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

April 20, 2007/20 avril 2007

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors Teresa Scassa, 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 Teresa Scassa, Chidi Oguamanam et Stephen Coughlan de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie. Les professeurs Pierre Trudel et France Abran de le Chaire en droit des technologies de l'information et du commerce électronique L.R. Wilson de la Faculté de droit de l'Université de Montréal ont rédigé la seconde partie du présent bulletin.

Part 1

Criminal Law: Child Pornography

The Ontario Court of Justice has delivered, in writing, reasons for its oral decision in *R v. Strohmeier.* In that case, a nephew saw disturbing images on his uncle's computer and called the police. The police executed a search warrant at the offender's home where they seized a computer connected with six extra hard drives with storage capacity of 29 laptop computers. Police discovered from the computer a vast amount of sexually explicit materials arranged in folders. This included 30, 000 pictures of child pornography out of which 10, 000 were duplicates, 378 porn videos (including 22 duplicates). The offender claimed that he was a recent immigrant from Germany and that he had obtained the images from that country for curiosity and that he did not believe that his conduct amounted to an offence in Germany. However, he expressed desire to plead guilty. Nonetheless, he remained in custody while the police reviewed the overwhelming data in his computer. After the police review, the Crown presented a representative sample of the child pornography in the offender's computer for purpose of use in sentencing. The sample consists of "150 pictures and 15 videos… All images involve the degradation and humiliation of young children, many of whom appear to be between five and seven years old. Most images record vaginal, anal, and oral penetration by adult men with prepubescent girls…" (¶4) In the words of the court, "[v]iewing these images was a painful duty" (*ibid.*)

The offender has served the equivalent of eight and half months and the Crown is inclined to have him serve an additional three and a half months to reflect an effective sentence of twelve months. The defence wants the court to impose a sentence of the time served. In reviewing the seriousness of the offence of child pornography, the court observes that minimum jail term for child porn "is a recent amendment of the *Criminal Code* that reflect Parliament's decision to remove the possibility of a conditional sentence for the offence" (¶6). In endorsing, in part, the recent decision in *R v. Kwok*, the court affirms that "there is a direct connection between the person who possesses child pornography and the abuse of children in those images" (¶7) However, the court notes that the *Kwok* decision which sentenced an offender to twelve months "may not represent a coherent and considered approach to sentencing for child pornography" (¶8).

The court held that as regards the offence in question, what is important to consider is the nature and collection of child pornography and noted that a small collection by a first offender could be a mere indication of curiosity and nothing else. In weighing the mitigating and aggravating factors, the court noted that the offender is aged 48 years, divorced, without children, a productive member of his German and Canadian communities, skilled in cabinet making and computer technology. He does not have a criminal record and he pleaded guilty. However, the court considered the particulars of this offence as "most aggravating" given that, *inter alia*, the offender "maintained a large and well-organized collection of images that record profound and violent physical contact between males and young children … The size and nature of the collection goes beyond mere curiosity and the mere possession of the images harms children" (¶¶10, 11). In addition to several ancillary orders, the court sentenced the offender to another nine and one-half months

culminating in an effective sentence of eighteen months. It acknowledged that "[t]his is at the top end of the range identified in *Kwok*" and noted that even though it is not bound to follow *Kwok*, the offender in this case was more aggravating than *Kwok*.

While ruling that the offender's seized computer be forfeited to the Crown, the court attempted to accommodate the offender's claim for personal and lawful information stored on the computer including immigration, medical and employment records. Consequently the court ruled:

> I do not know if this is an easy or difficult task and, in all circumstances, I do not wish to place an undue burden on scarce resources. The forfeiture of computer equipment seized by police is subject to reasonable efforts being made by the police, to preserve data and/or return equipment that is lawfully possessed by the offender. This data and/or equipment must be identified by the offender and communicated to the police within 90 days and he must pay for the reasonable coats of preserving data" (¶15).

Comment on the issues raised in this item at IT.Can blog

Electronic Disclosure

In *R v. Piakowski*, the Manitoba Court of Queen's Bench considered applications by a group of accused persons seeking relief on the basis that the prosecution's electronic disclosure of materials was not a proper disclosure and violated their *Charter* rights.

