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

June 2, 2011/2 juin 2011

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

Reproductive Technology and Equality Rights

The British Columbia Supreme Court has found that the province's *Adoption Act* violates section 15 of the Charter and is not saved under section 1 by reason of its failure to extend to people who were conceived through an anonymous sperm donor the same ability to get identifying information about biological parents as is available to people who were adopted. In *Pratten v. British Columbia (Attorney General)*, the applicant was a woman in her late twenties who had been conceived using sperm from an anonymous donor. She brought a challenge to legislation in the province of British Columbia, arguing that it violated both her section 7 and section 15 rights. The court rejected her section 7 claim, but accepted the argument that by being underinclusive the *Adoption Act* violated the applicant's equality rights. In particular, the offending distinction was illustrated by the statement of purpose of the Act, which held that:

> The purpose of this Act is to provide for new and permanent family ties *through adoption*, giving paramount consideration in every respect to the child's best interests. (emphasis added)

The argument was that the emphasised words, by extending certain guarantees only to adopted persons, create a distinction based "on the basis of manner of conception, and specifically conception by anonymous gamete donation" (para 224).

The trial judge heard considerable evidence concerning the situation of persons who were conceived through anonymous sperm donors, both in the form of expert evidence and personal reports. She concluded that there was a great deal to learn about the experience of donor offspring by looking at the situation of adopted persons. In particular she noted that that donor offspring share many of the same social, psychological and medical needs for information about biological parents that adopted children have, and that serious harm can be caused by cutting off a child from his or her biological roots. She also found that donor offspring have been recognised as a vulnerable group because of the lack of records and information about their biological fathers. These vulnerabilities include a lack of a complete family medical history, the risk of unknowingly forming a relationship with a half-sibling, and a sense of alienation. She noted as well that in one sense donor offspring were more vulnerable than adopted children: adoption is a matter of finding parents for a child who already exists, while anonymous gamete donation is a matter of creating a child for parents who want one. She noted as well that the situation of donor offspring had been left unlegislated, so that whether any type of information was available about a child's biological father was a matter entirely in the hands of the private sector such as fertility clinics, or private organizations devoted to allowing donor offspring and donors to research connections between themselves (such as the "Donor Sibling Registry", an online service with which individuals can register).

Much of the Crown's argument rested on the position that the provincial *Adoption Act* did not violate equality rights even though it did not protect donor offspring, because the needs of the latter group were met by federal legislation, the *Assisted Human Reproduction Act*. The judge noted that even at the time the case was argued there

were difficulties with this position: it depended on legislation from a different level of government and certain portions of the legislation had not been proclaimed. By the time *Pratten* was decided, however, the argument had suffered a severe blow: in *Reference Re Assisted Human Reproduction Act* the Supreme Court of Canada had decided that the relevant portions of that act were *ultra vires* the federal government.

The trial judge rejected the argument that there was a violation of the applicant's section 7 rights. She argued that section 7 created a positive right to life liberty and security of the person, and that the province therefore had an obligation—in which it had failed—to legislate to protect the applicant's right to the information she sought. The trial judge did not accept that section 7 could be used in that positive manner in this case. The "negative" argument would have depended on the claim that the applicant had suffered a deprivation of life liberty or security of the person, and that this deprivation had been caused by state action: this argument also failed. The judge accepted that the evidence about the effects of lacking information about one's biological father amounted to a deprivation of security of the person. However, the only action of the government was failing to legislate to require private fertility clinics to keep the kind of records and provide the kind of information the applicant sought: in effect, this was simply a different version of the "positive right" argument which had already been rejected. The government had not legislated to prevent the destruction of records, but it had also done nothing to require that such destruction occur. (In addition, it was noted that in the case of adoptees, there was no legislation which mandated that adopted children were entitled to information about their biological fathers: rather, they were entitled to see the relevant registration of birth, which might or might not allow the person to then obtain information about their father.)

Ultimately the judge found that the violation of section 15 was not saved under section 1 of the *Charter*. As the judge noted, virtually every aspect of the Attorney Generals section 1 argument had depended on the *Assisted Human Reproduction Act*, which had now been found invalid. Accordingly the judge found in favour of the applicant and struck down various provisions of the Adoption Act which did not, but should, refer to donor offspring. The judge declined to direct exactly how the provisions needed to be drafted, despite the invitation to do so from the applicant. Instead she suspended the declaration of invalidity for fifteen months to allow the government an opportunity to draft new legislation. She also granted a permanent injunction prohibiting the destruction, disposal, redaction or transfer out of B.C. of Gamete Donor Records in British Columbia.

