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

March 7, 2012/7 mars 2012

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors Robert Currie and Stephen Coughlan of the Law and Technology Institute of Dalhousie Law School, and David Fraser. 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 et Stephen Coughlan de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie, et David Fraser. 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

Craigslist Posting not Entrapment

The British Columbia Court of Appeal considered the interplay between procuring, Craigslist postings, and entrapment with their decision in *R. v. Chiang*. The accused was charged with charged with communicating for the purpose of obtaining for consideration the sexual services of a person under the age of 18 years. The police had received information from various sources suggesting that underage females were offering sexual services through the erotic services section of the website Craigslist. They concluded that they were unlikely to obtain the cooperation of any of those young women in an investigation, and so instead they composed their own Craigslist posting which purported to offer the services of young providers, and which had a return email address of freshtna16@gmail.com. The posting itself did not explicitly state that the females were underage, but anyone replying to the ad was sent information suggesting that that was so. Most of the respondents to the advertisement did not reply further, but the accused was one of two who did, and he was sent a message saying that he could choose between a 16 year old and a 17 year old, and that he should meet the undercover officer who was posing as the procurer in the parking lot of a specified motel.

The accused met the undercover officer and had a conversation with her in which he expressed surprised upon learning that the service provider he was to meet was only 16: he indicated that he had thought that was "just a number" in the email. He was assured by the undercover officer that 16 was in fact the service provider's age and the following exchange occurred:

B. Yeah, but is that alright?

M. Well no – I mean it's not the legal age of 19, but whatever.

The accused then said he would "check it out" and took the key: when he entered the motel unit, he was arrested.

One issue at trial was whether the accused had actually committed the *actus reus* of the offence: the trial judge had had a reasonable doubt about whether the email communications demonstrated that the accused was seeking the services of someone underage. If the accused was guilty, therefore, it was because of the conversation which occurred in the parking lot, and the accused argued that his statement that he would "check it out" should not be taken to constitute obtaining the services. On the same basis he argued that the mens rea of having the "purpose" of obtaining those services had not been established. The Court of Appeal, however, rejected this claim: the trial judge in looking at the evidence had reached a different conclusion about what "check it out" had meant in context and this conclusion was soundly based in the evidence.

The accused also argued that the police behaviour, in placing a posting on Craigslist, amounted to entrapment. One kind of police behaviour which is forbidden under the doctrine of entrapment is what is referred to as "random virtue testing". That is, in the absence of a *bona fide* inquiry, the police are not entitled simply to present a person with an opportunity to commit a crime. The accused argued that this was what had occurred.

The Court of Appeal held that the "shadowy new Internet universe" required that police be accorded some latitude in their investigative techniques, in recognition of the fact that "[m]odern Internet facilities afford easier access to young people for individuals minded to exploit their youth and vulnerability" (para 19). The Court of Appeal noted that in *R. v. Barnes* the police had been permitted to conduct random virtue testing with regard to trafficking in narcotics in downtown Vancouver, on the basis that they were engaged in a bona fide inquiry of that area. They held here that:

> [20]...The erotic services section of Craigslist is analogous to the geographic area referred to in *R. v. Barnes*. Random virtue-testing is permissible as part of a bona fide inquiry directed at a circumscribed area where it is reasonably suspected that criminal activity is occurring. In such a case, the police are entitled to present any person associated with the site, whether placing an ad or responding to one, with the opportunity to commit the s. 212(4) offence. ...

Accordingly placing the posting was not entrapment and the accused's conviction was upheld.

Forensic Computer Evidence of Child Pornography

The decision in *R. v. Allart* is a useful demonstration of the proper use of, and limits to, forensic evidence based on computer usage in determining possession of child pornography. The accused had been convicted of that offence at trial, and the Court of Appeal upheld the conviction.

Fragments of various video files which constituted child pornography were found on a computer to which the accused had access. The accused's common law partner at the time also had access to the computer, however (as did the partner's nine-year-old child, though she was essentially discounted from the analysis. The forensic evidence also established to the trial judge's satisfaction that the child pornography had not been downloaded unintentionally.

