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

February 8, 2012/8 février 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

Form of Disclosure in Access to Information Requests

In *[Re] Alberta Seniors*, Adjudicator Teresa Cunningham of the Alberta Office of the Information and Privacy Commissioner heard a dispute regarding the form and scope of information provided to an individual (the "Applicant") by Alberta Seniors. Alberta Seniors is a public body of the government of Alberta which regulates, *inter alia*, care homes for adults, including developmentally disabled individuals. In November 2009, the Applicant asked Alberta Seniors for information about complaints that had been made regarding care facilities, including information about the nature, type, location and description of any complaint which had been identified as "founded." In the course of communications as to the fulfillment of the request, Alberta Seniors referred the Applicant to summaries of complaints which were posted on its website and offered to provide the Applicant spreadsheets (a sample of which it did send him) which provided some basic information about the complaints. However, the Applicant was unable to cross-link the two types of information, and none of the information included the details about the complaints he had requested. He applied for review of Alberta Seniors' response to his request.

The Adjudicator noted that section 10(1) of the Alberta *Freedom of Information and Protection of Privacy Act* required the head of a public body to assist information seekers and includes an obligation to create a record for the Applicant from records already existing in electronic form, using the public body's "normal computer hardware and software and technical expertise," if so doing would unreasonably interfere with normal operations. She rejected Alberta Seniors' argument that their form of disclosure met their obligation to assist the applicant because he was only asking for "information" about the complaints and not "records." The nature of the Applicant's request was clear, and there was no way of cross-referencing the information to link the website descriptions with the information on the spread sheet, in terms of identifying the nature of any particular complaint. Accordingly, Alberta Seniors had not discharged its obligation to search its records for the information requested.

When queried by the Adjudicator as to whether it was possible for them to generate a spreadsheet that would create the linkage necessary to provide the information requested, Alberta Seniors had responded that there was no such type of record presently and it "would have to create such a record manually" (para. 43). The Adjudicator noted that it was unclear what "manually" meant in this response, as the initial provision of information was all generated from electronic records. She reasoned:

> section 10(2), quoted above, makes it mandatory for a public body to create a record from a record that is in electronic form, using its normal hardware and software and technical expertise, if doing so would not interfere with its operations and would assist the Applicant. If what [Alberta Seniors] means by "manually" is the manipulation of electronic data by a person, creating a new record "manually" from records in electronic form would appear to be contemplated, and required, by this provision. However, [Alberta Seniors'] evidence is ambiguous in this regard. (para. 44)

Accordingly, she ordered Alberta Seniors to determine whether it was possible to use its electronic records to create a new record that would link the website summaries to the data it had already provided.

Privacy Security Measures: The Case of the Lost Memory Stick

Also from the Alberta Office of the Information and Privacy Commissioner: in *[Re] Edmonton Public School District No. 7*, Portfolio Officer Veronica Chodak investigated a report of a missing USB memory stick by the Edmonton Public School District (the "District"). The event in question was reported by the District itself to the OIPC, which also notified potentially affected individuals. Three of the potentially affected individuals made complaints, and the Commissioner charged Officer Chodak with investigating. The USB memory stick contained a great deal of sensitive data about over 7,000 employees of the School District—police record checks, performance evaluations, identity verification information, benefits information, and for several, SIN numbers and banking information. The information, consisting mostly of scanned pdf images, was normally stored on two networked computers in the secure area of the District's office and deleted one year after retention. Because one of the computers had to be re-imaged, the data was loaded onto a USB stick and locked in a safe. The next day the stick was given to a District computer tech, who placed it in his pocket. Though he remained within the secure area of the office for the next two hours, the stick was lost and sustained efforts to locate it were unsuccessful. The District took a number of steps to deal with the loss, including the creation and circulation of documents and notifications, all of which cost $46,000.00.