Online Tracking, Profiling and Targeting, Cloud Computing

The Privacy Commissioner has issued its Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing. Although forming no definitive policy position on any issue, the Report explains the results from the various submissions received and consultations conducted on a variety of issues which are affecting consumers on the web today.

The Office of the Privacy Commissioner (OPC) spends some time discussing the reality of the experience of most people on the web today, and in particular the implications for privacy of various methods of tracking usage and marketing based on the information gathered. The Report considers not only traditional cookies (which consumers can turn off, though likely most do not) but also various more difficult to control features, such as flash cookies, super cookies, or web beacons. They also discuss behavioural advertising, which is based on a user's browsing history, and contextual advertising, defined as "advertising based on a consumer's current visit to a single web page or a single search query that involves no retention of data about the consumer's online activities beyond that necessary for the immediate delivery of an ad or search result." Although not as intrusive because it does not involve the collection or retention of an individual's online behaviour, contextual advertisements if clicked may be used later to deliver a targeted advertisement.

The report notes the special concerns around youth, who increasingly "are being given a digital presence before they can even say the word 'no.'"

The OPC also discussed social networking sites and privacy, and in particular the difficulties in retaining a professional/personal distinction when participating in them. It was noted that the reality of most such sites is "public by default, privacy by effort", an approach which carries some risks for users. In this regard, the OPC noted a number of proposed initiatives for itself, which included:

- The OPC will continue to monitor and fund research developments on the implications of changing perceptions of public and private spaces (as well as the challenges of maintaining a professional and personal presence online), through its Contributions Program.
- The OPC will conduct public opinion research on Canadians' perceptions of the public-private divide.
- The OPC will conduct outreach activities, including developing best practices for organizations to support people's capacity to be as private—or as public—as they want.

Another issue raised in the Report is the concept of a Do Not Track registry, which would be a browser-based mechanism by which users can monitor or prevent online tracking. The OPC noted that although such a mechanism would offer a practical means for individuals to protect their browsing activities, it would raise jurisdictional and technical issues.

A further issue discussed in the Report is cloud computing, by which users rely on services on other sites and computers in order to conduct their businesses. The OPC notes that particular issues around compliance with PIPEDA could arise in such circumstances, because those other sites and services might be located outside of Canada. PIPEDA might well still apply if the company or activity outside Canada's borders nonetheless had a real and substantial connection to Canada. Nonetheless the OPC noted the need for consistency in approach between jurisdictions. The proposed a number of actions, including:

- The OPC encourages organizations to make it clear to individuals that their personal information may be processed in foreign jurisdictions and may be accessible to law enforcement and national security authorities in those jurisdictions. This must be done in clear, understandable language, ideally at the time the information is collected.
- The OPC will continue to provide guidance to organizations vis-à-vis transborder data flows.
- The OPC will continue to work towards harmonized approaches to data protection and enforcement.
- The OPC will co-operate where appropriate with our international counterparts to further the protection of personal information globally.

Alberta Privacy Commissioner Requires Notification After Data Breach

In *[Re] Best Buy Canada Ltd., Case File No. P-1821*, the Information and Privacy Commissioner of Alberta considered whether a company, Best Buy Canada Ltd. ("Best Buy"), was required to provide notification to individuals potentially affected by a data breach, pursuant to ss. 34.1 and 37.1 of the Alberta *Personal Information Protection Act* (PIPA). Section 34.1 of PIPA requires a company within Alberta's jurisdiction to notify the Commissioner of any incident involving "the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure" (para. 2). In April 2011, Best Buy provided such a notification to the Commissioner, involving the U.S. company Epsilon Data Management LLC ("Epsilon"), which Best Buy had contracted to send e-mail marketing notifications to Best Buy's customers and to manage its "Reward Zone" loyalty program. In March 2011 Epsilon had notified Best Buy that Epsilon had been the target of a highly-sophisticated cyber attack that had compromised the login and password credentials for one of its e-mail application administrators. Over 50 million e-mail addresses had been downloaded to an FTP site in another country (i.e. not the U.S.) With specific regard to Best Buy, the hackers had downloaded the first name, last name and e-mail addresses of over 2 million of Best Buy's "Reward Zone" members. Best Buy had sent out a general e-mail warning to all of its customers regarding the breach.

Commissioner Work first noted that s. 5(1) of PIPA makes Best Buy responsible for its agent's compliance with the Act, even though the agent (Epsilon) is located in the U.S. In determining whether to order Best Buy to notify potentially affected individuals, he had to consider whether there was a "real risk of significant harm" resulting from the incident, which would include such factors as "the magnitude of the breach, that is the number of affected individuals, the maliciousness of the breach including whether there are indications personal information was misappropriated for nefarious purposes, the sensitivity of the information and the harm that may result" (para. 11). While the information itself was of low sensitivity, Best Buy had submitted that there was a possibility of both phishing and "spear phishing," the latter of which was:

> a targeted form of phishing where some information is already known about the target and this may improve the chance of success from a phishing attempt. In this case, affected individuals are likely to receive an email from criminals which has the appearance of originating from Best Buy which could invite the individual to open an attachment with malware or update a "profile" which would provide additional personal information to those with nefarious intentions (para. 14).

