounts in the accused's name without taking the risk of making the transaction with the accused's pre-existing bank accounts. Also, the accused expenses at a time when she was out of job did not suggest that she was oblivious to moneys being paid into her account.

The court noted that "the nature of the fraud was likely beyond the capacities of a person like Ms Asmelash acting alone. There are numerous e-mails from allegedly numerous persons from different e-mail accounts. Further, there was a very official website of International Payment House… The Crown has not proven beyond reasonable doubt that Ms Asmelash was the only participant in the e-mail fraud but that is not necessary for the Crown to prove. Consequently, I find Ms. Asmelash guilty as charged" (paras. 83, 84).

Criminal Procedure: Electronic Disclosure is Adequate for Section 7 Purposes

In *R. v. Oszenaris*, the Newfoundland and Labrador Court of Appeal considered an appeal from the finding of a trial judge that disclosing materials to the defence in electronic format did not constitute "meaningful" disclosure and thus violated the s. 7 *Charter* rights of the accused. The accused had been arrested and charged with various drug offences. The R.C.M.P. were using a case management called "SUPERText" that allowed for disclosure of documents in electronic form on CD-ROMs, which the Crown asserted could be used by anyone with basic computer skills. The Crown offered training in the use of the software, and the accused's lawyer had attended a training session. Nonetheless, the accused's lawyer applied for disclosure in hard copy instead of electronic form, and the Crown resisted the application. The trial judge ordered the Crown to disclose the documents in hard copy, on the basis that: even with the training, the accused's counsel was not "computer literate" enough to confidently use the software; there were concerns with the adequacy of the Crown's organization of the documents; and all of this raised the possibility that counsel might overlook relevant documents, thereby endangering the accused's right to full answer and defence by counsel of his choice.

Barry J.A. for the Court of Appeal noted that the trial judge had correctly identified that the overall question was whether, in the circumstances of this case, e-disclosure met the Crown's disclosure obligation, or whether failure to disclose in hard copy violated the accused's right to full answer and defence. He further noted that the trial judge had identified that there were two competing lines of caselaw as to whether CD-ROMs were adequate disclosure. Positing that "electronic disclosure is meaningful if the disclosure materials are reasonably accessible" on the facts of each case, Justice Barry further noted that accessibility can depend on the manner in which the data is organized and formatted, as well as on counsel's abilities (para. 19). However, "[i[n today's world, it is not unreasonable to expect that counsel will be in a position to utilize a computer for the management of large volumes of material" (para. 20). To discharge the accused's burden of proving a s. 7 violation on a balance of probabilities, it was insufficient for the accused's counsel to raise merely general concerns with counsel's own ability to use the information—rather, the evidentiary record must indicate that the document software in question has technical flaws that create difficulty in accessing some of the information. Here, the evidence given about the SUPERText had not disclosed significant flaws that compromised counsel's ability to use the documents. This was despite the fact that the trial judge had expressed "concern as to whether defence counsel could adequately identify such flaws for the court," given her lack of computer skills (para. 21). Accordingly, the trial judge's acceptance that counsel was in danger of overlooking something did not amount to proof on a balance of probabilities that the disclosure was deficient. The stay imposed by the trial judge was lifted and the case remitted for trial.

Domain Name Decisions

"yourcommunityrealty.ca"

In *Vivian Risi v. Ray Fattahi*, a 3-member CIRA panel (Allsebrook, Magnusson and Fashler, Chair) considered a dispute over the domain name yourcommunityrealty.ca. The Complainant ("Risi") carries on business as a realtor and purveyor of related services in Toronto. She registered the mark YOUR COMMUNITY REALTY in 2005, and uses the mark to advertise her business, including her website yourcommunityrealty.com. The Registrant ("Fattahi") operates a website at gooya.ca, which provides news and a business directory geared towards the Persian-Canadian community in Toronto. He registered the disputed domain name in 2006,

and linking to it redirects users to gooya.ca, which contains advertising for several realtors. In May 2008, Risi received a notice of domain name auction for yourcommunityrealty.ca. While Fattahi denied any involvement in the sale, the Panel noted that his administrative contact information was given as the contact point for the auction.