The accused persons were charged with offences under the *Controlled Drugs and Substances Act* and the *Criminal Code*. The charges were the result of a lengthy investigation, which produced "thousands of pages of written material, as well as hundreds of hours of video and audio taped surveillance." (at para 3). The Crown provided disclosure of all of this material in electronic form on both CD-ROMs and DVDs. The accused sought a remedy under s. 24(1) of the *Charter*, namely an order directing the Crown to provide disclosure of all documents and transcripts in hard copy format, or to subsidize the cost of having all the documents produced in this format.

In making this application, they alleged that their rights were infringed because "either the accused or counsel do not have the necessary skills, training or experience to make full use of the materials in the manner provided", the volume of materials is such that the cost of producing them in a usable format would be prohibitive, and that the failure to provide hardcopies violates s. 7 of the *Charter*. One of the accused was not represented by counsel, and in his case, he argued that "lacking computer equipment, he is unable to readily access the disclosure in electronic form." (at para 6) The Crown objected to providing disclosure in hard copy format because of both the time and costs that would be involved in doing so. Further, they argued that because of the volume and complexity of the material, it would be to the advantage of defence counsel to have the materials in electronic format.

In reviewing prior case law on electronic disclosure in great detail, Sinclair J. noted that electronic disclosure has been found to be acceptable in some cases, and not in others. He summarized what he distilled as the general principle as follows: "electronic disclosure is not *per se* objectionable so long as the accused can reasonably access the electronic materials." (at para 21) He noted that in some cases prior cases have found that "in special circumstances, an accused may not receive adequate disclosure if made in electronic form, particularly where the accused is unrepresented, in custody, computer illiterate or otherwise prevented from accessing the disclosure" (at para 43). Sinclair J. also observed that, for lawyers, the ability to use technology was a competency issue. He cited provisions from the codes of professional conduct for Alberta and Manitoba which make reference to the duty of lawyers to adapt to technological change.

The electronic materials in this case were complied using a program used by the RCMP called Supertext. The accused argued that this program was problematic for several reasons. One reason was that it required a learning curve to operate effectively, and that, as it was regularly used by police and the Crown, the prosecution was at an advantage in operating the program. It was also argued that the program had some limitations: it could not search handwriting or faded and small text. Thus there was still the necessity to go through many documents

line by line. The accused also argued that "the search function of Supertext does not assist in any way in figuring out all of the intricacies of a complex conspiracy trial" (at para 57).

Other issues were also raised by the accused. It was argued that the Crown would be obliged to produce documents in hard copy for admission at trial in any event, and that these documents would have to be made available to the accused parties. They also noted that "In electronic form, counsel and his/her client are unable to pass documents back and forth for discussion, thereby limiting the accused's right to make full answer in defence". (at para 61) Some of the lawyers for accused persons in this case objected to being required to change the manner of working with documents that they have become accustomed to throughout their careers, and that this created unfairness. If they were required to step aside to allow more computer literate lawyers to represent their clients, this would limit the right of the accused to counsel of their choice.

The lawyers for the accused persons also argued against being required to follow the document organization of the Crown. Their arguments were summarized by the court as follows:

> This allows the police and prosecution to dictate the manner in which counsel for the accused are able to conduct their defences. Counsel point out that it forces counsel to try to find the documents where the police have stored them instead of being able to put the documents into binders in a manner that counsel would prefer to organize. Counsel point out that the manner of organization for the prosecution of a matter is distinctly different from the manner in which defence counsel would organize their cases. Electronic disclosure limits counsel's ability to do that. In order to organize the data in a manner consistent with their approach to the case, counsel will have little choice but to print out the documents in order to physically organize the printed material. (at para 66)

The Crown took the view that they had taken all reasonable steps to address the concerns of the accused, including providing training and technical assistance to those who wished it. The Crown also argued that "there is distinction between disclosure in a form that the accused and counsel cannot access and disclosure in a form that the accused or counsel refuses or declines to access." (at para 75)