Officer Chodak found that there had been no actual disclosure of the information on the stick, based on the lack of evidence that any of the information had been accessed or used. However, she also found that the District had not met its obligation under s. 38 of the Alberta *Freedom of Information and Protection of Privacy Act* to make reasonable security arrangements to protect against unauthorized access or disclosure of information. The high sensitivity of the information on the stick, in combination with the risk associated with saving the information to a portable medium, "required a proportionally high obligation on the part of the School District to protect it" (para. 30). She noted that the District had in place a number of policies which would have protected the information if lost, but which had not been followed, including the encryption and password protection of a portable device if one needed to be used. Even though the relevant area of the building itself was a secure facility, there was a chance that the information could have made its way outside the secure area. "The fact that the USB Stick was used to transport sensitive personal information within the Building is not a reasonable security arrangement. Furthermore, the USB stick was not encrypted or password protected" (para. 36).

The Officer declined to give weight to the District's submission that it would take significant effort to read the documents on the USB stick, which was not searchable by terms that could be linked to the information, noting that reading and using the information was still possible—and this was compounded by the fact that there were 15 months worth of information on the stick, which the Officer described as "unnecessary." She was satisfied with the various measures taken by the District to address the breach, though directed it to review the kinds of information collected for employee file purposes, determine whether the collection was authorized under the Act, and report back. She concluded:

> The costs of this incident, both monetary and otherwise, serve as a reminder to the School District and to other public bodies of the importance of collecting only the personal information that is required and necessary, retaining that information for only as long as is necessary, and protecting that personal information while you have it. (para. 50)

Ontario Information and Privacy Commissioner's symposium against "lawful access"

The Information and Privacy Commissioner of Ontario has brought her recent campaign against so-called "lawful access" to a crescendo on January 27, 2012 with a large symposium held in Toronto. The Commissioner, Ann Cavoukian, assembled a

panel of prominent experts from across North America to speak to a full house at Toronto's MaRS Centre. The panel included representative from the Commissioner's office, the Canadian Civil Liberties Association, and academics from the United States and Canada. In addition, John Ibbitson of the Globe & Mail provided insight into where this issue fits within the present government's priorities and how to get the government's attention. At the conclusion of the symposium, Commissioner Cavoukian urged attendees to contact their members of parliament on the issue.

"Lawful access" refers to a range of legislative initiatives that have been introduced but not yet passed by the present and past governments. Most controversial have been proposed provisions that would require telecommunications service providers ensure that new technologies have the built-in capacity for lawful access to real-time communications. In addition, and perhaps more controversially, the last iteration of "lawful access" would require telecommunications service providers to hand over to law enforcing a range of customer information without a warrant.

The full proceedings of the January symposium are available online at http://www.realprivacy.ca/.

Supreme Court of Canada says that internet service providers are not broadcasters

The Supreme Court of Canada, in *Reference re Broadcasting Act*, 2012 SCC 4, has declared that internet service providers ("ISPs") are not "broadcasters" for the purposes of the *Broadcasting Act*. In a brief, unanimous decision delivered on February 9, 2012, the Court addressed an appeal from the Federal Court of Appeal derived from a reference to that Court by the CRTC.

In 1999, the CRTC had held that "broadcasting" in s. 2(1) of the *Broadcasting Act*, included programs transmitted to end-users over the internet but declined to regulate them. When this exact question was reopened at hearings, the CRTC elected to send it to the Federal Court of Appeal for determination. The question posed in the reference was:

> Do retail Internet service providers ("ISPs") carry on, in whole or in part, "broadcasting undertakings" subject to the *Broadcasting Act* when, in their role as ISPs, they provide access through the Internet to "broadcasting" requested by end-users?

The Supreme Court concluded that when ISPs provide only the means of access to content and services over the internet – even to audio-visual programming – they are not doing so as "broadcast undertakings." Communicating or broadcasting, the Court concluded, requires more than just providing the infrastructure or the means for others to communicate or broadcast.