A large number of files with names strongly suggestive of child pornography had been downloaded, and the evidence showed that this had occurred over a period in excess of two years. The forensic examination also disclosed numerous internet searches using phrases associated with child pornography, and visits to several websites with names indicative of child pornography. Further, the files were divided among specific named folders, bore names that were unmistakably indicative of child pornography and some had been accessed manually after having been saved.

In addition the expert testified that the computer's clock was accurate and functional, and that the had been downloaded to the machine over the internet over a period of years, rather than being copied to the computer from another machine. Finally the expert also testified that there was no indication that the computer had been operated remotely: the material had been stored and accessed by a person sitting at the computer.

That evidence, however, did not establish that it was the accused, as opposed to his common law partner, who had downloaded the material onto the computer, which was not password-protected. The forensic examination had also attempted to determine whether the internet searches had occurred just before or just after "proxemics" or "proximals": that is, uses of the computer that could be identified with a particular person, such as logging into a particular email account. However, no such evidence was found.

The trial judge was satisfied that it was the accused who had downloaded the child pornography, however, based on other evidence in the case. The charge had arisen when the accused's partner had been, with the assistance of another person, attempting to install anti-virus software: in the ensuing crash and copying of the hard drive, they discovered one of the relevant files. The accused subsequently reformatted the hard drive, but the accused's partner contacted the RCMP to inquire how the material might have ended up on the hard drive. The trial judge did not have a reasonable doubt based on the accused's argument that his partner had placed the child pornography on the computer in an attempt to frame him, because he had threatened to report her to Children's Aid. It was also uncontested that the partner had limited computer skills. The Court of Appeal found no error in the trial judge's

conclusion that he did not have reasonable doubt and upheld the conviction.

Internet Defamation: An Application of *Crookes v. Newton*

In *Tjelta v. Wang*, the plaintiff (Tjelta) sued the defendant (Wang) in defamation before the B.C. Supreme Court, arising from e-mails and letters which, among other things, adopted critical remarks made about the plaintiff on a third party website. Tjelta and Wang had been involved in a number of business ventures over several years, with Wang providing various forms of support to Tjelta in investigating and attracting funds for investment opportunities. The relationship soured and Wang withdrew from her business relationship with Tjelta. She sent various e-mails and letters to business associates and family members of Tjelta, calling him a "bloodsucker", complaining she had been taken advantage of by him and warning others from doing business with him. In some of these she directed readers to a website (referred to as the "Our Foundation" site or the "Black Page" in the decision) which appears to have been a page listing dishonest or unethical businesspeople, and which had a profile of Tjelta. Some of her letters included printouts of Tjelta's profile on the "Black Page."

In all of the communications Wang clearly adopted the negative comments being made about Tjelta, though evidence at trial indicated that she had never investigated the comments other than reading the website. Wang claimed to have been directed to the page by a former associate of Tjelta's but no supporting evidence of this was called. She nonetheless led the "Black Page" as evidence supporting her statements that Tjelta was dishonest and unethical.

In finding that Wang had defamed Tjelta without justification, Crawford J. invoked the Supreme Court of Canada's decision in *Crookes v. Newton* which held that publishing a hyperlink to defamatory material, without more, did not constitute publication of the defamatory remarks. Justice Crawford (at para. 121) quoted from the trial level decision (which the SCC had upheld), in which Kelleher J. of the B.C. Supreme Court had stated:

> It is not my decision that hyperlinking can never make a person liable for the contents of the remote site. For example, if Mr. Newton had written "the truth about Wayne Crookes is found *here*" and "here" is hyperlinked to the specific defamatory words, this might lead to a different conclusion.

In the instant case, Wang had not only provided a link to the defamed website and printouts of its content, she had expressly described it as providing "the truth" about Tjelta's business dealings. Her statements were found to be "patently defamatory" and not justified, and damages of $20,000 were ordered against Wang.

US Appeals Court Finds Warrantless Search of Cell Phone Constitutional

In *U.S. v. Flores-Lopez*, the U.S. Court of Appeals (7th Circuit) dealt with the issue of whether a warrantless search of a cell phone seized from an accused upon his arrest was permitted under the Fourth Amendment. The accused was a supplier of methamphetamine to another accused, and both were arrested when caught in a police sting. At the scene of the arrest an officer searched the accused and found a cell phone on his person. The officer searched the phone and obtained its number, and the police used the number to get a warrant for three months' worth of call history on the phone, which implicated the accused. The accused argued that the search of the phone was unreasonable because it was done without a warrant, and thus the call history was "fruit of the poisoned tree" and should be excluded. The prosecution argued that searching a "container" found on the accused incident to arrest was permitted under the case law (the *Robinson* rule), and as the phone was analogous to a container the evidence should be admitted.