This, according to the Commissioner, opened the possibility of "significant harm," but he next turned to whether there was a "real risk," a standard which "does not require that significant harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. Further, there must be a cause and effect relationship between the incident and the possible harm" (para. 16). Though Best Buy had argued that its general notification would make harm to individual customers unlikely, the Commissioner ruled that this was not a relevant consideration as to whether there was a "real risk." A small portion of the affected customers were likely to fall prey to a phishing attempt. Moreover, two factors were important: "1) the magnitude of the Epsilon breach and the number of affected Best Buy customers and 2) the sophistication of the attack and the belief that Epsilon was targeted for nefarious purposes" (para. 21). He further noted:

> I agree with Best Buy that there is a general awareness among most internet users that they should not provide personal information or click on attachments from unknown sources, but not every internet user has this level of knowledge, nor does every internet user with this knowledge always act accordingly. To put it into perspective, even if there is only a one in a million chance that a Best Buy customer will be misled by a spear phishing email, either by providing personal information or intentionally or accidentally clicking an attachment that will install malware, with those rare odds, at least two affected individuals in Canada would actually be affected as a result of the breach (para. 22).

Ultimately, given the magnitude of the breach and the likelihood of individuals being affected, Best Buy was required to notify the affected individuals. The Commissioner noted that Best Buy had, in fact, already notified these individuals by e-mail and declined to order Best Buy to do so again. He commended Best Buy as "one of the few organizations that took immediate steps to notify affected individuals and proactively take steps to mitigate any harm that may result" from the Epsilon data breach (para. 25).

Document in Multi-party E-mail Chain Covered by Solicitor-Client Privilege

In *Scott & Associates Engineering Ltd. v. Ghost Pine Windfarm*, Justice Bryan E. Mahoney of the Alberta Court of Queen's Bench heard a motion for a declaration that privilege did not apply to certain redacted portions of documents otherwise subject to production. The motion arose from underlying litigation involving allegations that trust property in favour of the Applicant, Scott & Associates, had been conveyed as part of an asset purchase agreement. Among the redacted documents in question was one identified as "an e-mail…between a counsel for [the Defendant] Ghost Pine and a representative of Ghost Pine" (para. 7). While Ghost Pine maintained that the e-mail was subject to solicitor-client privilege, Scott & Associates argued that since the e-mail appeared to be "part of a chain of emails between the solicitors for the Defendant [in a related action]

Finavera and the solicitors for [Ghost Pine]," it was simply a business communication related to the asset purchase deal (para. 36).

Having reviewed the unredacted e-mail and Ghost Pine's affidavit evidence, Justice Mahoney was satisfied that it was a communication between Ghost Pine's counsel and a company representative, and thus was "within the continuum of communication within which legal advice was sought and provided related to the purchase of the Ghost Pine Assets" (para. 37). Accordingly, the e-mail was ruled privileged.

2ième partie

Utilisation du profil Facebook pour établir la bonne foi

Le locateur explique que sa conjointe et lui ont des problèmes maritaux et veulent se séparer. Ils veulent reprendre le logement de la locataire afin de permettre à l'époux de s'y loger durant cette période difficile. La locataire ne croit pas en la bonne foi du locateur. Elle a entendu dire que non seulement les locateurs n'étaient pas séparés, mais qu'en plus, ils sont devenus ou devraient devenir d'heureux parents. Elle dépose des reproductions de leur profil facebook. La lecture des commentaires de leurs parents et amis permet de constater qu'ils sont devenus les fiers parents d'un garçon. On peut lire des commentaires sur le congé parental de l'épouse, le baptême de l'enfant et le bonheur des parties et voir des photos les représentant ensemble en vacance au Mexique.

Le tribunal rejette la demande des locateurs. Le législateur a imposé aux locateurs le fardeau de démontrer que la demande de reprise de logement aux fins d'habitation n'est pas un prétexte pour atteindre d'autre fin, généralement en établissant la bonne foi des demandeurs. Ici, la cour n'est pas convaincue de la bonne foi du demandeur pour plusieurs motifs, entre autres parce que l'arrivée du poupon, les vacances conjointes ainsi que les nombreux commentaires des amis et familles du couple sur leurs profils sociaux ne corroborent pas une séparation. Le choix du demandeur semble temporaire en prévision d'une réconciliation possible avec son épouse. Le degré de permanence de l'occupation n'est donc pas une certitude à ce stade.