2ième partie

Commentaires et photos sur Facebook contredisant l'incapacité de travailler : congédiement justifié

L'employé a été relevé de ses fonctions par l'employeur afin de procéder à une enquête relativement à son absence du travail, puis congédié. L'enquête menée par l'employeur a permis de constater que, durant son absence, l'employé s'est adonné à des activités incompatibles avec le diagnostic de son médecin, soit une dépression majeure, et l'état d'incapacité allégué sur les certificats médicaux fournis durant cette période. Une recherche sur le site Facebook ayant fait voir que durant la période d'absence pour maladie, des photos et des commentaires de l'employé en voyage à Cuba démontrent des activités incompatibles avec un épisode dépressif majeur. Sur son site Facebook, l'employé a écrit qu'il avait eu un contrat de mannequin.

L'arbitre conclut que la preuve démontre que l'employé n'avait aucun motif valable pour ne pas se présenter à son retour progressif au travail tel que l'avait prescrit son médecin traitant. Il s'agissait d'un retour à raison de 2 jours de travail pour la première semaine, soit la semaine où il était à Cuba. Le relevé des activités inscrites par l'employé sur sa page Facebook démontre que s'il était en mesure de faire la fête à Cuba, il était certes en mesure de travailler 2 jours sur 5 pendant cette semaine. Même avant son départ pour Cuba, son état de santé s'était considérablement amélioré; l'employé a fait état sur sa page Facebook de ses sorties dans les bars et il ne semble aucunement être privé de ses moyens. Le résumé de ses journées à Cuba démontre qu'il s'est amusé comme il est normal que des gens dans la trentaine le fassent, rien de moins.

L'arbitre convient « que le contenu d'une page Facebook est romancé la majorité du temps par leurs auteurs. Les personnes qui écrivent sur les réseaux sociaux ne sont pas assermentées lorsqu'elles prennent le clavier et elles ne s'engagent pas à dire toute la vérité… rien que la vérité! » Mais en l'espèce il considère les récits de l'employé dans leur ensemble et conclut que l'employé n'avait aucune condition invalidante pour reprendre son travail progressivement.

- *Syndicat canadien de la fonction publique (FTQ, section locale 3535) c Société des alcools du Québec (Logistique & distribution)*, 2011 CanLII 84831 (QC SAT), 22 décembre 2011.

Diffamation par un responsable de blogue

En août 2009, le défendeur Labelle lance un forum de discussions où il dénonce l'administration de la Ville de Montréal et, plus particulièrement, l'arrondissement Pierrefonds-Roxboro et ses conseillers. Il est le seul à administrer les blogues logeant entre autres au site Internet « www.pierrefonds-roxboro.com ». Il y reproduit certains articles de journaux, questionne et dénonce ce qu'il estime être des abus de la classe politique en place. Bertrand Ward, un conseiller de ville de l'arrondissement Pierrefonds-Roxboro, demande que Labelle soit condamné à lui payer 100 000 $ pour des dommages moraux et exemplaires en raison de propos diffamatoires à son endroit diffusés sur Internet. Il demande également une ordonnance d'injonction permanente intimant à Labelle de cesser de diffuser ces propos et de les retirer du réseau Internet, en plus de désactiver les sites Internet où ces propos se retrouvent.

Tout en convenant que plusieurs propos relèvent du débat public et ne sont pas diffamatoires, le tribunal relève certains propos qui sont clairement diffamatoires et visent à insinuer de la fraude, des malversations, des abus, de la corruption. Or, les faits auxquels monsieur Labelle fait référence visent des choix politiques ou l'application de politiques qui ne supportent pas les insinuations qu'il fait.