The Panel first considered the requirement under 4.1(a) of the CIRA Policy that a Complainant prove that the disputed name is "confusingly similar" to the Complainant's mark. They noted that the domain name (read, as is required under the Policy, without the "dot-ca" suffix) was identical to the mark, particularly since elimination of the spacing between the words "does not alter the appearance, sound or meaning of the Domain Name at all" (p. 4). Accordingly, the domain name was found to be confusingly similar to the mark. The Panellists next considered the requirement under 4.1(b) of the Policy that the registration have been made "in bad faith." It focused on whether the Registrant had registered the domain name primarily for the purpose of transferring it to the Complainant or a competitor, which constitutes bad faith under 3.7(a) of the Policy. Noting that prudent businesspeople will check the Canadian Trade-Marks Database before registering a domain name, and that Fattahi at least ought to have been aware of Risi's mark by the time he registered, the Panel further found as fact that the words contained in the name had nothing to do with the gooya.ca website, and that Fattahi himself had offered to sell the domain name to Risi. Citing previous CIRA authority that a Panel may use circumstantial evidence to establish bad faith, the Panel concluded that Fattahi had registered the name for the purpose of selling it to Risi, and "[f]ailing such sale, …was positioned to benefit from traffic intended for [Risi] by the sale of advertising space to realtors competing with [Risi]" (p. 6). Accordingly, bad faith was made out.

The Panel finally considered whether Fattahi had a "legitimate interest" in the domain name, under 4.1(c) of the Policy. It noted that of the various criteria constituting legitimate interest under 3.6 of the Policy, those set out in paras. 3.6(a), (b) and (c) all require that the Registrant be acting in good faith. Given the Panel's earlier finding that Fattahi had been acting in bad faith, Risi had met her "light burden" in relation to those paragraphs. None of the other criteria in 3.6 were met by the domain name, and Fattahi's own representations (which had been described by the Panel as "far-fetched and obviously contrived") were themselves convincing of the fact that he had no legitimate interest. The domain name was ordered transferred to Risi.

Musical Copyright Over the Internet: Tariff 22 B-G Decision of the Copyright Board of Canada

In *Statement of Royalties to be Collected by SOCAN for Communication to the Public by Telecommunications in Canada, of Musical and Dramatico-musical Works*, the Copyright Board of Canada released its latest decision on Internet Tariff 22 B-G on October 24, 2008. This decision is a follow-up to the Board's 2007 decision (Tariff 22.A) which focused exclusively on online music services. In this latest decision, the Board certifies a user-based tariff, which enables it to determine royalties payable by user rather than payable on the basis of use. In its essence, under this decision the Board is of the opinion that online use of music by broadcasters attracts the same liabilities as the traditional broadcast of music. The decision targets music uses over the internet including uses in the contexts of commercial and non-commercial radio broadcasts, satellite radio services, pay audio services; stand alone audio websites that play music, game sites, commercial television, non-broadcast television, CBC, TVO, and Télé Québec. Much to the dismay of the Society of Composers, Authors and Music Publishers of Canada, majority of the Board were of the opinion that it could not approve the setting of tariff for all other internet uses of music that the organization requested. Specifically, the Board argued that it did not have enough information in respect of music used by diverse websites including business establishments that use music mainly to publicize a brand or a store, social networking website initiatives on the cyberspace such as Facebook and MySapce, amateur podcasts, as well as video sharing websites like YouTube.