In considering the arguments and the evidence, Sinclair J. concluded that there had been no *Charter* violation. He noted that the limitations of the program in handling handwritten text could be worked around by printing and reviewing those documents with handwriting on them. He also took the view that "once counsel and accused gain some familiarity with the use of the Supertext software, the use of it will prove a benefit and not a burden." (at para 83) He also reached a number of conclusions regarding the principles of disclosure generally, and electronic disclosure more specifically. On this latter issue he noted: "electronic disclosure is not objectionable merely because of counsel's lack of computer skills unless it can be shown that access to the material swould be beyond the competence of the average reasonably skilled person." (at para 84) He also stated that: "Where the Crown wishes to make electronic disclosure as opposed to paper disclosure, the Crown has a further obligation to assist counsel lacking familiarity with the software utilized." (at para 84) The obligation is more extensive with an unrepresented accused "who *bona fide* has limited or no computer skills". He also stated that electronic disclosure must be in a format that permits the making of paper copies, and "If the cost of producing hardcopies of the electronic documents interferes with the accused's ability to make full answer and defence, the court can order the Crown to provide hardcopies of electronic disclosure at Crown expense." (at para 84)

Comment on the issues raised in this item at IT.Can blog

Electronic Documents

Adamo v. College of Physicians and Surgeons of Ontario is a decision of the Ontario Divisional Court on an appeal from an Order of the Discipline Committee of the College of Physicians and Surgeons of Ontario. The Committee had made a finding of professional misconduct against Dr. Adamo. The doctor operated a series of private radiology clinics. While certain complaints were being dealt with by the College, its Executive Committee had

placed conditions on the appellant's certificate of registration. One of these was a requirement that he appoint a quality advisor for his clinics who was acceptable to the College. The first person the appellant proposed was rejected by the College. The appellant then entered into discussions with another physician, Dr. Nitsch, regarding her willingness to assume the role of quality advisor for the clinics. A copy of the quality advisor agreement was faxed to her for her signature. At the same time, the appellant faxed a copy of the agreement to the College, to which he affixed an electronically generated version of her signature. A copy of this signature was in the clinic's computer system and had been used in the past to sign her reports.

The College never ultimately accepted Dr. Nitsch as a quality advisor, and one aspect of the penalty imposed on Dr. Adamo related to his operating of clinics in contravention of the College's requirement regarding the appointment of an acceptable quality advisor. However, he was also disciplined for falsifying a record relating to his practice, and this related to his affixing of Dr. Nitsch's electronic signature on a document to which she had not agreed. The appellant argued that there had been an innocent miscommunication between himself and Dr. Nitsch, and that he genuinely believed he had her permission to affix her signature to the document. The Discipline Committee had found that Dr. Nitsch had not given her permission, and that her signature was appended by Dr. Adamo without any authority to do so. The Court of Appeal upheld this aspect of the decision which found that Dr. Adamo had falsified a record relating to his practice.

Comment on the issues raised in this item at IT.Can blog

Labour & Employment Law

The British Columbia Supreme Court has delivered its ruling in *Rysstad v. Dependable Turbines Ltd.* In this case, the plaintiff applied to the court for damages arising from alleged wrongful dismissal. The plaintiff is an employee of the defendant, Mr. Prior, whose company operates a small business that builds and sells hydroelectric turbines. In 2001, Mr. Prior, who doubles as the owner and president of the defendant company, obtained two major contracts for the supply of turbines which were, by all standards, above the company's volume of business. Consequent upon the contract, Mr. Prior took some administrative decisions regarding the operations of the company. He also negotiated an immediate wage increase with his employees. Further, he made a commitment to consequently index their wages. Both parties were not in agreement in regard to details of the indexing program. The plaintiff championed the desire of the employees to have Mr. Prior make good on his commitment to index their wages. Prior to his campaign for wage indexing, the plaintiff's relationship with the defendant appeared to have deteriorated. That relationship was characterized by friction and altercations which only got aggravated by the wage indexing issue.