In a cogently-written judgment, Posner J. for the court emphasized that a cell phone is a computer, and thus analogizing it to a typical "container" such as a diary was a stretch:

> A modern cell phone is in one aspect a diary writ large. Even when used primarily for business it is quite likely to contain, or provide ready access to, a vast body of personal data.

> The potential invasion of privacy in a search of a cell phone is greater than in a search of a "container" in a conventional sense even when the conventional container is a purse that contains an address book (itself a container) and photos. Judges are becoming aware that a computer (and remember that a modern cell phone is a computer) is not just another purse or address book.

Justice Posner expressed surprise that the evidence did not indicate the make or model of the phone in question and whether it was "smart or dumb," but observed that "even the dumbest of modern cell phones give the user access to large stores of information." Moreover, there was no particular urgency regarding the phone, nor did the cases regarding search of a vehicle apply in the circumstances. Nonetheless, Justice Posner was content to apply *Robinson*, again employing the diary analogy:

> So opening the diary found on the suspect whom the police have arrested, to verify his name and address and discover whether the diary contains information relevant to the crime for which he has been arrested, clearly is permissible; and what happened in this case was similar but even less intrusive, since a cell phone's phone number can be found without searching the phone's contents, unless the phone is password protected—and on some cell phones even if it is.

Posner J. then queried the alternative scenario, where justification would be required to search a cell phone for its number, and noted the danger that a cell phone could be "wiped"—either by the accused ("local wiping") by pressing a button which could wipe the phone's memory and warn co-conspirators that something was amiss; or by co-conspirators themselves ("remote wiping"), a "capability… available on all major cell phone platforms" or obtainable via third-party software. Accordingly, it was imperative that police be able to search the device incident to arrest in order to prevent evidence from being destroyed. While obtaining the phone's number was of minimal immediate use to the police, and perhaps the potential for destruction of data was minimal in this case, the search involved only a minimal invasion of privacy.

2ième partie

L'employeur ne peut obliger à recevoir un document au moyen d'une technologie que l'employé ne possède pas

Le grief résulte du fait qu'à compter du 11 mars 2010, l'employeur a cessé de fournir une copie papier des relevés de salaire aux employés. Des ordinateurs et des imprimantes ont été mis à la disposition des employés dans les établissements de l'employeur et des dispositions ont été prévues afin de livrer sur support papier les relevés de salaire aux employés absents du travail et ne possédant pas d'ordinateur ou d'accès Internet. Appliquant l'article 29 de la *Loi concernant le cadre juridique des technologies de l'information*, l'arbitre décide que l'employeur ne peut obliger les membres du personnel visés par la convention collective à recevoir un document sur un autre support que le papier ou au moyen d'une technologie dont il ne dispose pas. La remise du bulletin de paie exigée par les règles en vigueur doit être effectuée sur support papier à moins que les personnes concernées acceptent sur une base volontaire de le recevoir en forme de document technologique.

- *Syndicat de l'Enseignement de la région de la Mitis et Commission scolaire des Monts-et-Marées*, tribunal d'arbitrage, SOQUIJ AZ-50833548, 31 janvier 2012.

L'obligation de l'employeur de fournir un bulletin de paie à l'employé est satisfaite en lui donnant accès à un document technologique