Privacy Law: Warrantless Search & Seizure

The Newfoundland and Labrador Provincial Court has delivered its decision in *Suprrell v. Canada* affirming that the Defendants have standing to challenge the validity of the search and seizure practices used by the Department of Fisheries and Oceans (DFO). In that case, DFO became suspicious of certain activities which were in turn fuelled by allegations in regard to Crab fishing in Black Tickle, Labrador. It obtained two search warrants in June 2004 which they executed simultaneously. The warrants only authorized "search for seizure of evidence in support of suspected offences committed between June 1 2001 and November 7, 2003" (para 20). Specifically the "search was to locate and seize all documents and records that related to crab purchased, or otherwise acquired, produced, held in storage, shipped or otherwise dealt with by Quinlan Brothers Limited, Bay de Verde" (para 23) and further records that related to named vessels within the time period. In a comprehensive search plan document, it was clear that search team members may come across some information not being sought but which may be of interest to other investigation. In any such event, they may have to obtain a separate search warrant under that search plan. According to the court, "it was clear that the DFO was aware of the obligation on Government to respect privacy, and obtain prior judicial authorization prior to invading personal privacy" (para 22). Nonetheless, a DFO fisheries officer, without ever referring to the scope of the warrant, operated without any restriction. He seized whole computer hard drives as well as floppy discs and cd-rom storage discs, copied the entire hard drives which were reviewed by DFO in its own premises. He accessed and examined all of the materials seized, including records about landings of crab from the previous five years. Specifically, those included records relating to 1999 crab fishing season and turned over everything found on the computers, making no distinction between search and seizure. He then claimed to have accessed the information not covered by the warrant inadvertently. Meanwhile, DFO used the information obtained to support further applications for additional search warrants without disclosing how the supporting information was obtained.

In its argument, the DFO was of the opinion that since the information in issue related to business record; it is not personal in nature and did not require high expectation of privacy. In rejecting the contention, the court relied on several authorities (*Southam, Plant, Law*, etc.) and concluded that on the authorities there is no discrimination in regard to records having less privacy interest simply because they related to business dealing. Quoting the Supreme Court (Binnie J) in *R v. Tesling*, the court ruled that "protection of informational privacy is predicated on the assumption that all information about a person is in a fundamental way his own" and that could include "commercial information locked up in a safe in a restaurant" (para 49).

International Cases of Interest

Is a "Hash Value" Analysis a Search?

In *U.S.A. v. Crist*, Chief Judge Yvette Kane of the U.S. District Court (Pennsylvania) considered whether a detailed forensic analytical procedure for computer hard drives, called a "hash" or "hash value analysis", was a search for the purposes of attracting Fourth Amendment Protection. A witness, Hipple, was given the accused's computer while the accused was being evicted. Upon searching it, he found two videos appearing to be child pornography. He deleted the videos and gave the computer to the police. A police forensics special agent, Buckwash, conducted a "hash value analysis" on the computer, which involved creating a "MD5 hash value" for the hard drive, "a unique alphanumeric representation of the data, a sort of 'fingerprint' or 'digital DNA.'" He then made an image of the hard drive and analyzed the image using EnCase software, which reads and indexes every file on the computer directly, bypassing the computer's operating system. He then generated "hash values" for each file on the computer, and comparing these to hash values of known child pornography images he was able to conclude that five of the files were known child pornography videos. He eventually found over 1600 child pornography images on the computer.

The prosecution argued, *inter alia*, that the "hash value analysis" was not a search, because in so doing the agents did not view any files but simply accessed the computer data using the software. Chief Judge Kane rejected this view:

> the "running of hash values" is a search protected by the Fourth Amendment. Computers are composed of many compartments, among them a "hard drive," which in turn is composed of many "platters," or disks. To derive the hash values of Crist's computer, the Government physically removed the hard drive from the computer, created a duplicate image of the hard drive without physically invading it, and applied the EnCase program to each compartment, disk, file, folder, and bit. ... By subjecting the entire computer to a hash value analysis–every file, internet history, picture, and "buddy list" became available for Government review. Such examination constitutes a search (p. 17).

The Court further held that Crist's privacy rights in the information had not been extinguished simply because of the search by Hipple. Chief Judge Kane specifically rejected "the Government's initial approach asking the Court to compare Crist's entire computer to a single closed container which was breached by the Hipple search. A hard drive is not analogous to an individual disk. Rather, a hard drive is comprised of many platters, or magnetic data storage units, mounted together. Each platter, as opposed to the hard drive in its entirety, is analogous to a single disk […]" (p. 18). She ordered that all evidence gained from the forensic analysis of the computer should be suppressed.