Sur la demande d'une ordonnance afin de cesser de diffuser des propos diffamatoires, le tribunal rappelle que l'ordonnance d'injonction en matière de diffamation doit viser des propos précis et être susceptible d'exécution. Elle ne peut se limiter à interdire ou à ordonner des propos diffamatoires, mais doit préciser et identifier clairement les propos visés. Procéder autrement aurait pour effet de porter atteinte à la liberté d'expression et à bâillonner le défendeur. Il ne doit pas s'agir par ailleurs

d'empêcher monsieur Labelle de questionner les actes ou les prises de position de monsieur Ward, non plus que de l'empêcher de critiquer son travail, mais de faire cesser la diffamation par les insinuations, les associations et les accusations gratuites. Bien qu'aucune preuve technique n'ait été présentée devant le Tribunal, monsieur Labelle a témoigné être le seul à alimenter le blogue. Il a mentionné y avoir déjà retiré certains articles. La preuve démontre ainsi qu'une ordonnance ciblée sur certains propos pourra être exécutée. En l'instance, le Tribunal a identifié les propos qu'il considère diffamatoires à l'endroit de monsieur Ward et ordonne à Labelle de cesser de les diffuser, de les publier, de les reproduire ou de les faire circuler sur son blogue ainsi que de désactiver et retirer de l'Internet ces propos qualifiés de diffamatoires dans le jugement.

- *Ward c. Labelle*, 2011 QCCS 6753 (CanLII), 7 décembre 2011.

Diffamation – Conséquences de l'inaction

Canoë inc. interjette appel du jugement ayant accueilli l'action en diffamation de Corriveau et l'ayant condamné à des dommages exemplaires et des honoraires extrajudiciaires. Selon la juge de première instance, Canoë ne pouvait ignorer les conséquences extrêmement négatives pour Corriveau de la publication de certains commentaires à son sujet sur le blogue de Martineau, qui utilise le portail Internet de Canoë. Canoë allègue que la juge de première instance n'avait pas de raison ou de preuve lui permettant de conclure qu'elle connaissait les conséquence probables de son inaction à intervenir afin de retirer les documents comportant des propos diffamatoires sur un blogue dont elle avait le contrôle. La Cour d'appel conclut qu'il existait une telle preuve.

Tout d'abord, à l'article 2 des règlements du blogue de Richard Martineau, on énonce ce qui n'est pas toléré dans les propos, messages ou contenus du blogue: «la vulgarité, les propos injurieux, diffamatoires, obscènes ou offensants, les menaces, le harcèlement, les attaques personnelles, les propos discriminatoires, racistes ou sexistes, l'incitation à la violence ou à la haine, les propos n'ayant aucun rapport avec les messages et destinés uniquement à provoquer, la divulgation d'informations personnelles et confidentielles permettant l'identification nominative d'une personne autre que vous-même, le manque de respect envers Richard Martineau, un autre membre, un admin ou des modérateurs».

Par ailleurs, les articles 4.8, 4.9 et 5.2 d'une convention de services entre Canoë et Richard Martineau prévoient que le blogueur s'engage à « prendre les mesures raisonnables afin de s'assurer que les usagers du Blogue respectent les règlements du Blogue; » et à « prendre les mesures raisonnables afin de surveiller et contrôler le contenu publié ou diffusé sur le Blogue pour que ledit contenu respecte les règlements du Blogue et respecte les lois applicables ». Le même règlement prévoit que « CANOË se réserve le droit de demander au BLOGUEUR de supprimer du contenu qui viole les règlements du Blogue ou pouvant exposer CANOË à toute poursuite d'un tiers. Pour aider le BLOGUEUR dans sa tâche de modération, les modérateurs de CANOË se rendront plusieurs fois par semaine dans le Blogue pour modérer les commentaires. CANOË se réserve également en tout temps le droit de suspendre sans préavis le Blogue ainsi que d'y supprimer tout contenu qu'elle considère inadéquat ».

Or, Richard Martineau a ensuite été relevé de son obligation d'agir comme modérateur de son blogue, sans que Canoë prenne de mesures pour s'assurer que l'article 2 des règlements du blogue soit respecté. Dans de telles circonstances, la juge de première instance était justifiée de conclure que Canoë connaissait les conséquences probables de son inaction à cet égard.