- *Limoges c. Fassette*, (Régie du logement 2011-04-20), 2011 QCRDL 14938, SOQUIJ AZ-50745670.

Usurpation de titre professionnel diffusée sur Internet – pas de preuve de diligence raisonnable

Coulombe est accusé d'une infraction à l'article 22(2) de la *Loi sur les ingénieurs*, soit d'avoir pris le titre d'ingénieur, en faisant suivre son nom de l'abréviation «i.n.g.» sur le site Internet (www.cctd.ca) de l'entreprise pour laquelle il travaille à titre de directeur général. Le défendeur ne nie pas que l'abréviation «i.n.g.» s'est retrouvée à la suite de son nom sur le site web de CCTD le 4 décembre 2009. Le tribunal s'attache à déterminer si la défense d'erreur raisonnable de faits ou de diligence raisonnable doit être reçue. Le défendeur fait valoir que la nature même de l'Internet rend difficile d'effacer les traces dans les différents engins de recherche tel que Google parce que les utilisateurs d'Internet peuvent télécharger et copier de l'information. Le résultat est que même si le site CCTD est fermé, en inscrivant CCTD dans Google, on pourrait éventuellement trouver la notation, Fabien Coulombe i.n.g. Mais le tribunal estime que le défendeur a été peu diligent pour corriger l'inscription. La preuve est insuffisante pour soutenir la défense d'erreur raisonnable de faits. Le défendeur n'a pris aucune mesure pour s'assurer de la véracité de l'information véhiculée. La preuve que le site n'était pas actif ni à jour n'est pas une raison de ne pas vérifier. Le fait que le site soit inactif ne veut pas dire pour autant que l'information qui y est versée n'est pas diffusée. Au contraire, la fausse information est répandue vers Internet hors du contrôle du défendeur vers les différents moteurs de recherche. Le Tribunal conclut que la défense d'erreur raisonnable sur les faits ne rencontre pas les exigences jurisprudentielles quant au caractère raisonnable ou sincère de la croyance.

- *Ordre des ingénieurs du Québec c. Coulombe*, 2011 QCCQ 4079 (CanLII), 5 mai 2011.

Conséquences de l'achat de billets d'avion par Internet

Le demandeur achète par Internet trois billets d'avion pour Cuba au coût de 2 537,49 $. Le billet d'avion électronique imprimé contient une clause précisant de confirmer le vol 12 heures avant le départ et le retour prévu. Le départ devait avoir lieu le 22 février à 21 heures. Le demandeur se rend à l'aéroport pour constater que le départ avait été devancé à 10 heures. Voyage à Rabais a envoyé un courriel au demandeur l'informant de cette modification d'horaire. Le courriel ne lui a pas été retourné comme n'ayant pas été reçu. Elle présume que celui-ci a été reçu. Le demandeur admet qu'il n'a pas confirmé son vol dans les 12 ou 24 heures, comme le prévoit son contrat afin de vérifier

l'horaire du vol, mais que même s'il l'avait fait, il n'aurait pu se rendre à l'aéroport.

Le tribunal conclut que les clauses imprimées sont acceptables. Il constate que le système de réservations par Internet n'est pas sans lacunes, dont celui de pouvoir communiquer et d'échanger avec un agent de voyage. C'est le mode choisi par le demandeur et il doit assumer son choix. Il est donc victime de sa propre négligence et le tribunal rejette la requête du demandeur.

- *Wrzesinki c. Voyage à rabais*, 2011 QCCQ 5120 (CanLII), 12 avril 2011.

Une mesure ordonnant le blocage et le filtrage des communications Internet pour protéger les droits d'auteur limite les droits fondamentaux et doit découler de la Loi – Conclusions de l'Avocat général, Cour de justice de l'Union européenne