The frictions peaked on a particular day the plaintiff irritated the defendant that the latter "left work in mid-afternoon and did not return" (¶ 10) A few days after, the defendant "took a concealed tape into the computer room where Mr. Rysstad was eating lunch", an act that was prohibited in the computer room (¶11). In holding that the defendant's subsequent termination of the plaintiff's employment was for a just cause, the court observed as follows:

> The tape recording, because of the fact that only Mr. Prior was aware of its presence, provides evidence that must be approached with caution. However, even making generous allowances for the circumstances under which the recording was obtained. Mr. Rysstad's behaviour toward Mr. Prior was inexcusable, and in my view, is a fundamental breach of the employment relationship. It is clear from the tape recording, in which Mr. Rysstad calls Mr, Prior a liar and a "fucking asshole" and clearly indicates to him that that he considers him an incompetent employer, that the employment relationship was irreparably ruptured and having viewed the tape recording, I conclude that it is likely that Mr. Prior's characterization of Mr. Rysstad as the conversational aggressor in the previous confrontation is correct (¶¶12, 13)

Comment on the issues raised in this item at IT.Can blog

The British Columbia Supreme Court has delivered its ruling in *Stuart v. Navigata Communications Ltd* – a company that provides voice and telecommunication services to businesses. The plaintiff was an employee of the defendant company for 24 years before her employment was terminated in March 2006. In terminating the plaintiff's employment, the defendant did not allege any cause nor did it give the plaintiff any notice. In this action, the plaintiff sues the defendant for damages in lieu of reasonable notice and damages for bad faith dismissal (*Wallace* damages) and for punitive damages. The plaintiff, a mother of two children aged 6 and 8, originally had a three-day work week. After one of her children was diagnosed with Type I Juvenile Diabetes, she secured a leave of absence (with pay) from the company. She was tentatively scheduled to return in April 2006. While on leave of absence, the defendant asked her to consider a severance package. She did by entering into negotiations. She was under the impression that she had the option to return to work if she was not able to reach a suitable agreement with the defendant.

The court found that "a major reason for Ms. Stuart's dismissal was the fact that she was working part-time and the company felt that there was no longer room for part-time employment such as hers" (¶81). That decision was made in 2005 even though the company scheduled the plaintiff's return date for 2006 and did not change that decision at any time between those two periods. The company deliberately delayed informing the plaintiff of the decision because it was yet to figure out how to deal with the accounts that the plaintiff left behind (the plaintiff was the Manager of Strategic Accounts and was in charge of the company's top ten accounts). Overall, the company took advantage of the plaintiff's request for a leave of absence in order to perfect her dismissal through offering her an option for severance package and entering into a negotiation with her even when it had pretty much decided on her dismissal and predetermined a severance package of $111,000. The plaintiff's conducts including e-mail she sent indicated that she was under the impression that negotiation was still going on, but the company did not correct her. She was led to believe by the company executives that the meeting at which the decision to terminate her employment was finally made was one to further discuss her severance package. The court found that "[a]ll of these was happening at a time when she [the plaintiff] was vulnerable because of her son's serious and unexpected illness" (¶84)

In holding that the company acted in bad faith and as such liable for Wallace damages in its dealing with the plaintiff, the court noted, inter alia, that "Navigata immediately cut off access to her [the plaintiff's] computer, including personal information. The fact that it did so because it was company policy does not make it any less high-handed" (¶85). The court followed the BC Court of Appeal decision in *Health Sciences Association of BC v. Campbell River and North Island Transition Society* and adopted the latter court's definition of "family status" and held that the defendant company's treatment of the plaintiff amounted to *prima facie* discrimination based on family status. It ruled, *inter alia*, that the plaintiff was entitled to 20 months' notice which includes 2 months' notice for *Wallace* damages.

Privacy

The Federal Privacy Commissioner has issued her findings in her investigation of the Society for Worldwide Interbank Financial Telecommunication (SWIFT). The Commissioner had initiated this complaint following a newspaper report that alleged that SWIFT had disclosed a substantial number of financial records to the U.S. Treasury. The Commissioner's complaint had a Canadian focus; she alleged that SWIFT "inappropriately disclosed personal information originating from or transferred to Canadian financial institutions to the US Department of the Treasury (UST)". (at para 2)

SWIFT is a co-operative organization serving the financial industry at the global level. It operates as a "messaging intermediary for transmitting secure and confidential financial messages on behalf of, and between, financial institutions." (at para 3) Six of Canada's largest banks are shareholder members of SWIFT, and they are regular users of SWIFT services.