Dans ce grief, il s'agit de décider si l'employeur a le droit de remettre aux salariés un bulletin de paie électronique, compte tenu de la convention collective et de la législation applicable. Invoquant tout un ensemble de législations fédérales et provinciales, la partie syndicale soutient que le bulletin de paie doit être transmis sur support papier. L'arbitre explique que c'est à tort que le syndicat s'est attardé aux législations des autres provinces ou territoires du Canada alors que le droit québécois règle entièrement la question soulevée par le grief. La *Loi concernant le cadre juridique des technologies de l'information* prévoit l'équivalence entre le document électronique et le document sur support papier. En l'espèce, l'employeur a mis en place un système qui répond à son obligation et respectant les exigences de l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information* en ce que les renseignements ne sont accessibles qu'aux personnes qui ont droit de les consulter. L'arbitre décide qu'à la différence de l'article 42 de la *Loi sur les normes du travail* qui subordonne à une convention collective ou un décret le paiement du salaire par virement bancaire, rien de tel est prévu pour le bulletin de paie. Or, dans le système établi par l'employeur, chaque salarié peut prendre connaissance de son bulletin de paie courant sur le site sécurisé destiné à cette fonction. L'employeur met des ordinateurs à la disposition des employés et leur procure de la formation et un soutien informatique en lien avec ces postes de travail.

- *Union des routiers, brasseries, liqueurs douces et ouvriers de diverses industries, local 1999 et L'Oréal Canada*, tribunal d'arbitrage, SOQUIJ AZ-50832524, 6 février 2012.

Le commencement de preuve doit rendre vraisemblable que c'est la personne visée qui est l'expéditeur des messages

L'avocat du défendeur s'objecte à toute preuve concernant le prêt d'argent en faisant valoir l'absence d'un commencement de preuve; l'objection a été prise sous réserve.

Le demandeur connaît le défendeur depuis 2008. Ils communiquent ensemble de temps à autre par messagerie électronique. À chaque occasion, le demandeur utilise soit l'adresse personnelle X ou, à l'occasion d'un « chat », le pseudonyme « J.J. Abrisan.exp entreprise », qui correspond d'ailleurs au nom de son entreprise. Au cours de l'année 2010, le demandeur tente d'obtenir le solde du prêt, mais en vain. C'est alors que des conversations par messagerie électronique interviennent. Dans l'une des conversations, faites en espagnol, mais

traduites par une traductrice agréée, il est écrit: « Une autre chose: le montant est de 20 000 dollars. J'ai donnée (sic) à ton père 15 000 000 millions de pesos, montant qui divisé par 1 850 est égal à 8 100 dollars. Je ne vous dois donc que 11 900 dollars. » Dans une autre, il écrit: « […] C'est vrai que je vous dois de l'argent. Je ne nie pas ça. Je n'aime pas voler personne. Je veux que ça soit clair, clair, clair. En mars 2008, j'avais 20 000 dollars canadiens pour vous. » Le tribunal doit déterminer si le demandeur bénéficie d'un commencement de preuve.

L'article 2862 du *Code civil du Québec* énonce l'interdiction d'une preuve testimoniale lorsque la valeur du litige excède 1 500 $, à moins qu'il y ait commencement de preuve. L'article 2865 du *Code civil du Québec* décrit ce qu'est un commencement de preuve: « Le commencement de preuve peut résulter d'un aveu ou d'un écrit émanant de la partie adverse, de son témoignage ou de la présentation d'un élément matériel, lorsqu'un tel moyen rend vraisemblable le fait allégué. » C'est dans ce cadre législatif que le demandeur a déposé en preuve la transcription des messages transmis par voie électronique à titre d'aveux extrajudiciaires écrits.

Aucune forme particulière n'est requise pour qu'un écrit puisse servir de commencement de preuve. Toutefois, le *Code civil du Québec* exige que le commencement de preuve émane de la partie à qui on entend l'opposer. Selon le procureur du défendeur, rien n'indique que les messages proviennent véritablement du défendeur.

Or, dans l'établissement d'un commencement de preuve, le Tribunal n'a pas à être convaincu hors de tout doute raisonnable de l'expéditeur du message. Il suffit que le commencement de preuve rende vraisemblable l'affirmation que c'est le défendeur qui est l'expéditeur des messages. La vraisemblance exige toutefois que le fait soit probable et non seulement possible. La preuve contextuelle présentée au Tribunal rend probable que le défendeur soit l'expéditeur des messages électroniques. Le demandeur communique régulièrement avec le défendeur à l'adresse de messagerie électronique auparavant mentionnée et par l'entremise du pseudonyme utilisé.

- *Claro c. Lizarazo*, 2012 QCCQ 710 (CanLII), 1er février 2012.