2ième partie

Production en preuve de courriers électroniques

Dans cette affaire, l'une des questions en litige est de déterminer la nature de la relation d'affaires entre le demandeur ICTS et Koop. Koop soutient qu'il est associé tandis ICTS prétend qu'il est employé. Pour soutenir ses prétentions, Koop produit plusieurs courriers électroniques, documents de travail, projets et propositions écrites. ICTS s'oppose à la production des courriers électroniques soutenant que cela est contraire à l'article 2860 C.c.Q.

Les courriers électroniques ne sont pas des originaux au sens de cet article puisqu'ils n'ont pas été certifiés selon les articles 12 et 16 de la *Loi concernant le cadre juridique des technologies de l'information*. Toutefois, selon le tribunal, *« il appert que ces courriers électroniques du 19 janvier 2001 et du 3 avril 2001 ne visent pas à faire la preuve d'un acte juridique. Ils établissent la preuve des circonstances entourant leur relation d'affaires lesquelles sont prouvables par tous moyens selon l'article 2857 C.c.Q. »*. Le tribunal rejette l'objection.

- *Intercontinental Corporate Technology Services Ltd. c. Bombardier inc.*, 2008 QCCS 5086 (CanLII), 30 octobre 2008.

Appréciation de la littérature médicale extraite d'internet comme preuve médicale

L'employeur demande à la Commission des lésions professionnelles de réviser une décision qui détermine qu'un travailleur a subi une maladie professionnelle. L'un des arguments de l'employeur est que la première commissaire aurait commis une erreur dans l'appréciation de la preuve médicale. L'avocate de l'employeur soutient que la preuve soumise par le travailleur, soit de la littérature médicale extraite d'internet, n'est pas probante en l'instance. Elle n'a pas eu l'occasion de contre-interroger les auteurs de cette littérature, diminuant ainsi la force probante de ces documents. Seule la preuve par le médecin de l'employeur aurait dû être retenue.

La Commission rejette ce moyen de l'employeur. Le rôle du commissaire est d'apprécier la preuve. Cette appréciation est une opération complexe demandant l'analyse de tous les éléments, autant ceux qui sont au dossier que ceux qui lui sont soumis au cours de l'audience. Il en va de même de la preuve médicale. En l'instance, conclut la Commission, la première commissaire a analysé la preuve médicale qui lui était soumise et on ne peut lui reprocher de tenir compte de la littérature médicale provenant d'internet. La Commission ajoute : *« Il est vrai que l'on trouve toutes sortes d'informations sur internet. Même les décisions de la Cour suprême y sont accessibles. Spécifiquement, le document dont il est question est préparé par un médecin, orthopédiste, pour le Tribunal d'appel de la sécurité professionnelle et de l'assurance contre les accidents d'Ontario »*.

- *Grondines et Centre hospitalier Robert Giffard*, 2008 QCCLP 6208 (CanLII), 29 octobre 2008.

Cybersurveillance et utilisation d'internet au travail à des fins personnelles

Dans cette étude, l'auteur passe en revue les principes qui balisent le droit pour les employés de naviguer sur internet dans le cadre du travail. Tout en constatant qu'il existe une vie privée au travail, l'auteur relève que les exigences de la relation de confiance qui caractérise le lien d'emploi de même que d'autres impératifs légitimes de l'entreprise peuvent justifier des intrusions ou des sanctions de l'employeur. L'auteur explique les exigences quant à la preuve de l'utilisation inappropriée de l'ordinateur de l'employeur. Dans une autre partie de l'étude, on trouvera une revue des manquements identifiés comme pouvant donner ouverture à des sanctions disciplinaires. Mais on relève les facteurs aggravants et atténuants qui sont considérés par les instances judiciaires et arbitrales.

- Sylvain LEFEBVRE, « Naviguer sur Internet au travail : Et si on nageait en eaux troubles ? », dans Développements récents en droit du travail (2008), Service de formation permanente du Barreau du Québec, 2008, disponible à http://rejb.editionsyvonblais.com.