SWIFT confirmed that it had disclosed data regarding certain financial transactions to the U.S. government in response to subpoenas issued by the UST. These disclosures occurred after 9/11, and were part of U.S. anti-terrorism investigations. The Commissioner noted that SWIFT had taken care to establish that

subpoenas were valid. They explained that the provided only requested data, and did not provide general access to their databases. They also sought assurances that the data would only be used for terrorism investigation purposes. SWIFT expressed the view that it was bound to comply with the subpoenas, and noted that it negotiated terms for privacy protection of the data provided to the UST. The Commissioner was given the opportunity to view detailed confidential documents provided by SWIFT relating to the privacy protections negotiated with the UST. She stated: "Based on the information presented to us, I am of the opinion that SWIFT did indeed ensure that the UST abided by the protections negotiated by SWIFT." (at para 35)

In dealing with the complaint the Commissioner considered two main issues. The first was jurisdictional: did PIPEDA apply to the collection, use, or disclosure of personal information by SWIFT in the course of operations in Canada. The Commissioner found a real and substantial connection to Canada on the basis that SWIFT operated in Canada, collected and disclosed personal information from and to Canadian banks in the course of commercial activity, and has shareholders and one Director who are Canadian. She noted that the SWIFT network is "an integral part of the Canadian financial system" (at para 41). Later, in formulating the conclusions of her reasons, Commissioner Stoddard stated: "I must stress that organizations operating in and connected in a substantial way to Canada are subject to the Act…Simply because an organization might operate in two or more jurisdictions will not alleviate it of its obligations to comply with Canadian law." (at para 54)

The second issue considered by the Commissioner was whether SWIFT's actions in responding to the subpoenas complied with Canadian law. She noted that PIPEDA "allows for an organization such as SWIFT to be able to abide by the legitimate laws of the other countries in which it operates." (at para 46) She describes her interpretation of the Act as one "that recognizes that some organizations operate in more than one jurisdiction". (at para 46) She stated:

> [I]n my opinion, the Act acknowledges that an organization that is subject to the Act and that has legitimately moved personal information outside the country for business reasons may be required at times to disclose it to the legitimate authorities of that country. In this case, I am of the view that paragraph 7(3)(c) operates to allow SWIFT to respond to a valid subpoena issued in the United States. (at para 48)

The Commissioner found that there was no violation of PIPEDA.

In her conclusions, the Commissioner noted that Canada had responded to the need to fight terrorism through surveillance in a different manner from the US. She observed that Canada has separate legislation and a separate oversight body designed for the investigation of terrorism financing. While noting that there are still some issues with the privacy protections under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, "there is at least some notion of transparency". (at para 55) She also stated that she would be recommending "that the appropriate Canadian officials work with their US counterparts in order to encourage the US government to use its anti-money laundering/anti-terrorism financing regime instead of the subpoena route used in the present case." (at para 57) She stated: "If US authorities feel that they need to obtain information about financial transactions that have a Canadian component, they should be encouraged to use existing information-sharing mechanisms that have some degree of transparency and built-in privacy protections." (at para 57) She also noted that European officials have already approached SWIFT about finding a "better way of achieving its business needs to provide enhanced protection over the personal information held by SWIFT." (at para 59)

Comment on the issues raised in this item at IT.Can blog

In a related set of findings, the Assistant Privacy Commissioner, Heather Black, released the results of her investigation against six Canadian banks which were related to the same disclosures of information by SWIFT to the UST. The complainant took the position that "the banks were responsible for the personal information that was transferred to SWIFT for processing of money orders", and that the disclosures by SWIFT violated PIPEDA.