Rapport Gautrin sur le Web 2.0 et le gouvernement – « Gouverner autrement »

Le 31 janvier 2011, on dévoilait un avant-goût du rapport « Gouverner autrement », portant sur l'utilisation du Web 2.0 par le gouvernement du Québec. Ce rapport, issu d'une démarche interactive, doit être déposé très bientôt par M. Henri-François Gautrin à l'Assemblée nationale.

Parmi les constats de ce rapport, on signalera qu'avec le Web 2.0, les individus ne sont plus isolés face à une source d'information. Ils sont désormais constitués en réseaux et manifestent de plus en plus d'intérêt à interagir avec le gouvernement par l'intermédiaire des médias sociaux. De même, l'accroissement et la diversité des technologies numériques offrent de nouvelles possibilités pour l'administration québécoise, qui lui permettront de répondre aux attentes et aux besoins de la population.

Le rapport observe que plusieurs gouvernements ont pris le virage du Web 2.0 en l'intégrant à leur administration, comme les États-Unis, l'Australie et le Royaume-Uni. Ceux-ci ont mis en place une politique de divulgation proactive des données en plus d'en libéraliser l'accès. Ils se sont munis d'une vision de l'évolution des services publics, qui leur a permis d'innover dans la prestation de services, dans les processus de gestion et dans leurs relations avec leur personnel. Le Web 2.0 au gouvernement du Québec n'est pas uniquement un projet technologique, mais un changement de culture et de comportements organisationnels qui doit émaner de la plus haute autorité gouvernementale.

La démarche avait pour objectif d'expliquer comment le gouvernement du Québec peut tirer pleinement profit des nouvelles technologies et des nouveaux modes de communication pour améliorer la prestation de services aux citoyens et le fonctionnement interne de l'État. La démarche souligne l'importance d'aborder différemment les rapports entre le gouvernement et les citoyens et entre les ministères et organismes en adoptant une stratégie de communication Web 2.0, qui nécessite, de la part du gouvernement, la transparence de ses activités, une participation active des citoyens à ses actions, la collaboration entre les employés des ministères et organismes gouvernementaux. Il

importe en outre de susciter l'engagement des plus hautes instances gouvernementales.

Pour réaliser ce changement, le gouvernement doit entreprendre des actions stratégiques et établir un échéancier relativement à la mise en œuvre d'un tel projet. Il doit tenir compte des questions de gestion des ressources humaines, de protection des renseignements personnels et des problèmes liés à la sécurité informationnelle ainsi qu'à la fracture numérique.

- Consultation publique Web 2.0, « Le dévoilement du rapport approche à grands pas! », 31 janvier 2012.

Gouverner par Wiki-Canada

Intitulée « Gouverner par wiki : rapide, net, et intense », cette étude prospective sur les médias sociaux propose un regard exploratoire de l'incidence de ces médias sur les institutions, les comportements et les valeurs des individus. Présentant des cas fictifs, les auteurs identifient les outils et les services numériques que le gouvernement canadien pourrait mettre en place, au cours des prochaines années afin de répondre aux besoins de la population en matière d'inclusion numérique, de cybersécurité, de télétravail, etc. L'analyse n'aborde pas les enjeux majeurs relatifs à la façon dont sont structurés les processus décisionnels et qui paraissent peu susceptibles d'être transformés par le recours aux médias interactifs.

- Gouvernement du Canada, Horizons de politiques Canada, *Gouverner par Wiki : rapide, net, et intense – Étude prospective sur les médias sociaux*, Décembre 2011.

Un guide pour contrôler les conséquences imprévues du recours aux dossiers de santé électroniques (USA)

L'Agency for Healthcare Research and Quality a conçu un guide pour aider à maîtriser les conséquences imprévues découlant de la gestion informatique des dossiers de santé. Il procure aux organisations des aides afin d'éviter les problèmes pouvant survenir lors de l'implantation d'un système de dossiers électroniques ou de les anticiper et de mieux y répondre. Le guide présente une compilation des meilleures pratiques afin de gérer les enjeux et risques associés à la migration des dossiers de santé vers les environnements numériques.

- S.S. Jones, R. Koppel, M.S. Ridgely, T.E. Palen, S. Wu, and M.I. Harrison. *Guide to Reducing Unintended Consequences of Electronic Health Records*, Prepared by RAND Corporation under Contract No. HHSA290200600017I, Task Order #5. Agency for Healthcare Research and Quality (AHRQ). Rockville, MD. August, 2011.