La législation belge habilite les tribunaux à émettre des ordonnances d'injonction afin de contraindre à la cessation de toute atteinte à un droit de propriété intellectuelle. En particulier, il est prévu que lorsqu'un tiers utilise les services d'un intermédiaire pour réaliser une atteinte de ce type, les juridictions sont autorisées à adopter une injonction de cessation à l'encontre de cet intermédiaire. La Société belge des auteurs compositeurs et éditeurs (Sabam) a demandé l'adoption d'une mesure provisoire à l'encontre de Scarlet Extended SA, un fournisseur d'accès à Internet (FAI). La Sabam demandait, tout d'abord, que soit constatée l'existence d'atteintes au droit d'auteur sur les oeuvres musicales appartenant à son répertoire, lesquelles résulteraient de l'échange non autorisé, par l'intermédiaire des services fournis par Scarlet, de fichiers électroniques musicaux réalisés notamment, au moyen de logiciels *peer-to-peer*. La Sabam demandait, en outre, que Scarlet soit condamnée à faire cesser ces atteintes sous peine d'astreinte, en rendant impossible ou en paralysant toute forme d'envoi ou de réception par ses clients, au moyen de logiciels peer-to-peer, de fichiers reprenant une oeuvre musicale sans l'autorisation des ayants droits. Dans un jugement du 26 novembre 2004, l'existence de ces atteintes au droit d'auteur a été constatée. Après une expertise technique, Scarlet a été condamnée, par un second jugement rendu le 29 juin 2007, à faire cesser ces atteintes au droit d'auteur en rendant impossible toute forme d'envoi ou de réception par ses clients, au moyen d'un logiciel *peer-to-peer*, notamment, de fichiers électroniques reprenant une oeuvre musicale du répertoire de la Sabam.

C'est dans ce contexte que la Cour d'appel de Bruxelles a demandé à la Cour de justice de l'Union européenne si le droit de l'Union et en particulier les droits fondamentaux garantis par la Charte des droits fondamentaux permettent à une juridiction nationale d'adopter, sous la forme d'une injonction, une mesure ordonnant à un fournisseur d'accès à Internet la mise en place d'un système de filtrage et de blocage des communications électroniques aux fins de protéger les droits de propriété intellectuelle.

Dans ses conclusions (qui ne lient pas la Cour) l'Avocat général Cruz Villalon estime que la mesure d'injonction revêt la forme d'une obligation de caractère général ayant vocation à être étendue, à terme, de manière permanente à tous les fournisseurs d'accès à Internet. En particulier, il souligne que la mesure affecterait durablement un nombre indéterminé de personnes morales ou physiques sans tenir compte de leur relation contractuelle avec Scarlet ni de leur État de résidence. En effet, le système doit pouvoir bloquer tout envoi d'un internaute abonné à Scarlet à un autre internaute—abonné ou non à Scarlet et résidant ou non en Belgique—de tout fichier censé porter atteinte à un droit dont la Sabam assure la gestion, la collecte et la défense. De même, il doit également pouvoir bloquer la réception par tout internaute abonné à Scarlet de tout fichier portant atteinte au droit d'auteur en provenance de tout autre internaute. De plus, la mesure serait appliquée *in abstracto* et à titre préventif, c'est-à-dire sans qu'il n'ait été au préalable constaté une atteinte effective ou encore un risque d'atteinte imminente à un droit de propriété intellectuelle. L'avocat général précise en outre que la mesure en cause se présente comme une obligation nouvelle car elle imposerait à Scarlet une obligation de résultat en ce qui concerne la protection des droits d'auteur défendus par la Sabam par ce système instauré et ce, sous peine d'astreinte. De plus, elle

mettrait à sa charge les coûts de mise en place du système de filtrage et de blocage. Ce faisant, à travers le système à mettre en place, la responsabilité juridique et économique de la lutte contre le téléchargement illégal d'oeuvres piratées sur Internet serait largement déléguée aux fournisseurs d'accès à Internet.

Partant de ces caractéristiques, l'Avocat général estime que la mise en place de ce système de filtrage et de blocage se présente comme une limitation du droit au respect du secret des communications et du droit à la protection des données personnelles, protégés par la Charte des droits fondamentaux. De même, le déploiement d'un tel système limiterait la liberté d'information protégée également par la Charte des droits fondamentaux. En application de la jurisprudence développée en la matière par la Cour européenne des droits de l'homme, M. Cruz Villalon estime qu'une limitation de l'exercice des droits et libertés garantis par la Charte des droits fondamentaux doit reposer sur une base légale répondant aux exigences tenant à « la qualité de la loi » en question. Dès lors, de son point de vue, une limitation des droits et libertés des internautes telle que celle en cause ne serait admissible que si elle reposait sur une base légale nationale, accessible, claire et prévisible.

Or, selon l'avocat général, il ne peut être considéré que l'obligation des fournisseurs d'accès à Internet de mettre en place, à leurs seuls frais, le système de filtrage et de blocage en cause ait été prévue de façon expresse, préalable, claire et précise dans la disposition légale belge en cause. En effet, l'obligation mise à la charge des fournisseurs d'accès à Internet est très singulière, d'une part, et « nouvelle » voire inattendue, d'autre part. Par ailleurs, l'avocat général souligne que ni le système de filtrage—qui a vocation à s'appliquer de façon systématique et universelle, permanente et perpétuelle—ni le mécanisme de blocage—qui peut entrer en action sans que ne soit prévue la possibilité pour les personnes affectées de le contester ou de s'y opposer—ne sont assortis de garanties suffisantes.