Ms. Black reviewed the agreements in place between the banks and SWIFT. She also reviewed the operations of SWIFT. She concluded that "SWIFT and its members have collaboratively developed and implemented a highly sophisticated and elaborate set of security measures to ensure the integrity, confidentiality, security and reliability of the financial messages that SWIFT delivers." She found that the banks were in compliance with their obligations under PIPEDA regarding providing notice of third-party and out of country processing of data, and stated that the law cannot prevent an organization from responding to a lawful subpoena.

Comment on the issues raised in this item at IT.Can blog

2ième partie

Accès à distance à des renseignements personnels ayant un caractère public

Il est admis que le nom d'un propriétaire constitue un renseignement personnel qui a un caractère public puisque ce nom est contenu au rôle d'évaluation et est aussi accessible au registre foncier. Mais la Ville de Montréal conteste le droit de l'appelante d'avoir accès au rôle d'évaluation en ligne ou à distance avec la mention du nom du ou des propriétaires d'un immeuble. La Commission d'accès à l'information avait avalisé la position de la ville de Montréal (décision rapportée dans le *Bulletin IT.Can* du 1 juin 2006.

Le Tribunal renverse sur ce point la Commission d'accès et conclut que le refus de la Ville de Montréal de donner accès à distance au rôle d'évaluation qui contient le nom des propriétaires n'est pas conforme à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* L.R.Q., c. A-2.1 (*Loi sur l'accès*). Le Tribunal ne comprend pas pourquoi la Ville de Montréal refuse l'accès en ligne ou à distance, à un élément d'information qui fait partie intégrante de tout rôle d'évaluation, soit le nom du ou des propriétaires d'un immeuble. Le juge affirme qu'il n'y a rien d'illégitime ou de contraire à la Loi qu'une personne puisse avoir accès non seulement aux données de l'évaluation foncière d'un immeuble, mais aussi au nom du ou des propriétaires de cet immeuble. Le régime de la publicité des droits réels et plus généralement du droit immobilier au Québec est à l'effet que le nom d'un propriétaire d'un bien immobilier possède un caractère public et est accessible à toute personne qui désire obtenir un renseignement à cet effet. Il est admis que le nom du propriétaire d'un immeuble apparaît au rôle d'évaluation. Restreindre le rôle d'évaluation uniquement à la question de l'évaluation foncière est contraire à une des constituantes mêmes de ce rôle d'évaluation, soit de connaître le nom d'un propriétaire d'un immeuble.

Le Tribunal considère qu'à titre de journaliste, l'appelante a le droit d'avoir accès à distance et en ligne à un document qui est déjà détenu par la Ville de Montréal sur support informatique, en l'occurrence les rôles d'évaluation foncière de l'ensemble des immeubles de la Ville de Montréal.

Le nom d'un propriétaire, bien qu'il puisse être qualifié de renseignement personnel au sens de l'article 54 de la *Loi sur l'accès,* possède un caractère public, si bien qu'il ne peut être soumis aux règles de protection des renseignements personnels prévues par cette Loi, le tout en application de son article 55.

Le Tribunal n'avait pas à tenir compte du deuxième paragraphe de l'article 55 de la *Loi sur l'accès* qui n'était pas en vigueur au moment de la décision rendue par la Commission d'accès. Mais le juge note qu'il serait difficilement compréhensible qu'un responsable de la Ville de Montréal puisse refuser l'accès au nom d'un ou des propriétaires sur un rôle d'évaluation alors que ce renseignement ou cette donnée fait partie intégrante du rôle d'évaluation foncière.

Par contre le tribunal répond que le refus de la Ville de Montréal de donner accès à un rôle d'évaluation permettant les recherches à partir du nom d'un propriétaire est conforme à la *Loi sur l'accès*. Le Tribunal considère que la décision à cet égard est bien fondée et ce, en appliquant la norme de contrôle de la décision correcte. La Loi ne permet pas à une personne d'obtenir des outils informatiques qui n'existent pas et qui nécessiteraient une création ou une conception, aussi facile puisse-t-elle être. Il est admis que la Ville de Montréal n'utilise pas d'outils de recherche par nom d'un propriétaire en rapport avec son rôle d'évaluation. Le Tribunal considère qu'il serait extraordinaire de permettre à une personne d'obliger la Ville de Montréal à lui fournir un outil informatique qui n'existe pas actuellement. Aucune disposition d'une loi permet au Tribunal d'ordonner à la Ville de Montréal de créer ou de mettre à la disposition de toute personne un tel outil informatique.