Susciter la participation publique par les technologies de l'information – Europe

Fondé sur l'idée de départ que les technologies de l'information ont favorisé l'émergence d'une nouvelle forme de participation citoyenne aux affaires publiques et à l'élaboration des politiques, les auteures expliquent que le succès de la participation en ligne dépend de l'accessibilité des ménages à Internet et de la capacité des administrations publiques à s'adapter à ce mode de communication.

- ARCHMANN, S. et A. GUIFFART, *Engaging Citizens: How Can Public Institutions Take Advantage of ICT for More Inclusion?*, Institut européen d'administration publique, février 2012.

Les Binding Corporate Rules (BCR), outil prometteur de protection des données personnelles – Europe

Les *Binding Corporate Rules* (BCR) sont un code de conduite définissant la politique d'une entreprise en matière de transferts de données. Les BCR permettent d'offrir une protection adéquate aux données transférées depuis l'Union européenne (UE) vers des pays tiers à l'Union européenne au sein d'une même entreprise ou d'un même groupe. Les entreprises concernées par cet outil sont les multinationales exportant des données depuis leurs filiales situées au sein de l'Union européenne vers des pays tiers

n'assurant pas un niveau de protection équivalent à celui de l'Union européenne.

Ces règles constituent une alternative aux clauses contractuelles types puisqu'elles permettent d'assurer un niveau de protection suffisant aux données transférées hors UE au regard des données personnelles et des droits fondamentaux. En ce sens, elles constituent également une alternative aux principes du *Safe Harbor* pour les transferts vers les États-Unis.

Les BCR permettent à une organisation d'être en conformité avec les principes de la directive européenne 95/46/CE en matière de données à caractère personnel. Elles offrent un moyen d'uniformiser les pratiques relatives à la protection des données personnelles au sein d'un groupe. Elles contribuent à prévenir les risques inhérents aux transferts de données personnelles vers des pays tiers. Le recours aux BCR permet d'éviter de conclure autant de contrats qu'il existe de transferts au sein d'un groupe. Elles constituent donc un bon moyen de communication sur la politique d'entreprise en matière de protection des données personnelles auprès de ses clients, partenaires et salariés et de leur assurer un niveau de protection satisfaisant lors des transferts de leurs données personnelles. Le recours à cet outil facilite la mise en place d'un guide interne en matière de gestion des données personnelles.

Les auteurs Naftalski et Desgens-Pasanau soulignent la consécration par le législateur européen de cet outil qui permet d'encadrer de façon plus effective les transferts de données hors de l'Union européenne. C'est une alternative pertinente aux clauses contractuelles types et qui surtout permet d'anticiper la révision prochaine de la Directive européenne. En particulier, le recours aux BCR permettra aux entreprises de se conformer plus facilement à l'obligation de justifier des mécanismes internes afin de garantir la conformité des traitement d'informations personnelles à la réglementation sur la protection des données personnelles.

- Fabrice NAFTALSKI et Guillaume DESGENS-PASANAU, « À l'aune du nouveau règlement européen en matière de protection des données à caractère personnel, les BCR se profilent comme le meilleur moyen pour un groupe international d'assurer sa conformité 'informatique et libertés' », *Communication Commerce électronique*, mars 2012, p. 2.
- CNIL, *Les règles internes d'entreprise BCR*.

Le filtrage des contenus des réseaux sociaux contraire au droit communautaire européen

Dans son arrêt du 16 février 2012 sur le filtrage préventif par un réseau social, la Cour de Justice de l'Union européenne (CJUE) conclut qu'« en adoptant l'injonction obligeant le prestataire de services d'hébergement à mettre en place le système de filtrage litigieux, la juridiction nationale concernée ne respecterait pas l'exigence d'assurer un juste équilibre entre le droit de propriété intellectuelle, d'une part, et la liberté d'entreprise, le droit à la protection des données à caractère personnel et la liberté de recevoir ou de communiquer des informations, d'autre part ».