Proposition de directive européenne pour moderniser le droit de la protection des consommateurs, notamment pour les transactions en ligne

La Commission européenne a adopté, le 8 octobre 2008, une proposition de directive qui simplifie quatre directives existantes et porte sur tous les aspects des achats: informations sur le produit, clauses contractuelles, livraisons, retours de marchandises, remboursements, réparations, garanties et annulations. L'objectif est de mettre en place un véritable marché intérieur pour les consommateurs en offrant un juste équilibre entre la protection de ces derniers et la compétitivité des entreprises. Plus qu'une refonte de l'existant, la future directive est le fruit d'un travail de réduction de la fragmentation réglementaire, d'un travail de renforcement de la protection du consommateur et d'un travail visant à améliorer l'information de ce dernier pour lui donner confiance dans le marché intérieur.

Les nouvelles règles proposées fixent un délai de 30 jours pour la livraison des marchandises; accordent aux consommateurs un délai de réflexion de 14 jours (avec remboursement dans les 30 jours) ; établissent une liste noire des clauses contractuelles abusives ; définissent des règles communes applicables aux enchères en ligne et renforcent la protection contre la vente forcée et harmonisent les voies de recours en cas de produits défectueux. Ces règles doivent être approuvées par les 27 pays membres de l'UE et par le Parlement européen.

- Commission des communautés européennes, *Proposition de directive du Parlement européen et du conseil relative aux droits des consommateurs*, 8 octobre 2008.
- Commission européenne, *La Commission veut renforcer les droits des consommateurs dans toute l'Union européenne*, 8 octobre 2008.
- Raphaëlle HECQUET, *L'Union Européenne dans la course à la protection du « cyberacheteur »*, 9 octobre 2008.

Propositions pour le développement de l'économie numérique – France

Le secrétaire d'État chargé de la Prospective, de l'Évaluation des politiques publiques et du Développement de l'économie numérique, a déposé un rapport proposant 154 actions pour le développement de l'économie numérique dans le plan « France Numérique 2012 ». Ce plan, présenté le 20 octobre, fait suite aux Assises du numérique qui se sont déroulées en France entre juin et juillet 2008. Il est construit autour de quatre grands axes qui sont de « permettre à tous les Français d'accéder aux réseaux numériques», de « développer la production et l'offre de contenus numériques», de « diversifier les usages et les services numériques» et de « rénover la gouvernance et l'écosystème de l'économie numérique».

Plus particulièrement, le plan prévoit, dans un objectif «d'efficacité de notre gouvernance de l'économie numérique», la création au 1er janvier 2009 d'un Conseil national du numérique regroupant les attributions de certains comités et entités de concertation et d'autorégulation dont le Forum des droits sur l'internet (action n° 145 du plan). Le Conseil national du numérique « reprendrait les trois fonctions essentielles de ces différentes instances » qui sont : *« Une fonction d'orientation stratégique de l'économie numérique organisant une concertation de haut niveau (responsables des principales entreprises du secteur et des PME innovantes) ». « Une fonction de concertation avec l'ensemble des acteurs du numérique conduisant, notamment, à l'élaboration de chartes d'engagements et de bonne conduite. Cette fonction serait assurée par une assemblée large et représentative des différentes composantes de l'économie numérique, avec le travail de commissions thématiques (protection de l'enfance, protection des données personnelles, contrefaçon, etc.) »*. Et enfin, *« une fonction de vérification du respect des engagements. Cette fonction serait assurée par un comité plus restreint, présidé par exemple par un magistrat »*.

Le Conseil national du numérique se verra également confier *« une mission d'information et de pédagogie vis-à-vis du grand public sur le cadre*

juridique et les risques de l'univers numérique ». Il est également prévu qu'il abrite le « médiateur du numérique ».

- Éric BESSON, *Plan de développement de l'économie numérique,* octobre 2008, disponible à *Préparer la France numérique*.
- Forum des droits sur l'internet, « Le plan de développement de l'économie numérique présenté par Éric BESSON », 23 octobre 2008.