- *Gyulai c. Montréal (Ville de)*, Cour du Québec, chambre civile, 14 mars 2007, 2007 QCCQ 2225.

Commentez cet article au Blogue de IT.CAN

Problèmes de sécurité dans les systèmes de dossier médicaux personnels – France

À l'occasion de contrôles exercés chez les participants à la phase d'expérimentation du dossier médical personnel (DMP), la CNIL a relevé un certain nombre d'insuffisances relatives à la sécurité des données. Menés auprès des centres hospitaliers, des réseaux de santé, médecins, centres d'appel et hébergeurs, les contrôles concluent que « la courte durée d'expérimentation du DMP ne permet pas de mesurer son fonctionnement effectif et que les mesures de sécurité doivent être renforcées ».

Dans son communiqué, la CNIL explique que certains hébergeurs transféraient les identifiants de patients aux établissements de soins par voie électronique sans protection particulière. Certains centres d'appel, en cas de perte des identifiants permettant la consultation ou l'alimentation des DMP, envoyaient un mot de passe par courrier électronique non crypté au patient, ou lui communiquaient ce mot de passe par téléphone. Ces pratiques sont de nature à compromettre la confidentialité de ces informations. Les modalités pratiques retenues pour permettre au patient de désigner nominativement les professionnels de santé autorisés à consulter et à alimenter le DMP se sont parfois traduites par des désignations collectives d'établissements ou de cabinets médicaux. La CNIL a aussi relevé que les patients n'étaient pas tous parfaitement informés que l'accès aux données médicales contenues dans leur DMP nécessitait une connexion Internet. De plus, il leur a été parfois indiqué que l'accès à ces données était possible par l'intermédiaire du centre d'appel de l'hébergeur, alors que ce dernier a pour seule fonction d'assister techniquement les patients ou de leur permettre de modifier les données administratives les concernant, leur mot de passe ou la composition de leur cercle de confiance.

En droit français, c'est la *Loi relative aux droits des malades* (Loi n° 2002-303 du 4 mars 2002, J.O. 5 mars 2002) qui a introduit l'article L. 1111-8 au *Code de la santé publique*. Cette disposition organise le régime juridique du contrat d'hébergement de données de santé. Aux termes de l'article L.1111-8, « la prestation d'hébergement fait l'objet d'un contrat ». Elle dispose que : « Les professionnels de la santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès des personnes physiques ou morales agréées à cet effet. »

La détention matérielle des données étant transférée à l'hébergeur, celui-ci se trouve en position de dépositaire. Seuls les hébergeurs agréés sont autorisés à conclure des contrats d'hébergement. Pour l'hébergeur, le défaut d'agrément expose à une sanction pénale et à la nullité du contrat. Les parties au contrat sont les professionnels de la santé, les établissements de santé et la personne concernée. L'accord de cette dernière est une condition de validité du contrat.

- Vincent DELFAU, « Dossier médical personnel : la Cnil soulève des problèmes de sécurité », *LeMondeInformatique.fr,* 17 avril 2007.
- Aussi CNIL, « La CNIL contrôle le dossier médical personnel », 14 avril 2007.

Responsabilité des opérateurs de sites à contenu défini par les usagers – France

Dans une décision rendue le 7 mars 2007, la Cour d'appel de Paris pose un principe de responsabilité pour les opérateurs économiques lorsque leurs utilisateurs portent atteinte aux droits de tiers. La décision reconnaît l'obligation des opérateurs de veiller à ce que leur site ne soit pas le moyen pour des usagers de se prêter à des actes illicites. Ils engagent donc leur responsabilité en cas de manquement à ce devoir. La cour d'appel a retenu la responsabilité de la société Sedo qui opère un site de vente aux enchères de noms de domaine et tire une rétribution des transactions effectuées par les usagers.