La société d'auteur belge Sabam avait introduit un recours contre la plateforme de réseau social Netlog qui met à la disposition des internautes un espace personnel sur lequel les usagers peuvent, sans autorisation, mettre à la disposition de tiers des œuvres musicales ou audiovisuelles inscrites dans le répertoire de la Sabam. Le recours de la Sabam au tribunal de Bruxelles visait à enjoindre Netlog de cesser cette mise à disposition illicite, ce qui, selon Netlog, reviendrait à lui imposer une obligation générale de surveillance. Le tribunal a décidé de poser une question préjudicielle à la CJUE afin qu'elle se prononce sur la compatibilité de cette demande avec quatre directives européennes.

La Cour a répondu par la négative aux questions. Elle estime que l'ordonnance demandée *« imposerait au prestataire de services d'hébergement une surveillance générale qui est interdite par l'article 15, paragraphe 1, de la directive 2000/31 ».* De plus, cette démarche *« entraînerait une atteinte caractérisée à la liberté d'entreprise du prestataire de services d'hébergement puisqu'elle l'obligerait à mettre en place un système informatique complexe, coûteux, permanent et à ses seuls frais, ce qui serait d'ailleurs contraire aux conditions prévues à l'article 3, paragraphe 1, de la directive 2004/48, qui exige que les mesures pour assurer le respect des droits de propriété intellectuelle ne soient pas*

inutilement complexes ou coûteuses ». De plus, le système de filtrage réclamé serait, contraire à la directive de 1995 relative à la protection des données personnelles dans la mesure où il *« impliquerait, d'une part, l'identification, l'analyse systématique et le traitement des informations relatives aux profils créés sur le réseau social par les utilisateurs de ce dernier, les informations relatives à ces profils étant des données protégées à caractère personnel, car elles permettent, en principe, l'identification desdits utilisateurs ».* Selon la Cour, un pareil mécanisme *« risquerait de porter atteinte à la liberté d'information, puisque ce système risquerait de ne pas suffisamment distinguer entre un contenu illicite et un contenu licite, de sorte que son déploiement pourrait avoir pour effet d'entraîner le blocage de communications à contenu licite. »*

- *Sabam c. Netlog NV*, Cour de justice de l'Union européenne, 3ème chambre, Arrêt du 16 février 2012.
- « Le filtrage de contenus par un réseau social est contraire au droit communautaire », *Legalis.net*, 16 février 2012.

Statut des sites de revente de billets de spectacles – France

L'Opéra de Paris avait demandé au tribunal de commerce de Paris d'ordonner le retrait de toutes les annonces passées, présentes et à venir de vente et d'achat de billets de spectacles sur le site de vente de billets Viagogo.fr. Le recours était fondé sur l'article 1er de la loi 27 juin 1919 qui réprime le trafic de billets de théâtre subventionnés. Dans une ordonnance de référé rendue le 15 février 2012, le tribunal de commerce a rejeté les demandes puisqu'il existe une contestation sérieuse sur le statut de Viagogo. La détermination du statut de ce site comme éditeur ou hébergeur relève du juge du fond. Le site Viagogo.fr. se présente comme un *« système d'échange de billets en ligne permettant d'acheter ou de vendre des billets de spectacles, de matchs, de concerts ou de théâtre en toute sécurité et de manière garantie ».*

- *L'Epic l'Opéra National c. Viagogo Ltd, Tribunal de commerce de Paris*, Ordonnance de référé, 15 février 2012.
- « Bourse d'échange de billets de spectacles : contestation sérieuse sur le statut d'hébergeur », *Legalis.net*, 5 mars 2012.