- *Canoë inc. c. Corriveau*, 2012 QCCA 109 (CanLII), 19 janvier 2012.

Application de la législation québécoise à un intermédiaire agissant depuis les Iles Vierges

Le Bureau de décision et de révision en valeurs mobilières est saisi d'une demande afin qu'il prononce une ordonnance d'interdiction d'exercer l'activité de conseiller et une interdiction d'opération sur valeurs à l'encontre des intimés. La principale question est de savoir si les intimés devaient s'inscrire auprès de l'Autorité des marchés financiers, en vertu de l'article 148 de la *Loi sur les valeurs*

mobilières, afin d'exercer leurs activités de conseiller, telles qu'elles sont définies à l'article 5 de la même loi. Ces activités auraient été exercées pour le compte de la société Blue Horizon (BVI) Fund Ltd, une personne morale constituée selon les lois des Îles Vierges Britanniques le 21 juin 2005. Les intimés soutiennent que tout se passe ailleurs que sur le territoire québécois et que les lois québécoises sur les valeurs mobilières ne sont pas applicables à leurs activités de conseiller en valeurs.

Le Bureau retient qu'au moins 13 investisseurs québécois ont fait l'acquisition de titres de Blue Horizon pour des montants variant entre 2 et 2.5 millions de dollars, sur un total de placements des titres du fonds qui s'élève à des montants variant entre 3.5 et 4 millions de dollars. Ces épargnants sont en droit de s'attendre à ce que les mécanismes de protection de la loi soient activés afin d'assurer leur protection lorsqu'on s'adresse à eux pour investir. Puis, les intimés sont situés physiquement au Québec, à partir duquel ils rayonnent ensuite pour exercer leurs activités. Cela est suffisant pour donner à l'Autorité le pouvoir d'agir à leur égard pour surveiller leurs activités, comme l'a d'ailleurs déterminé la Cour suprême du Canada dans l'arrêt Gregory [*Gregory and Company Inc. c. The Quebec Securities Commission*, 1961 CanLII 75 (SCC), [1961] R.C.S. 584]. Peu importe où se déroulent les activités que l'Autorité veut encadrer, cette dernière agira s'il existe au Québec un facteur de rattachement suffisant pour que soient mis en marche les mécanismes destinés à protéger le public investisseur, en assurant que ceux qui agissent comme leurs intermédiaires de marché « shall be honest and of good repute and, in this way, to protect the public, in the province or elsewhere, from being defrauded as a result of certain activities initiated in the province by persons therein carrying on such a business ». Le Bureau ajoute que « Cette interprétation ne constitue pas un refus de la modernité. Le Bureau a précédemment reconnu l'usage de l'Internet comme un moyen de sollicitation légitime en valeurs mobilières; en même temps il a rappelé que cela ne change en rien les principes de base qui gouvernent le commerce des valeurs mobilières et assurent la protection du public » .

- *Autorité des marchés financiers c. Investissements de capital Dynahedge inc.*, 2011 QCBDR 119 (CanLII), 21 décembre 2011.

Ordonnance de s'abstenir de harceler ou intimider par courriel ou via Facebook

Le Tribunal statue sur une requête pour garde d'enfant, pension alimentaire et mesures de sauvegarde, laquelle est présentée par madame. Il est évident que la relation entre les parties est malsaine, surtout quand on considère les propos menaçants inscrits par monsieur sur sa page Facebook et le témoignage des parties. Ainsi, considérant la nature du dossier et les échanges menaçants ayant eu lieu entre les parties, que ce soit verbalement ou par les mentions faites par le biais de réseaux sociaux (Facebook) de la part de monsieur, et suite à la suggestion faite par monsieur, le Tribunal est d'avis que monsieur devrait remettre toutes ses armes à feu à la Sûreté du Québec. Le tribunal lui ordonne de ne par harceler ou autrement intimider madame, que ce soit verbalement, par courriel ou même par le biais de messages laissés sur des réseaux sociaux (Facebook – Twitter ou autres) sous peine de perdre ses droits d'accès à ses enfants

- *Droit de la famille — 114259*, 2011 QCCS 7282 (CanLII), 7 décembre 2011.