Par conséquent, l'avocat général propose à la Cour de justice de déclarer que le droit de l'Union s'oppose à l'adoption par une juridiction nationale, sur la base de la disposition légale belge, d'une mesure ordonnant à un fournisseur d'accès à Internet de mettre en place, à l'égard de toute sa clientèle, *in abstracto* et à titre préventif, aux frais exclusifs de ce dernier et sans limitation dans le temps, un système de filtrage de toutes les communications électroniques transitant par ses services en vue d'identifier sur son réseau la circulation des fichiers électroniques contenant une oeuvre musicale, cinématographique ou audio-visuelle sur laquelle un tiers prétend détenir des droits et ensuite de bloquer le transfert de ceux-ci, au niveau de la requête ou à l'occasion de l'envoi.

- *Scarlet Extended SA c. Société belge des auteurs compositeurs et éditeurs (Sabam)*, Conclusions de l'avocat général M. Pedro Cruz Villalon présentées le 14 avril 2011 (1), Affaire C-70/10.

Internet ouvert et neutralité d'Internet – Commission européenne

La Commission européenne a publié une communication à l'issue d'une consultation publique qu'elle a tenue sur « l'Internet ouvert et la neutralité d'Internet en Europe » du 30 juin au 30 septembre 2010. Cette consultation a suscité plus de 300 contributions émanant des opérateurs de réseau, des fournisseurs de contenu, des États membres, des organisations de consommateurs et de la société civile ainsi qu'un certain nombre de particuliers. La neutralité d'Internet touche à plusieurs des droits et principes consacrés dans la Charte des droits fondamentaux de l'Union européenne (UE), en particulier au respect de la vie privée et familiale, à la protection des données personnelles et à la liberté d'expression et d'information. C'est pourquoi toute proposition législative en la matière fera l'objet d'une analyse approfondie de son incidence sur les droits fondamentaux et de sa conformité à la Charte de l'UE [conformément à la « Stratégie pour la mise en œuvre effective de la Charte des droits fondamentaux par l'Union européenne », COM(2010) 573 final du 19.10.2010].

Toute réglementation supplémentaire doit éviter de dissuader l'investissement ou les modèles d'entreprise innovants, aboutir à une utilisation plus efficace des réseaux et à la création de nouveaux débouchés aux différents niveaux de la chaîne de valeur Internet, tout en garantissant aux consommateurs les avantages d'un choix de

produits d'accès à Internet répondant à leurs besoins. Si des problèmes importants et persistants sont avérés et si l'ensemble du système—comprenant les multiples opérateurs—ne permet pas aisément aux consommateurs d'accéder aux contenus—et d'en diffuser—ainsi qu'aux services et applications de leur choix à l'aide d'un seul abonnement à Internet, la Commission déterminera s'il faut prendre des mesures plus contraignantes pour que la concurrence s'exerce et que les consommateurs aient le choix qu'ils méritent. La transparence et la facilité à changer d'opérateur sont des éléments déterminants pour les consommateurs lorsqu'ils choisissent un FSI ou en changent, mais ne sont peut-être pas des instruments adaptés pour remédier aux restrictions de services ou d'applications licites. En parallèle, la Commission entend poursuivre son dialogue avec les États membres et les parties prenantes pour assurer un développement rapide du haut débit, qui permettrait de réduire la pression sur le trafic de données.

- *L'Internet ouvert et la neutralité d'Internet en Europe,* Communication de la Commission au Parlement européen, au Conseil économique et social européen et au Comité des régions, Bruxelles, 19 avril 2011, COM (2011) 222 final.

Rapport d'information sur la neutralité de l'Internet et des réseaux – France

Dans un rapport d'information déposé à l'Assemblée nationale, les députées Corinne Erhel et Laure de la Raudière proposent de consacrer la neutralité de l'Internet comme objectif politique et de donner au principe une portée juridique en fixant de manière générale sa promotion comme objectif aux autorités réglementaires. Le rapport propose dans cet esprit de définir le principe de neutralité. Les députées recommandent d'encadrer strictement les obligations de blocage de l'Internet et de s'interroger plus avant sur la justification des mesures de blocage légales, en dépit de leur légitimité apparente, du fait de leur inefficacité et des effets pervers qu'elles sont susceptibles d'engendrer. Ces procédures de blocage devraient dès à présent être encadrées par une procédure unique faisant intervenir le juge. Un autre ensemble de propositions visent à protéger l'universalité et garantir la qualité de l'Internet notamment en réservant l'appellation « Internet » aux seules offres respectant le principe de neutralité. Il est aussi suggéré de mettre en place un observatoire de la qualité de l'Internet et de garantir l'accès à un Internet de qualité suffisante. Dans la perspective d'assurer le financement pérenne de l'Internet, le rapport préconise de documenter les enjeux économiques liés au réseau Internet et d'évaluer de manière approfondie la mise en oeuvre d'une terminaison d'appel data au niveau européen.