Proposition de loi visant à promouvoir le télétravail – France

S'appuyant sur la Recommandation *Le télétravail en France* de décembre 2004 publiée par le Forum des droits sur l'internet ainsi que sur le rapport *Du télétravail au travail mobile : un enjeu de modernisation de l'économie française* présenté le 10 novembre 2006 au Premier ministre par le député Pierre MOREL-A-L'HUISSIER, 59 députés ont déposé à l'Assemblée nationale le 15 octobre 2008 une proposition de loi visant à promouvoir le télétravail en France.

La proposition de loi prévoit notamment : la création d'une présomption simple de télétravailleur; la consultation des délégués du personnel ou du comité d'entreprise lors du recours au télétravail; l'insertion du télétravail au sein des obligations générales de l'employeur en matière de protection de santé et de sécurité de ses salariés; le bénéfice d'une réduction d'impôt sous certaines conditions et la présentation d'un projet de loi par le Gouvernement visant à promouvoir et à développer le télétravail au sein des administrations publiques, dans un délai d'un an à compter de la date de la promulgation de la présente loi.

Diverses actions, s'appuyant sur le rapport précité, ont également été proposées dans le Plan « France Numérique 2012 » présenté par Éric BESSON, secrétaire d'État chargé de la Prospective, de l'Évaluation des politiques publiques et du Développement de l'économie numérique, et notamment, le développement du télétravail dans le secteur public (action n° 114) et le lancement d'une action nationale associant les principaux acteurs concernés.

- *Proposition de loi visant à promouvoir le télétravail en France*, Assemblée nationale, première lecture, 15 octobre 2008.
- *Rapport parlementaire – Du télétravail au travail mobile : un enjeu de modernisation de l'économie française*, 2006.
- Forum des droit sur l'internet, Recommandation « Le télétravail en France », Recommandation adoptée le 14 décembre 2004.

Conditions nécessaires à la mise en place du filtrage des sites pédopornographiques par les fournisseurs d'accès à l'internet – France

Le Forum des droits sur l'internet publie sa Recommandation « Les enfants du Net III ». Les actions menées par les services de police se heurtent souvent à l'impossibilité de faire fermer certains sites pédopornographiques hébergés à l'étranger. C'est pourquoi le filtrage au niveau de l'accès de ces sites fait l'objet d'un intérêt particulier de la part des instances impliquées dans la lutte contre la cybercriminalité. Dans le contexte d'une probable décision des pouvoirs publics en faveur d'une telle mesure, ceux-ci ont demandé au groupe de travail multiacteur du Forum des droits sur l'internet (pouvoirs publics, acteurs économiques et société civile), de réfléchir à l'élaboration d'un cadre juridique et technique acceptable par l'ensemble des acteurs.

La question du filtrage au niveau de l'accès est délicate car les solutions recherchées doivent résoudre une difficile équation: empêcher les accès involontaires et complexifier les accès volontaires aux contenus pédopornographiques, tout en garantissant le respect de la liberté d'expression et de communication. Le Forum propose un dispositif constitué de quatre étapes assorti de garanties du respect des libertés fondamentales. Ces étapes comprennent : 1. Identification des sites pédopornographiques par les forces de police et de gendarmerie, les internautes (plates-formes de signalement) et la coopération internationale. 2. Constitution, par les services spécialisés de

l'OCLTIC, d'une liste quotidienne de sites à filtrer et transmission de celle-ci de manière sécurisée et cryptée à une autorité nationale compétente. 3. Validation de la liste par l'autorité nationale compétente, intermédiaire entre les forces de l'ordre et les fournisseurs d'accès à l'internet, puis transmission de la liste de façon sécurisée et cryptée aux opérateurs de communication électronique. Cette autorité est la seule habilitée à demander aux opérateurs de procéder au filtrage. 4. Contrôle a posteriori par l'autorité nationale compétente de la procédure et du blocage des sites.