Gérer les risques juridiques du Web 2.0 : un guide pour les entreprises et organisations

Les internautes, entreprises privées et organismes publics qui explorent les multiples applications du Web 2.0 sont nombreux à se questionner sur les enjeux et risques que comportent de telles applications. Sans précautions, les activités d'échange, de recherche et de diffusion d'information sur Internet peuvent comporter des écueils. En particulier, il y a des risques de se trouver dans une situation pour laquelle la loi a prévu des exigences ou des interdits. Il importe donc de savoir identifier de telles situations et de se donner les moyens de reconnaître une situation nécessitant des précautions. Ce guide vise à accompagner les individus et les organisations concernés par l'utilisation des applications associées au Web 2.0 afin d'assurer que leurs activités se déroulent dans le respect des lois applicables au Québec.

- Pierre TRUDEL et France ABRAN, *Gérer les enjeux et risques juridiques du Web 2.0,* Centre de recherche en droit public, décembre 2011, disponible sur le site du CEFRIO.

Réforme de la directive sur la protection des données personnelles – Commission européenne

Le 25 janvier 2012, la Commission européenne a proposé une révision majeure de la Directive sur la protection des données personnelles. La réforme soumise par la Commission met à jour et modernise les principes inscrits dans la directive de 1995 relative à la protection des données afin de garantir à l'avenir les droits en matière de respect de la vie privée.

Les principales modifications apportées par la réforme sont notamment les suivantes :

- *un corpus unique de règles relatives à la protection des données sera valable dans toute l'Union. Les obligations administratives inutiles, comme celles en matière de notification qui incombent aux entreprises, seront supprimées, ce qui représentera pour ces dernières une économie annuelle de quelque 2,3 milliards d'EUR;*
- *en lieu et place de l'obligation actuelle imposée à toutes les entreprises de notifier l'ensemble des activités concernant la protection de données à des autorités de contrôle compétentes en la matière – cette obligation étant à l'origine de formalités administratives inutiles coûtant 130 millions d'EUR par an aux entreprises, le règlement impose davantage d'obligations aux entités procédant au traitement de données à caractère personnel et accroît leur responsabilité;*
- *Ainsi, les entreprises et organisations devront, dans les meilleurs délais (si possible, dans un délai de 24 heures), notifier à l'autorité de contrôle nationale les violations graves de données à caractère personnel;*
- *les organisations n'auront plus comme interlocuteur qu'une seule autorité nationale chargée de la protection des données dans le pays de l'Union où elles ont leur établissement principal. De même, les citoyens pourront s'adresser à l'autorité chargée de la protection des données dans leur pays, même lorsque leurs données sont traitées par une entreprise établie en dehors du territoire de l'UE. Chaque fois que le consentement de la personne concernée est exigé pour que ses données puissent être traitées, il est précisé que ce consentement ne sera pas présumé mais devra être donné explicitement.*
- *l'accès des personnes concernées à leurs propres données sera facilité, de même que le transfert de données à caractère personnel d'un prestataire de services à un autre (droit à la portabilité des données). La concurrence entre prestataires de services s'en trouvera renforcée.*
- *un «droit à l'oubli numérique» aidera les citoyens à mieux gérer les risques liés à la protection des données en ligne: ils pourront obtenir la suppression de données les concernant si aucun motif légitime ne justifie leur conservation.*
- *les règles de l'Union devront s'appliquer si des données à caractère personnel font l'objet d'un traitement à l'étranger par des entreprises implantées sur le marché européen et proposant leurs services aux citoyens de l'Union.*
- *les autorités nationales indépendantes chargées de la protection des données seront renforcées afin qu'elles puissent mieux faire appliquer et respecter les règles de l'UE sur le territoire de l'État dont elles relèvent. Elles seront habilitées à infliger des amendes aux entreprises qui enfreignent les règles de l'Union relatives à la protection des données. Ces amendes pourront atteindre 1 million d'EUR ou 2 % du chiffre d'affaires annuel global de l'entreprise.*
- *Une nouvelle directive appliquera les règles et principes généraux relatifs à la protection des données à la coopération policière et judiciaire en matière pénale. Les règles s'appliqueront aux traitements aussi bien*

transfrontières que nationaux de données à caractère personnel.