- Corinne Erhel et Laure de La Raudière, *Rapport d'information sur la neutralité de l'Internet et des réseaux*, Assemblée nationale, 13 avril 2011.

Ordonnance de blocage de l'accès à un site de jeux – France

L'Autorité de régulation des jeux de cercle en ligne (Arjel) a mis en demeure le site de jeux et de paris en ligne, *5dimes.com*, de cesser de proposer au public français des jeux en ligne dans la mesure où celui-ci n'était pas titulaire de l'agrément délivré par l'Arjel en vertu de la *Loi du 12 mai 2010 relative à l'ouverture à la concurrence du secteur des jeux d'argent et de hasard en ligne*. Le site *5dimes* ayant maintenu son offre, l'Arjel a fait assigner l'hébergeur et huit fournisseurs d'accès français de bloquer le site de jeux en ligne.

Le Tribunal de grande instance de Paris a confirmé le fait qu'il n'était pas nécessaire de mettre en cause l'opérateur du site *5dimes.com* qui n'a pas respecté la loi. En effet, la loi n'a pas prévu que la mise en cause de l'opérateur soit une condition préalable à l'injonction sollicitée par l'Arjel. Le tribunal a aussi disjoint la procédure liée à l'hébergeur, qui n'a pas comparu et qu'on ne peut établir s'il a été bien assigné. Le Tribunal a enjoint les huit fournisseurs d'accès à Internet de bloquer le site de jeux en ligne et ils sont libres de déterminer les modalités techniques à mettre en œuvre pour se conformer à l'ordre du tribunal.

Les fournisseurs d'accès soutiennent néanmoins que le caractère illicite du site en cause ne résulte pas du seul refus d'agrément de l'Arjel mais comme 5dimes.com est édité en langue anglaise et qu'il ne visait pas spécifiquement le public français, la question

se pose de la destination véritable de celui-ci. Le Tribunal répond que *« si la seule condition visée par la loi est l'absence d'autorisation, en vertu d'un droit exclusif ou de l'agrément prévu à l'article 21, il peut néanmoins être observé que le site en cause est bien, pour partie, destiné au public français et accessible en France, de sorte que les mesures sollicitées le concernant sont justifiées »*. Le tribunal observe qu'il est possible pour un internaute français de s'inscrire à *5dimes.com*, en ayant recours à un traducteur automatique et en effectuant des versements en euros. Il se fonde aussi sur les propos d'habitués sur un forum spécialisé français pour affirmer que le site est connu sur le territoire français.

- *Autorité de régulation des jeux en ligne / Numéricable, Orange France et autres*, Tribunal de grande instance de Paris, Ordonnance de référé, 28 avril 2011.
- « Blocage de l'accès à un site de jeux : pas besoin d'assigner l'opérateur », *Legalis.net*, 5 mai 2011.

Google Suggest ne commet pas lui-même de violation du droit d'auteur – France

La cour d'appel de Paris a estimé que Google ne commettait pas d'atteinte à un droit d'auteur ou à un droit voisin lorsque sa fonctionnalité *Google Suggest* faisait apparaître les mots *Torrent*, *Megaupload* ou *Rapidshare*, à l'occasion d'une requête d'un internaute sur le nom d'un artiste ou d'un album. Le Syndicat national de l'édition phonographique (Snep) reprochait à Google d'offrir aux internautes un raccourci vers des fichiers illicites mis à disposition par trois modes de partage que sont *Torrent*, *Megaupload* et *Rapidshare* et demandait la suppression des termes litigieux.

La cour rappelle que la suggestion de ces sites ne constitue pas en elle-même une atteinte au droit d'auteur dès lors que les fichiers figurant sur ces sites ne sont pas tous nécessairement destinés à procéder à des téléchargements illégaux. En effet, l'échange de fichiers contenant des œuvres protégées notamment musicales sans autorisation ne rend pas ces sites en eux-mêmes illicites. C'est l'utilisation qui en est faite par ceux qui y déposent des fichiers et les utilisent qui peut devenir illicite. D'autre part, mentionne la cour, la suggestion automatique de ces sites ne peut générer une atteinte à un droit d'auteur ou à un droit voisin que si l'internaute se rend sur le site suggéré et télécharge un phonogramme protégé et figurant en fichier sur ces sites. Les sociétés Google ne peuvent être tenues pour responsables du contenu éventuellement illicite des fichiers échangés figurant sur les sites incriminés ni des actes des internautes recourant au moteur de recherche. En effet, le téléchargement de tels fichiers suppose un acte volontaire de l'internaute dont les sociétés Google ne peuvent être déclarées responsables. Le fait que depuis l'assignation, Google a filtré ses suggestions n'emporte pas de sa part une reconnaissance de responsabilité. Cet arrêt du 3 mai 2011 confirme une ordonnance de référé qui avait débouté le Snep de l'ensemble de ses demandes et l'avait condamné à verser au moteur de recherche 5 000 € au titre des frais de justice.