- *Hôtels Meridien c. Sedo*, Cour d'appel de Paris 4ème chambre, section A Arrêt du 7 mars 2007.

Condamnation à retirer d'un site une vidéo attentatoire au droit à l'image – France

La société éditrice du magazine Choc et du site Internet du magazine accessible à l'adresse URL http://www.choc.fr/ diffusait une vidéo publicitaire intitulée « Delarue la vidéo » d'une durée d'une minute et quarante huit secondes. La vidéo qui semble avoir été captée au moyen d'un téléphone portable, était présentée comme étant la vidéo d'un incident survenu le 14 février 2007 pendant le vol Air France Paris-Johannesburg à la suite duquel « trois hôtesses et stewards d'Air France du vol AF 990, ont déposé plainte le 16 février auprès de la police des frontières de l'aéroport de Roissy contre Jean Luc Delarue, qui aurait eu un comportement agressif et injurieux à l'encontre du personnel navigant et des passagers ».

Le nom de Jean Luc Delarue est cité par une personne proche de celle qui filme la scène ... « c'est Delarue là » ; les traits du personnage central sont fortement ressemblants à ceux de Jean Luc Delarue ; l'acteur principal est un sosie du journaliste dont le jeu reproduit l'incident relaté dans la presse. Une minute et vingt deux secondes après le début du film, le déroulement des faits prend une tournure de violence extrême, révélant la supercherie et apparaît à l'écran le slogan publicitaire « Si c'était vrai ce serait dans Choc ». Cette vidéo était librement téléchargeable sur le site du magazine Choc.

Jean Luc Delarue a fait assigner en référé la Scpe se plaignant que cette vidéo crée une réelle confusion dans l'esprit du public et constitue un trouble manifestement illicite en portant une atteinte exceptionnellement grave à son image, sa voix, son nom par cette utilisation promotionnelle, dévalorisante et non autorisée. Il a également fait valoir que depuis la mise en ligne de cette publicité « virale », celle-ci a été détournée sur les sites Dailymotion.com et Youtube.com ainsi que sur des dizaines de blogs, assurant une large diffusion à cette publicité sans débourser de frais techniques ou d'achat d'espace.

Le tribunal convient qu'un fait d'actualité peut légitimement être repris dans des conditions non contraires à la dignité. Mais il ne saurait être détourné à des fins manifestement et exclusivement commerciales, quel que soit le ton humoristique du procédé, fût-ce en faisant appel à un sosie qui entretient en l'espèce la confusion.

Le tribunal a ordonné l'interdiction d'utiliser les vidéos litigieuses et d'insertion sur le seul site www.choc.fr considérant que cela serait de nature à mettre un terme au trouble manifestement illicite résultant de ce procédé publicitaire.

Le fait que le tribunal n'a pas jugé à propos d'ordonner le retrait de la vidéo litigieuse des autres plate formes sur lesquelles elle a été reprise surprend le rédacteur de LÉGALIS.NET qui observe que « Si on estime que choc.fr n'est pas responsable juridiquement de la présence de ces vidéos sur les autres sites, il a quand même pris la responsabilité d'utiliser un procédé de publicité virale, qui une fois lancée sur Internet n'est plus guère contrôlable. D'ailleurs, son opération de promotion a formidablement bien marché puisque la vidéo s'est répandue comme une traînée de poudre sur le web comme sur les messageries électroniques. Grâce à cette publicité détournée, Choc Hebdo s'est, en effet, vendu à 420 000 exemplaires. Dans un tel contexte, ne faudrait-il pas appliquer à l'Internet le principe du « pollueur-payeur » que connaît l'industrie ? ».

- LÉGALIS.NET, *Choc.fr condamné à retirer « Delarue la vidéo » de son site mais pas de l'Internet*, 29 mars 2007.
- *Jean Luc Delarue / Société de conception de presse et d'édition (Scpe)*, Tribunal de grande instance de Nanterre Ordonnance de référé 23 mars 2007.

Commentez cet article au Blogue de IT.CAN

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 Teresa Scassa, 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 Teresa Scassa, 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.