eBay n'est pas un intermédiaire neutre ou un hébergeur – France

La cour d'appel de Paris a confirmé dans sa décision du 23 janvier 2012 la condamnation exemplaire d'eBay International pour recel de vente de contrefaçons. eBay percevait des commissions sur des transactions portant sur des produits qu'elle savait contrefaisants. La cour a considéré que *« la société eBay international AG, par la passivité de ses services de surveillance et les rares sanctions totalement inefficaces prononcées par ses organes de contrôle (retraits ponctuels des annonces et remboursement aux annonceurs de ses frais d'annonce), a démontré sa volonté de préserver ses intérêts en ne suspendant pas ou en ne fermant pas les comptes des deux contrevenants afin de ne pas interrompre une activité qui lui profitait directement ».* Des vendeurs sur eBay détenaient plusieurs comptes sous différents pseudonymes. Ces comptes leur servaient pour écouler les marchandises contrefaites et pour faire monter les enchères. La cour en est venue à la conclusion que eBay, en sa qualité de plate-forme de mise en relation, ne pouvait ignorer le caractère frauduleux de l'activité. Le fort volume de produits de marques prestigieuses écoulés par des particuliers ne pouvait que soulever des interrogations. D'ailleurs eBay avait fait des retraits « pro-actifs » et suspendu des comptes pour surenchère, à la suite d'alertes répétées des titulaires de droits. En dépit de ces faits, eBay n'a pas fermé les comptes. La cour écarte la qualification d'hébergeur car eBay n'occupe pas une position neutre entre le client vendeur et les acheteurs potentiels. eBay tient plutôt un rôle actif en leur permettant d'optimiser les ventes. La Cour d'appel estime pour cette raison *« que l'hébergement des annonces n'est que le support de l'activité principale d'eBay, à savoir l'intermédiation entre vendeurs et acheteurs pour laquelle elle a mis en place des outils destinés à promouvoir les ventes et à les orienter pour optimiser les chances qu'elles aboutissent à des transactions effectives sur le montant desquelles elle percevra une commission ».*

Étant donné que eBay tire profit de la valeur des biens mis aux enchères et non du stockage, elle *« perd son caractère de neutralité par rapport aux données qu'elle ne se contente pas d'héberger mais qu'elle exploite »*.

- *eBay International c. Burberry Ltd et autres*, Cour d'appel de Paris, Pôle 5, chambre 12, Arrêt du 23 janvier 2012.
- « eBay condamnée à 200 000 € d'amende pour recel de contrefaçons », *Legalis.net,* 6 mars 2012.

À signaler

- Pierre DUCHAINE, « Commentaire sur le projet de loi 37, intitulé Loi modifiant le Code civil et d'autres dispositions législatives en matière de publicité foncière-Retour vers le futur? », Repères, Décembre 2011, EYB2011REP1123.
- Antoine GUILMAIN, « La règle de la meilleure preuve à l'aune de la distinction copie-transfert », *Lex electronica*, vol. 16, no. 2, hiver 2012.
- Nicolas W. VERMEYS, « Commentaire sur la décision Crookes c. Newton – Comment hyperelier sans risque de poursuite », Repères, Novembre 2011, EYB2011REP1116.

This newsletter is intended to keep members of IT.Can informed about Canadian legal developments as well as about international developments that may have an impact on Canada. It will also be a vehicle for the Executive and Board of Directors of the Association to keep you informed of Association news such as upcoming conferences.

If you have comments or suggestions about this newsletter, please contact Professor Robert Currie, Director of the Law & Technology Institute, at robert.currie@dal.ca if they relate to Part 1 or Pierre Trudel at pierre.trudel@umontreal.ca if they relate to Part 2.

Disclaimer: The IT.Can Newsletter is intended to provide readers with notice of certain new developments and issues of legal significance. It is not intended to be a complete statement of the law, nor is it intended to provide legal advice. No person should act or rely upon the information in the IT.Can Newsletter without seeking specific legal advice.

Le présent bulletin se veut un outil d'information à l'intention des membres d'IT.Can qui souhaitent être renseignés sur les développements du droit canadien et du droit international qui pourraient avoir une incidence sur le Canada. Le comité exécutif et le conseil d'administration de l'Association s'en serviront également pour vous tenir au courant des nouvelles concernant l'Association, telles que les conférences à venir.

Pour tous commentaires ou toutes suggestions concernant la première partie du présent bulletin, veuillez contacter le professeur Robert Currie à l'adresse suivante : robert.currie@dal.ca ou en ce qui concerne la deuxième partie, veuillez contacter Pierre Trudel à pierre.trudel@umontreal.ca.

Avertissement : Le Bulletin IT.Can vise à informer les lecteurs au sujet de récents développements et de certaines questions à portée juridique. Il ne se veut pas un exposé complet de la loi et n'est pas destiné à donner des conseils juridiques. Nul ne devrait donner suite ou se fier aux renseignements figurant dans le Bulletin IT.Can sans avoir consulté au préalable un conseiller juridique.