- *Snep c. Google France, Google Inc.*, Cour d'appel de Paris Pôle, chambre 3, Arrêt du 3 mai 2011.
- « P2P : les suggestions de Google ne sont pas des atteintes au droit d'auteur », *Legalis.net*, 11 mai 2011.

Réapparition d'un contenu illégal après son retrait d'un site de partage de vidéos – France

Lorsqu'un contenu réapparaît sur un site de partage après avoir été retiré suite à une notification transmise à l'hébergeur, le titulaire de droit n'a pas à effectuer une nouvelle notification si le prestataire intermédiaire est doté de moyens techniques capables de détecter la rediffusion de documents déjà signalés comme illicites. Mais le titulaire de droit a le devoir de coopérer avec l'intermédiaire afin de prévenir la réapparition de contenus non autorisés. Dans un jugement du 28 avril 2011, le tribunal de grande instance de Paris a examiné les droits et responsabilités de ceux qui sont concernés par la présence en ligne d'un document qui contrevient aux droits d'auteurs. Les titulaires ou ayants droits ont l'obligation de collaborer avec les entités intermédiaires. Dans cette affaire, les

responsables du site Youtube avaient proposé de mettre à la disposition des ayants droits un système d'identification des œuvres par empreinte. Mais en s'abstenant de donner suite, le tribunal estime que la société détentrice de droits a empêché Youtube de faire fonctionner correctement le système qu'elle a mis en place afin de rendre l'accès impossible aux contenus déjà signalés. Le tribunal écrit que *« dès lors que la société Youtube ne pouvait procéder à la réalisation et la conservation des empreintes de vidéomusiques déjà notifiées, elle ne disposait plus de moyens techniques lui permettant de détecter de nouvelles mises en ligne illicites »*. Compte tenu de cette absence de collaboration de la société ayant droit, la responsabilité de YouTube en tant qu'hébergeur ne peut pas être engagée. Pour qu'elle le soit, il aurait fallu que l'ayant droit lui procure la localisation des nouveaux fichiers litigieux.

- *Sppf c. Youtube, Google France, Google Ireland*, Tribunal de grande instance de Paris, 3ème chambre, 4ème section, 28 avril 2011.
- « La SPPF perd contre Youtube à cause de son absence de collaboration », *Legalis.net*, 10 mai 2011.

Le moteur de recherche Google condamné pour violation des droits d'auteur – Belgique

Google *moteur de recherche – Google search* a été condamné par la Cour d'appel de Bruxelles, le 5 mai 2011, pour violation des droits d'auteur des journalistes et des auteurs scientifiques représentés par les sociétés d'auteurs belges SAJ et ASSUCOPIE. La reproduction d'articles de presse ou scientifiques dans la mémoire cache des serveurs de Google est soumise au droit d'auteur comme la reproduction, même partielle, de ces articles sur le portail Google news. La Cour d'appel de Bruxelles a décidé que Google ne pouvait exercer son activité de moteur de recherche (SEARCH), en reproduisant dans la mémoire cache des serveurs de Google, des articles de journaux sans obtenir l'accord préalable des journalistes et des auteurs d'œuvres scientifiques, représentés par la SAJ et ASSUCOPIE.

Cette décision vise le cœur même de l'activité de moteur de recherche qui implique la reproduction intégrale d'œuvres dans la mémoire cache des serveurs de Google. La décision s'étend à l'activité de portail de Google news, le portail d'informations de presse en ligne de Google, sur lequel Google reproduisait d'importants passages d'articles de journaux sans l'accord des auteurs et des éditeurs de presse. Google est condamné à retirer les contenus protégés tant que la question des droits d'auteur n'aura pas été réglée sous peine d'astreintes de 25.000 euros par jour de retard.

- *Google c. Copiepresse et Société de droit d'auteur des journalistes et ASSUCOPIE*, Cour d'appel de Bruxelles, 9e ch, 5 mai 2011, disponible sur le site de la *Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique*, section Actualités.

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 Professors Robert Currie, Chidi Oguamanam and Stephen Coughlan at it.law@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 les professeurs Robert Currie, Chidi Oguamanam et Stephen Coughlan à l'adresse électronique it.law@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.