Les propositions de la Commission seront transmises au Parlement européen et aux États membres de l'UE pour y être examinées et débattues et elles entreront en vigueur deux ans après leur adoption.

- COMMISSION EUROPÉENNE, *Communiqué – La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données, et réduire les coûts grevant les entreprises*, 25 janvier 2012.

Consultation sur les enjeux du « Cloud Computing » – Commission européenne

La Commission européenne a rendu public les résultats de sa consultation publique sur l'informatique en nuage. Cette consultation s'inscrit dans la démarche de l'exécutif européen afin de déterminer la meilleure stratégie pour développer cette technologie dans les années à venir. La consultation portait sur des problématiques juridiques et techniques, notamment au niveau des données personnelles et de la résistance des services en nuage. Ceux qui ont participé à la consultation en ligne ont exprimé le voeu que les droits et les responsabilités relatifs à l'infonuagique soient plus explicites. Des lignes directrices et la diffusion de pratiques exemplaires seraient également utiles et appréciées. Les participants estiment que cette clarification accélérerait le déploiement de l'infonuagique, mais que des normes internationales doivent être élaborées.

La réflexion de la Commission se déploie en trois axes principaux. Un premier axe vise la réglementation du secteur, au niveau «par exemple de la protection des données et de la vie privée, des règles claires pour l'allocation de la juridiction, la responsabilité, et la protection des consommateurs». Se pose notamment la question de savoir «qui sera responsable si quelque chose va mal avec le cloud et si des données sont perdues ou compromises». La Commission semble peu encline à s'en remettre à l'autorégulation des professionnels du secteur. Le deuxième axe concerne les fondamentaux techniques et commerciaux du cloud computing. La Commission souhaite participer activement à la standardisation des API et du formatage des données, qui doivent «améliorer l'interopérabilité et la concurrence entre les fournisseurs». Enfin, le troisième axe s'intéresse à l'application concrète sur le marché, avec la promotion de programmes pilotes et l'incitation du secteur public à utiliser des services en cloud.

- EUROPEAN COMMISSION, *Cloud Computing Consultation Report*, 5 décembre 2011.

L'affaire MegaUpload mettrait en lumière les risques pour les services d'infonuagique (cloud computing)

L'auteur constate que la justice a réussi la fermeture de MegaUpload notamment grâce à une particularité dans la manière dont le site a conçu sa structure informatique : plusieurs serveurs étaient physiquement aux États-Unis, dont des serveurs de mails, ce qui a permis de recueillir avec plus de facilité un certain nombre d'informations et de mettre au point l'acte d'accusation.

Cela a permis aux autorités de justice d'agir au niveau des fournisseurs de MegaUpload pour prendre connaissance d'informations qui y sont relatives. D'où la rumeur selon laquelle les données contenues dans les serveurs de MegaUpload vont être effacées. Par un curieux effet de ricochet, l'affaire MegaUpload pourrait poser un problème majeur à ceux qui ont recours aux services d'infonuagiques (Cloud).

De moins en moins de fournisseurs en ligne possèdent en propre l'intégralité de l'architecture technique nécessaire à la fourniture des services. Or, la justice va maintenant probablement obtenir *de facto* l'effacement des données car ces mêmes fournisseurs ne sont plus payés. Si cela devait se confirmer l'affaire MegaUplaod aurait montré que tout service fondé sur ce modèle peut aisément être *de facto* arrêté d'une seconde à l'autre (surtout s'il implique des fournisseurs américains) et que la pérennité des données n'est pas toujours assurée. Cela indiquerait l'ampleur des risques associés à certains modèles d'infonuagique notamment au plan de la continuité du service, de la sécurité et de la disponibilité des données.