La forme juridique précise de l'autorité nationale compétente devra être arbitrée par les pouvoirs publics. En tout état de cause, l'autorité devra être constituée selon quatre axes qui sont la réactivité; la protection des libertés fondamentales : indépendance, impartialité, principe du contradictoire, confidentialité; le respect de la transparence; et le recours en cas de filtrage abusif ou de décision infondée : gracieux, devant l'autorité nationale compétente, ou contentieux, devant le juge.

- *Le Forum des droits sur l'internet publie sa Recommandation « Les enfants du Net III »*.

Obligation d'indiquer avec précision les faits litigieux pour pouvoir engager la responsabilité de l'hébergeur – France

Des propos diffamatoires ont été tenus à l'égard d'une personne sur un blogue. La personne visée par ces propos a mis en demeure l'hébergeur de retirer ce contenu du blogue. Appliquant la règle voulant qu'un hébergeur est responsable des contenus illicites dès lors qu'il en a connaissance, le Tribunal de grande instance de Paris a appliqué la disposition de la loi française du 21 juin 2004 sur la confiance dans l'économie numérique qui définit à partir de quel moment on peut considérer que l'hébergeur peut être considéré comme ayant connaissance d'un contenu illicite. Le Tribunal a considéré qu'il faut que la mise en demeure adressée à l'hébergeur et destinée à faire retirer un contenu soit rédigée dans les termes permettant à celui-ci d'avoir connaissance du contenu.

- *M. B. K., Mme A. G. épouse K. c/ M. C. B., M. P. B. et S.A.S. 20 Minutes France*, Tribunal de grande instance de Paris, 17e chambre, 13 octobre 2008.
- Murielle CAHEN, « Nécessité d'un formalisme très strict pour mettre en demeure un hébergeur », *Droit & technologie*, 6 novembre 2008.
- « Le TGI de Paris impose un formalisme strict pour la notification de contenus illicites », *Legalis.net*, 22 octobre 2008.

Limitation de la compétence des tribunaux français pour les contrefaçons en ligne – France

La Cour de cassation a cassé un arrêt de la cour d'appel de Paris qui avait conclu que la loi pénale française était applicable aussitôt que l'atteinte portée aux droits de l'auteur, bien que d'origine italienne, a eu lieu en France. Dans son arrêt rendu le 9 septembre 2008, la Cour de cassation statue que : *« attendu qu'en se déterminant ainsi sans répondre aux conclusions du prévenu qui, pour contester la compétence des juridictions françaises, faisait valoir que le journal, dans lequel l'article avait été publié en Italie, n'était pas diffusé en France dans sa version papier et que le site internet, accessible à partir de l'adresse www.ilfoglio.it, était exclusivement rédigé en langue italienne et n'était pas destiné au public du territoire français, aucune commande du quotidien ne pouvant être effectuée à partir du territoire français, la cour d'appel, à qui il appartenait de vérifier si les faits avaient été commis en France dès lors que la perpétration de la contrefaçon sur le territoire français est un élément constitutif de cette infraction, n'a pas justifié sa décision. »*

- *Giuliano F. c. Ministère public*, Cour de cassation, Chambre criminelle, Arrêt du 9 septembre 2008, disponible à *Legalis.net*.
- « La Cour de cassation rappelle les limites de l'application de la loi pénale française à un site étranger », *Légalis.net*, 27 octobre 2008.
- Étienne WERY, « La cour de cassation met un terme à la compétence systématique des juges français pour les contrefaçons en ligne », *Droit & Technologie*, 3 novembre 2008.

Enjeux juridiques de la baladodiffusion (podcasting)

La qualification juridique à appliquer à la baladodiffusion, au podcasting et au podcast joue un rôle essentiel dans l'analyse des enjeux de ce mode de communication, de la conception jusqu'à la diffusion du podcast, tant du point de vue des ayants droit que du point de vue du public. Or, il en ressort que, si dans l'ensemble le droit existant trouve remarquablement à s'appliquer dans le cadre du podcasting, certaines adaptations sont nécessaires, la plus conséquente concernant la copie privée, dont le champ d'application devrait en l'espèce être plus large.

- Anne-Sophie JOUANNON, « Les enjeux juridiques du podcast », *Juriscom.net*, 1er novembre 2008.