- Étienne WERY, « L'affaire MegaUpload mettra-t-elle en péril le modèle du cloud ? », *Droit & Technologies,* 1er février 2012.

Obligation de l'employeur d'informer le salarié de la vidéosurveillance – France

La Cour de Cassation, dans son arrêt du 10 janvier 2012 a indiqué que : « Si l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, il ne peut être autorisé à utiliser comme mode de preuve les enregistrements d'un système de vidéosurveillance installé sur le site d'une société cliente permettant le contrôle de leur activité dont les intéressés n'ont pas été préalablement informés de l'existence ».

Un employeur a demandé une ordonnance pour obtenir les enregistrements des caméras de vidéosurveillance placées à l'entrée de l'établissement de la cliente afin de comparer les entrées et sorties de ses salariés avec les relevés d'activités du chef d'équipe. Les employés ont demandé la rétractation de l'ordonnance et l'annulation des actes qui en ont découlé. Selon eux, ces images ne constituent pas une preuve licite car ils n'avaient pas eu d'information préalable sur le fait que le dispositif de vidéosurveillance destiné à surveiller les intrusions pouvait également servir à contrôler leur activité.

- *M. X. /TFN*, Cour de Cassation, Chambre sociale, Arrêt du 10 janvier 2012, *Legalis.net.*

Caractère licite des moteurs de recherche d'annonces publicitaires – France

Dans une décision rendue le 26 janvier 2012, le Tribunal de Grande Instance de Paris a statué que les moteurs de recherche qui référencent automatiquement des petites annonces provenant de différents sites qui eux-mêmes relaient les données d'agences ne commettent aucun acte de contrefaçon de bases de données, de concurrence déloyale et de parasitisme. Avec un robot explorateur, les moteurs de recherche Yakaz.com, Gloobot.co et comintoo.com indexent automatiquement les annonces qu'ils trouvent sur des sites. L'internaute qui souhaite obtenir les détails d'une annonce doit cliquer sur l'annonce pour être dirigé vers le site dont elles sont issues. Le tribunal a considéré que le seul fait d'agglomérer des messages n'équivaut pas à produire une banque de données. *« La seule centralisation par la SAS Pressimmo On Line des annonces immobilières des agences clientes ne caractérise pas des actes de constitution, de vérification ou de présentation du contenu de la base de données et encore moins un investissement financier, matériel ou humain substantiel ».* De même, il n'y a pas en l'espèce de concurrence déloyale et parasitaire pour la reprise des contenus et des images. Les moteurs de recherche ne sont pas concurrents des sites sur lesquels se trouvent les différentes annonces. L'internaute est obligé de se rendre sur le site source pour avoir les informations essentielles. Le tribunal rappelle que les sites qui ne veulent pas être référencés peuvent poser des règles spécifiques pour empêcher l'indexation. Le tribunal écarte aussi l'accusation d'agissements parasitaires car l'essentiel des informations proposées n'est pas communiqué. *« Aucune faute ne peut être reprochées aux défenderesses et la SAS Pressimo On Line n'a subi aucun préjudice, les défendeurs ne réalisant aucune captation de clientèle mais au contraire orientant les internautes vers le site Seloger.com ».*

- *Pressimmo on Line c. Solus Immo, Yakaz, Gloobot*, Tribunal de grande instance de Paris, 3ème chambre, 4ème section, Jugement du 26 janvier 2012, *Legalis.net.*

À signaler

- Ètienne WERY, « MegaUpload, Anonymous, etc. : l'Internet entrera-t-il en rébellion ? », *Droit & Technologies*, 25 janvier 2012.

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.